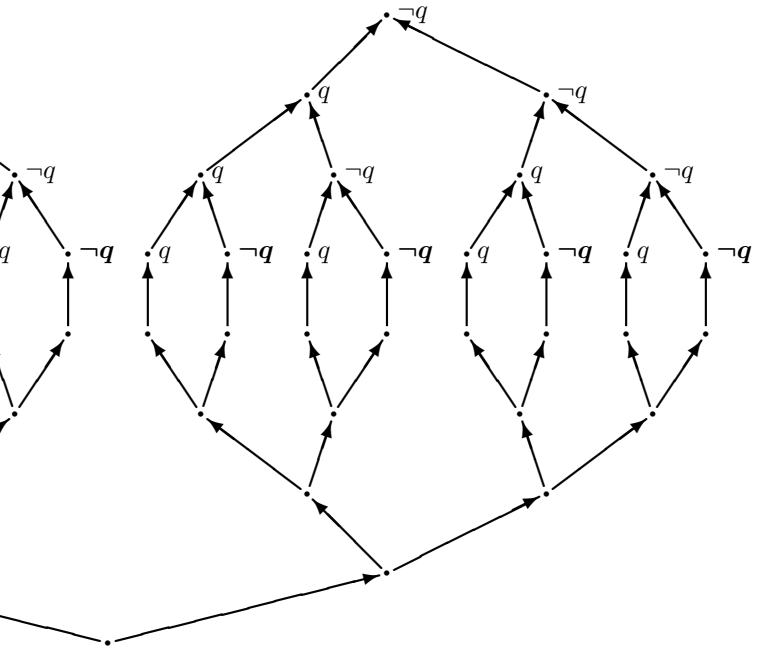
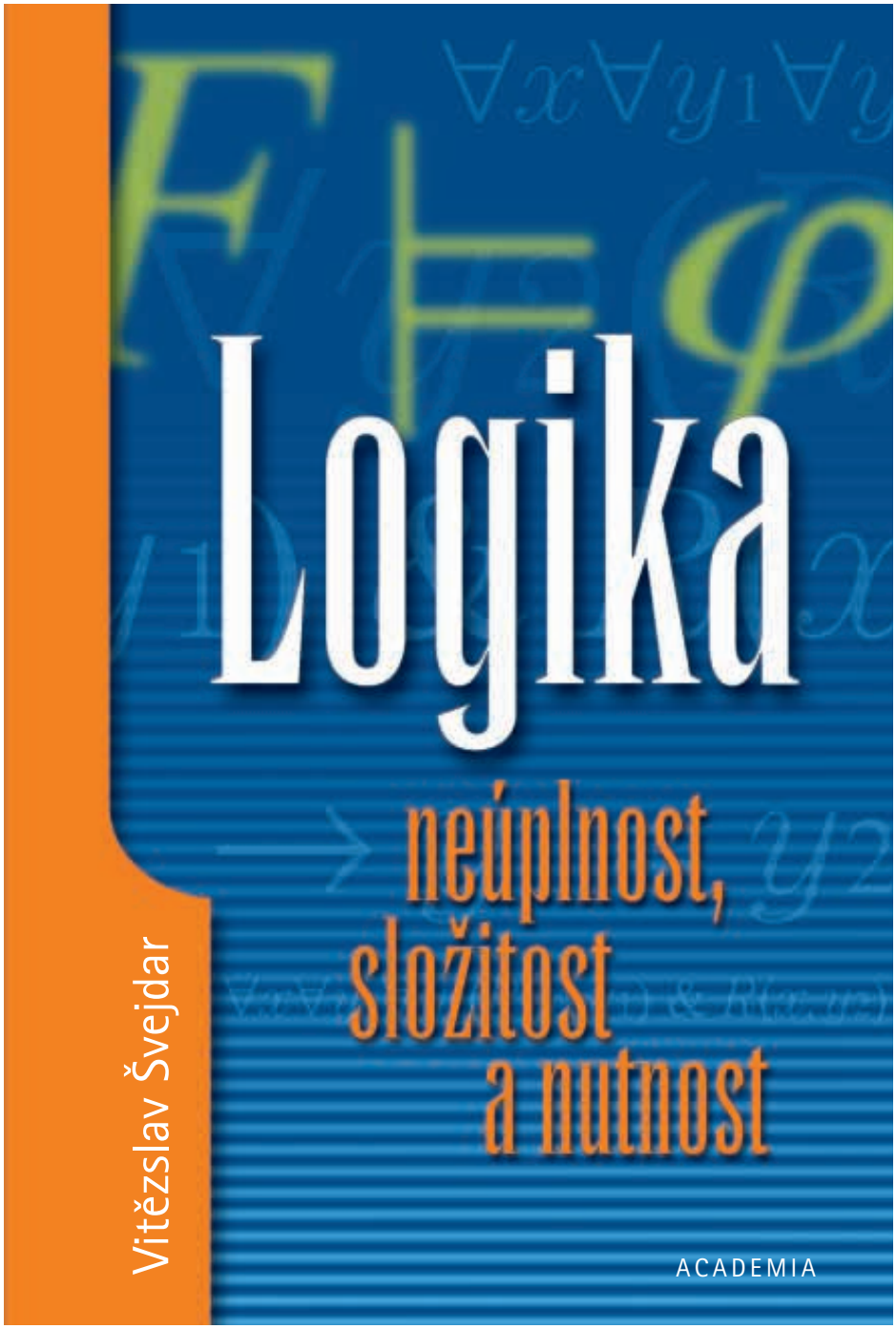
VÍTĚZSLAV ŠVEJDAR

LOGIKA
neúplnost, složitost a nutnost

Tento dokument ve formátu pdf pořídil a zpřístupnil autor knihy za podmínek, které byly domluveny s nakladatelstvím Academia. Dokument nesmí být nijak modifikován a žádná jeho část nesmí být tisknuta.



Publikace vyšla s podporou Akademie věd České republiky


Logika
neúplnost,
složitost
a nutnost
Vítězslav Švejdar
ACADEMIA

© Vítězslav Švejdar, 2002

ISBN 80-200-1005-X

Předmluva

V letech 1992–94 přednášel Petr Hájek logiku pro studenty informatiky na Matematicko-fyzikální fakultě UK a já jsem vedl cvičení. K této výuce jsme napsali učební text [32], který však byl velmi stručný a na desítkách míst se odvolával na skripta P. Štěpánka [88]. Tehdy Petr nadhodil, že by bylo dobré všechny chybějící důkazy vypracovat, a pořídit tak kompletní skripta či knihu. Protože jsem chtěl, aby nějaký učební text doprovázel i kurs logiky, který učím na FF UK, rychle jsem tuto myšlenku přijal za svou.

Tak vznikl projekt napsat společně knihu o logice, která je určena nikoliv čtenářům, kteří se chtějí naučit logicky myslet, nýbrž čtenářům, kteří logicky myslet už dávno umějí, a to zpravidla proto, že udělali nějakou zkušenost s *univerzitní matematikou*. Zejména by měli mít určitou představu o teorii množin a o programování. Rozumělo se přitom, že kniha položí důraz na ty části logiky, jejichž výzkum má v pražském či středoevropském prostředí dobrou tradici, zejména na problematiku Gödelových vět o neúplnosti a obecně metamatematiky teorií obsahujících aritmetiku, na souvislosti logiky a teoretické informatiky a na (některé) neklasické logiky.

Po více než pěti letech, když byl text už téměř hotov, Petr usoudil, že nemůže být spoluautorem, neboť jeho podíl je příliš malý. To je formalistické stanovisko — Petr sice fakticky napsal pouze oddíl 5.2 o Gödelově fuzzy logice, avšak podstatně větší část a možná *všechno* inspiroval. Chci mu tedy alespoň co nejsrdečněji poděkovat za jeho příspěvek, za stálou podporu a za všechna ta léta, kdy byl mým učitelem.

Za cenné poznámky k textu chci poděkovat kolegům, studentům a přátelům Tomáši Auerovi, Kamile Bendové, Radku Honzíkovi, Petru Jansovi, Petru Jirků, Janu Krajíčkovi, Ladislavu Nebeskému, Michalu Pelišovi, Petru Savickému, Jiřímu Sgallovi, Haně Skřivanové, Jiřímu Vaňkovi a Martě Vlasákové. Mnoha dalším studentům děkuji za podnětné poznámky a otázky, které kladli při mých hodinách. Za zájem a podporu děkuji Pavlu Pudlákovi, Petru Štěpánkovi a Petru Vojtášovi. Zvlášť chci poděkovat Janu Štěpánkovi, který velkou část textu přepsal na počítači a měl přitom užitečné připomínky, a Emilu Jeřábkovi, který odhalil řadu závad v přípravných verzích.

Děkuji také Grantové agentuře UK, která grantem podpořila přípravu knihy, Ediční radě AV ČR, která dotovala její vydání, a Vladimíru Petkevičovi, který finální text v krátké době přečetl a měl užitečné poznámky k využívání a zneužívání

češtiny. Nakonec a především děkuji své rodině. Haně za zázemí, které mi vytvářela, a za rady a poznámky, které mi byly mnohokrát užitečné v pedagogické práci, a dcerám Idě a Sylvě za to, že mi občas připomněly, jak některé věci vypadají z pohledu studenta.

Vítězslav Švejdar, březen 2002

Obsah

Úvod

The reader (...) learns the language of say predicate logic in much the same way as the notion of polynomial; he is not tempted to that misplaced pedantry which led to the odd idea that logic is the hygiene of mathematics (...).

(G. Kreisel, J. L. Krivine v [51])

V matematice jsou velmi často užívány symbolické zápisy. Mohou označovat výroky, například $\forall x \forall y(x \cdot y = y \cdot x)$, vlastnosti objektů, například $\exists v(v^2 = x)$, nebo vztahy mezi objekty, například $x \in y$. Lze říci, že jejich užití je všeobecné a pro matematiku typické. Zdaleka to však neznamená, že se vyskytují jen v matematice. Symbolické zápisy výroků, vlastností a vztahů mezi objekty budeme nazývat *formulemi*.

Uvažujme nyní těchto pět formulí (axiomů):

Ax1: $\forall x \forall y(x \leq y \equiv \exists v(v + x = y))$,

Ax2: $\forall x \forall y \forall z(x + z \leq y + z \rightarrow x \leq y)$,

Ax3: $\forall x \forall y \forall z((x + y) + z = x + (y + z))$,

Ax4: $\forall x \forall y(x \cdot y \leq x \ \& \ x \cdot y \leq y)$,

Ax5: $\forall x \forall y \forall z(z \leq x \ \& \ z \leq y \rightarrow z \leq x \cdot y)$,

a položme si otázku, zda z uvedených formulí *vyplývá* následující formule D

$$\forall a \forall b \forall c((a + c) \cdot (b + c) \leq (a \cdot b) + c),$$

tj. zda formule D je *důsledkem* axiomů Ax1–Ax5. Na první pohled by se mohlo zdát, že než se na tuto otázku pokusíme odpovědět, musíme vědět, o čem se mluví (zda například o číslech nebo o jiných objektech) a jaký význam mají symboly $+$, $\cdot$ a $\leq$ vyskytující se v našich formulích. Pak budeme moci rozhodnout o pravdivosti všech formulí. Například o formulích Ax1–Ax3 lze říci, že platí v oboru nezáporných čísel, pokud symboly $+$ a $\leq$ mají obvyklý význam. Formule D by platila, kdyby $+$ a $\cdot$ označovalo operace spojení a průsek v nějaké booleovské algebře. Každá z operací

spojení a průsek je totiž v každé booleovské algebře distributivní vůči druhé. V tom případě by platily i formule Ax1 a Ax3–Ax5, ale neplatila by formule Ax2.

Na otázku, zda D vyplývá z Ax1–Ax5, lze ve skutečnosti odpovědět kladně i bez informace, o čem se mluví a jaký význam mají symboly $+$, $\cdot$ a $\leq$. Formuli D lze totiž z formulí Ax1–Ax5 *odvodit* následující úvahou:

> Nechť a, b a c jsou dány. Pišme d místo $(a+c)\cdot(b+c)$. Máme ověřit, že $d \leq (a\cdot b)+c$. K c lze něco přičíst zleva (totiž a) tak, aby výsledek byl $a+c$. Z předpokladu Ax1 tedy plyne $c \leq a+c$. Ze stejného důvodu platí také $c \leq b+c$. V tom případě ale vzhledem k Ax5 platí $c \leq d$. Použijme nyní Ax1 ve směru zleva doprava: existuje q takové, že $q+c=d$. Podle Ax4 použitého na $x := a+c$ a $y := b+c$ platí $q+c \leq a+c$ a $q+c \leq b+c$. Teď použijme Ax2: máme $q \leq a$ a $q \leq b$. Ax5 dává $q \leq a\cdot b$. To je téměř to, co jsme potřebovali, neboť Ax1 a Ax3 dávají $q+c \leq a\cdot b+c$ a $q+c$ je d.

Místo odvození se také říká *důkaz*. Čtenář se při svém studiu matematiky jistě už setkal s větším množstvím důkazů více nebo méně podobných našemu příkladu. S trochou nadsázky můžeme říci, že matematika se neskládá z ničeho jiného než z důkazů.

Přestože zdůrazňujeme, že naše formule D vyplývá z Ax1–Ax5 bez ohledu na význam symbolů $+$, $\cdot$ a $\leq$, prozraďme, kde má náš příklad původ. Všechny předpoklady Ax1–Ax5 platí v oboru nenulových přirozených (případně celých) čísel, pokud $+$ znamená násobení a $x\cdot y$ je největší společný dělitel čísel x a y. V tom případě $\leq$ musí znamenat relaci dělitelnosti (Ax1 je vlastně její definice) a formule D vyjadřuje ne zcela triviální fakt, totiž víceméně to, že v oboru přirozených nebo celých čísel pro operace největší společný dělitel a násobení platí distributivní pravidlo.

Intuitivně je téměř jasné, jaká posloupnost symbolů je a jaká není formulí, čili jaká posloupnost symbolů je správně utvořeným zápisem nějakého vztahu mezi objekty či správně utvořeným zápisem nějakého (pravdivého nebo nepravdivého) výroku. Není překvapivé, že na této intuici lze založit formální definici syntakticky správné formule. Lze něco podobného jako o formulích říci i o důkazech, tj.

- *Lze formálně definovat pojem důkazu?*

Uvidíme, že odpověď na tuto otázku je ANO. To se může zdát překvapivé, víme přece, že nalézt důkaz určitého tvrzení často vyžaduje značnou dávku invence a nelze předem říci, jaké obraty budou v onom důkazu použity. Přesto je tomu tak; ukazuje se, že všechny dosud vytvořené důkazy vyhovují definici, která se skládá z několika jednoduchých pravidel. Tento fakt lze pokládat za důležitý objev a úspěch logiky.

Formální definice formule a důkazu umožňuje s formulemi a důkazy zacházet jako s matematickými objekty, to znamená řešit problémy, které se jich týkají, a dokazovat o nich tvrzení. Představme si například, že máme odpovědět na otázku, zda existuje důkaz nějakého konkrétního tvrzení z nějaké dané množiny předpokladů. Tvrdíme-li, že ano, můžeme se případně obejít bez jakékoliv logické teorie

a důkaz prostě napsat. Čtenář si to může vyzkoušet na tomto cvičení: formule

$$\forall a \forall b \forall c((a \cdot b) + c \leq (a + c) \cdot (b + c)) \quad \text{a} \quad \forall a \forall b \forall c(a \leq b \ \& \ b \leq c \rightarrow a \leq c)$$

jsou také odvoditelné z našich předpokladů Ax1–Ax5. Teorie pracující s pojmem formálního důkazu a obsahující jeho přesnou definici je ale nezbytná, tvrdíme-li, že ne, dané tvrzení *není* dokazatelné z dané množiny předpokladů. Pěkným příkladem tohoto druhu je tvrzení známé jako hypotéza kontinua: *každá nespočetná podmnožina množiny* R *všech reálných čísel má tutéž mohutnost, jako celá množina* R. Po mnoho desetiletí selhávaly všechny pokusy dokázat hypotézu kontinua z axiomů teorie množin a otázka, zda takový důkaz existuje, byla velmi známým otevřeným problémem. Až v roce 1963 dokázal P. Cohen, že odpověď na tuto otázku je negativní, hypotézu kontinua z axiomů teorie množin dokázat *nelze*.[1]

Definice důkazu spolu s faktem, že formule a důkazy jsou dosti konkrétními objekty, skládajícími se ze znaků, umožňují kromě otázek o dokazatelnosti jednotlivých formulí položit také otázky týkající se množin důkazů nebo množin formulí:

- *Existuje algoritmus, který pro danou posloupnost znaků rozhodne, zda je nebo není důkazem z daných předpokladů?*

Každá posloupnost symbolů vyhovující definici důkazu je důkazem a zdůraznili jsme, že důkaz je důkazem bez ohledu na význam symbolů v něm obsažených. To znamená, že typickou odpovědí na tuto otázku je ANO. Přesněji, odpověď je ANO za podmínky, že existuje algoritmus schopný rozhodovat o tom, co je a co není předpokladem, tj. za podmínky, že množina předpokladů je algoritmicky rozhodnutelná. Tato podmínka je ovšem automaticky splněna ve všech případech, kdy množina předpokladů je konečná. Domyšleno trochu dále, odpověď ANO na naši otázku znamená, že kdybychom autora jakéhokoliv důkazu přinutili napsat jeho důkaz dostatečně podrobně, mohl by pak správnost důkazu zkontrolovat počítač.

Zkontrolovat správnost již existujícího důkazu může být užitečné, ale v době, kdy důkaz ještě nemáme, bychom jistě velice uvítali informaci, zda hledaný důkaz existuje. Uvidíme, že na otázky

- *Existuje algoritmus, který pro danou formuli rozhodne, zda je nebo není dokazatelná z daných předpokladů?*
- *Existuje algoritmus, který pro danou formuli rozhodne, zda platí v určitém konkrétním oboru, například v oboru reálných čísel nebo v oboru přirozených čísel?*

neexistuje žádná typická odpověď. Pro některé množiny předpokladů nebo číselné (nebo jiné) obory je odpověď ANO a pro jiné NE.

Odpověď ANO na otázku po algoritmické rozhodnutelnosti znamená, že máme algoritmus, který správně vyřeší všechny instance dané úlohy. Odpověď NE však znamená víc než to, že jej nemáme. Nemáme jej z dobrého důvodu, totiž proto,

[1] Za předpokladu, že existuje vůbec nějaké tvrzení, které nelze z axiomů teorie množin dokázat.

že neexistuje. Ve 30. letech dvacátého století, tedy dříve, než byly vyvinuty elektronické počítače, vznikly teoretické modely počítačů a o některých úlohách vyskytujících se v logice bylo skutečně dokázáno, že nejsou algoritmicky rozhodnutelné. Od té doby logika úzce souvisí s teoretickou informatikou. Mezi pojmy algoritmus, výpočet a důkaz existují četné analogie, algoritmicky zajímavé úlohy často vznikají právě v logice a logické metody se naopak uplatňují v informatice. Jsme přesvědčeni, že pojem algoritmu dnes patří spolu s pojmy důkaz a důsledek k základním logickým pojmům.

Úmluva, že s formulemi a důkazy zacházíme jako s čísly, funkcemi, množinami a ostatními matematickými objekty a v úvahách o nich užíváme matematické prostředky, na první pohled nebudí žádné podezření. Už v kapitole 1 se ale čtenář možná pozastaví nad důkazem věty o kompaktnosti ve výrokové logice, ve kterém použijeme topologické pojmy a vlastně i Tichonovovu větu o kartézském součinu topologických prostorů. Čtenáře by mohlo napadnout, že než si dovolíme užívat metod teorie množin při studiu konkrétních objektů, měli bychom teorii množin prozkoumat hlouběji a nezpochybnitelným způsobem prokázat oprávněnost jejích prostředků. Případně bychom to mohli udělat ve více krocích: v každém kroku bychom pomocí prostředků, o kterých dosud víme, že jsou oprávněné a nezpochybnitelné, prokázali správnost, oprávněnost a nezpochybnitelnost dalších prostředků, které by pak bylo dovoleno užívat v příštím kroku. Toto je zhruba obsah tzv. *Hilbertova programu* (budování matematiky a logiky). V kapitole 4 se seznámíme s Gödelovými větami o neúplnosti, z nichž slavnou Druhou větu o neúplnosti interpretujeme tak, že Hilbertův program je neproveditelný. Z matematických metod nelze vydělit ty, které jsou finitní, tj. nezpochybnitelné a nezávislé na formálních teoriích. Teorie množin nebo některá jiná formální teorie nutně hraje v logice dvojakou roli: poskytuje prostředky k výzkumu logických objektů, tedy i formálních teorií, a zároveň jako formální teorie je předmětem výzkumu.

- *Lze se v důkazech tvrzení o konkrétních objektech, jako jsou formule, důkazy nebo počítačové programy, vždy obejít bez náročnějších a abstraktnějších pojmů a prostředků, jako jsou funkce na nekonečných množinách, prostory různého druhu nebo třeba ordinální indukce či ordinální rekurze?*

Odpověď na tuto poněkud vágní otázku tedy zní NE.

Bohužel, chtělo by se dodat. Má ale dobrý smysl říci bohužel, když se nepodařilo udělat něco, co udělat nelze?

V kapitole 4 a v oddílu 5.3 uvidíme, že Gödelovy věty o neúplnosti lze chápat také pozitivně, tj. jako něco, co lze hlouběji prozkoumat a osvětlit a co může sloužit jako nástroj k řešení problémů.

Takže formule, důkazy, důsledek, úlohy a algoritmy. To, co vypadá jako rozumný plán výzkumu, nemusí být vždy také proveditelné a někdy lze dokázat, že proveditelné není. A netýká se to jen Hilbertova programu. O tom to všechno bude.

1

Výroková logika

Všechny důležité matematické věty mají tvar ekvivalence. *(J. Krajíček)*

Nebo jsou to spodní odhady. *(J. Sgall)*

1.1 Formule a sémantika výrokové logiky

V příkladu obsaženém v úvodu jsme viděli, že v symbolických zápisech výroků, vlastností a vztahů se uplatňují symboly několikerého druhu: symboly pro relace mezi objekty a pro operace s objekty (například $\leq$ a $+$), proměnné x, y, ..., pomocné symboly, totiž závorky, a konečně *logické symboly*, které můžeme rozdělit na *logické spojky* ($\&$, $\vee$, $\rightarrow$ a $\neg$) a *kvantifikátory* ($\forall$ a $\exists$). Složitější formule jsou sestaveny z jednodušších pomocí logických spojek a kvantifikátorů. V této kapitole se zabýváme *výrokovou logikou*, ve které se z logických symbolů uvažují pouze logické spojky. Kvantifikátory se ignorují spolu se vším, co k nim patří. Formule začínající kvantifikátorem a také formule jako $v \cdot v \leq x$, jež neobsahují žádné logické symboly, se ve výrokové logice považují za dále nedělitelné. Složitější výrokové formule jsou tedy sestaveny z jednodušších pomocí logických spojek.

Předpokládejme, že jsme pevně zvolili neprázdnou množinu symbolů At neobsahující žádný ze šesti symbolů $(,), \&, \vee, \rightarrow, \neg$. Prvkům množiny At říkejme *výrokové atomy* nebo jen *atomy*. Následující definice říká, které z výrazů sestavených z prvků množiny $\mathrm{At} \cup \{(,), \&, \vee, \rightarrow, \neg\}$ jsou výrokovými formulemi.

Definice 1.1.1 *Množina všech* výrokových formulí *je nejmenší množina výrazů splňující podmínky*

- *každý výrokový atom je výroková formule,*
- *je-li φ výroková formule, pak $\neg\varphi$ je výroková formule,*
- *jsou-li φ a ψ výrokové formule, pak $(\varphi \,\&\, \psi)$, $(\varphi \vee \psi)$ a $(\varphi \rightarrow \psi)$ jsou výrokové formule.*

Jsou-li p, q a r výrokové atomy, pak $((p \vee \neg q) \to r)$, dále $\neg(p \,\&\, \neg p)$ a ovšem také p a $\neg p$ jsou příklady výrokových formulí. Výrazy

$$\neg(p), \qquad p \,\&\, \neg q, \qquad p \vee q \to r$$

podle naší definice výrokovými formulemi nejsou, ale přinejmenším druhý a třetí z nich posuzujme shovívavě. Domluvme se, že úplně vnější pár závorek je povoleno vypouštět, a dále, že spojkám & a $\vee$ přisuzujeme vyšší prioritu než spojce $\to$. Výraz $p \vee q \to r$ je tedy přípustný zápis pro výrokovou formuli $((p \vee q) \to r)$.

Formule označujeme malými řeckými písmeny nebo velkými latinskými písmeny ze začátku abecedy. Množiny formulí označujeme velkými latinskými písmeny T, S, T_1, ... nebo velkými řeckými písmeny.

Spojky &, $\vee$, $\to$ a $\neg$ nazýváme *konjunkce*, *disjunkce*, *implikace* a *negace*. Formule $\varphi \,\&\, \psi$, $\varphi \vee \psi$, $\varphi \to \psi$, $\neg\varphi$ čteme „φ a ψ“ (případně „φ et ψ“), „φ nebo ψ“ (případně „φ vel ψ“), „pokud φ, pak ψ“ (případně „φ implikuje ψ“ nebo neutrálně „φ šipka ψ“) a „non φ“ (případně „není pravda, že φ“ nebo „ne φ“). V literatuře se vyskytují i jiné značky pro logické spojky: $\wedge$ pro konjunkci, | pro disjunkci, $\supset$ nebo $\Rightarrow$ pro implikaci, $\sim$ pro negaci.

Termíny konjunkce, disjunkce, implikace a negace vztahujeme nejen na samotné logické spojky, ale i na formule, které jsou z nich utvořeny. Říkáme například, že formule $\neg\varphi$ je negací formule φ. Má-li formule χ tvar $\varphi \to \psi$, pak formuli φ nazýváme *premisou* a formuli ψ *závěrem* implikace χ.

Definice 1.1.2 Pravdivostní ohodnocení *je každá funkce v z množiny všech výrokových formulí do množiny $\{0, 1\}$, která pro libovolné formule φ a ψ splňuje podmínky*

- $v(\varphi \,\&\, \psi) = 1$, *právě když* $v(\varphi) = 1$ *a* $v(\psi) = 1$,
- $v(\varphi \vee \psi) = 1$, *právě když* $v(\varphi) = 1$ *nebo* $v(\psi) = 1$,
- $v(\varphi \to \psi) = 1$, *právě když* $v(\varphi) = 0$ *nebo* $v(\psi) = 1$,
- $v(\neg\varphi) = 1$, *právě když* $v(\varphi) = 0$.

Zápis $v(\varphi) = 1$ čteme „formule φ je splněna (pravdivostním) ohodnocením v“ nebo „(ohodnocení) v splňuje formuli φ“. Místo $v(\varphi) = 1$ se někdy píše také $v \models \varphi$.

Sémantika klasické výrokové logiky je založena na představě, že každému výroku lze přisoudit právě jednu ze dvou pravdivostních hodnot 1 a 0. Hodnota 1 reprezentuje pravdu, 0 nepravdu. Podmínky v definici 1.1.2 určují, jak souvisí pravdivost výrokové formule s pravdivostí jejích komponent. Lze je schematicky znázornit následujícími tabulkami:

&	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

$\to$	1	0
1	1	0
0	1	1

	$\neg$
1	0
0	1,

kterým říkáme *pravdivostní tabulky logických spojek*. K tabulce implikace pro jistotu poznamenejme, že řádky se vztahují k premise a sloupce k závěru implikace, tj. že $v(\varphi \to \psi) = 1$ platí právě (pouze) tehdy, platí-li současně $v(\varphi) = 1$ a $v(\psi) = 0$. Z tabulky disjunkce je zřejmé, že spojku „nebo“ chápeme v obvyklém, tj. nevylučovacím smyslu: disjunkce $\varphi \vee \psi$ je nějakým ohodnocením v splněna i v případě, kdy jsou jím splněny obě formule φ a ψ.

Příklad 1.1.3 Je-li φ formule $(\neg p \vee q)$ & $(\neg p \to q)$ a v je ohodnocení takové, že $v(p) = v(q) = 0$, pak platí $v(\neg p) = 1$ a $v(\neg p \to q) = 0$, a tedy $v(\varphi) = 0$.

Každé pravdivostní ohodnocení je jednoznačně určeno svými hodnotami na výrokových atomech, a ty mohou být voleny libovolně a navzájem nezávisle. Někdy se pravdivostní ohodnocení definuje trochu jinak než v 1.1.2, totiž jako libovolná funkce z množiny At všech výrokových *atomů* do $\{0, 1\}$. Pravdivostní tabulky pak jednoznačně určují rozšíření $\overline{v}$ libovolného ohodnocení v na všechny výrokové formule. Je zřejmé, že takováto definice se od naší liší jen nepodstatně.

O některých formulích lze říci, že jsou automaticky pravdivé, tj. pravdivé díky své logické struktuře. Říká se také, že jsou logicky platné. Ve výrokové logice takovým formulím říkáme tautologie.

Definice 1.1.4 *Řekneme, že výroková formule φ je* splnitelná*, jestliže existuje pravdivostní ohodnocení v takové, že $v(\varphi) = 1$. Formule φ je* tautologie*, jestliže $v(\varphi) = 1$ pro každé pravdivostní ohodnocení v. Množinu všech splnitelných výrokových formulí a množinu všech tautologií značíme* Sat *resp.* Taut.

Příklad 1.1.5 V příkladu 1.1.3 je uvedena formule φ a pravdivostní ohodnocení v takové, že $v(\varphi) = 0$. Formule φ tedy není tautologie. Pro libovolné ohodnocení v takové, že $v(p) = 0$ a $v(q) = 1$, platí $v(\varphi) = 1$. Formule φ je tedy splnitelná.

Slovem „libovolné“ v předchozím příkladu chceme zdůraznit, že pravdivostní ohodnocení je definováno na množině *všech* výrokových formulí, tj. je definováno i na atomech jiných než p a q, a může tedy existovat mnoho (dokonce nespočetně mnoho, je-li množina At všech výrokových atomů nekonečná) ohodnocení v s vlastností $v(p) = 0$ a $v(q) = 1$. Je ale zřejmé, že pravdivostní hodnota $v(\varphi)$ závisí na ohodnocení jen těch atomů, které se ve φ vyskytují. Chceme-li určit, zda nějaká formule je tautologie, stačí probrat všechny funkce z F do $\{0, 1\}$, kde F je (konečná!) množina všech výrokových atomů, které se vyskytují v dané formuli. Ukažme si postup na formuli $B = \neg(p \vee q \to p \,\&\, r) \to (r \to q)$. Množina F všech atomů vyskytujících se v B má v našem případě tři prvky a všech funkcí z F do $\{0, 1\}$ je osm. Označme C formuli $p \vee q \to p \,\&\, r$ a utvořme tabulku jako na obrázku 1.1.1. V záhlaví tabulky jsou všechny podformule formule B a v prvních třech sloupcích jsou všechny možnosti, jak lze přiřadit pravdivostní hodnoty atomům p, q a r. Řádky tabulky odpovídají pravdivostním ohodnocením a pravdivostní tabulky logických spojek jednoznačně určují, jak v daném řádku na základě prvních tří hodnot stanovit pravdivostní hodnoty ostatních (neatomických) formulí. Pro

p	q	r	$r \to q$	$p \vee q$	$p \,\&\, r$	C	$\neg C$	$\neg C \to (r \to q)$
1	1	1	1					1
1	1	0	1					1
1	0	1	0	1	1	1	0	1
1	0	0	1					1
0	1	1	1					1
0	1	0	1					1
0	0	1	0	0	0	1	0	1
0	0	0	1					1

Obrázek 1.1.1: Tabulková metoda

přehlednost jsme nepodstatné hodnoty ponechali nevyplněné. Ve všech případech, kdy $v(q) = 1$ nebo $v(r) = 0$, platí $v(r \to q) = 1$, a tedy $v(B) = 1$ bez ohledu na hodnotu $v(\neg C)$. A ve zbývajících dvou případech rovněž platí $v(B) = 1$ díky tomu, že $v(\neg C) = 0$. Zjistili jsme, že formule B je tautologie. Při určování pravdivostních hodnot jsme ovšem mohli postupovat čistě mechanicky, čili systematicky vyplnit všechny hodnoty v tabulce bez úvah o tom, které jsou a které nejsou podstatné.

Právě popsaný postup, kterým lze zjistit, zda daná formule je nebo není tautologií nebo splnitelnou formulí, se nazývá *tabulková metoda*. Díky ní můžeme říci, že problém určit, zda daná formule je tautologie, je algoritmicky rozhodnutelný. Tabulková metoda ale není příliš efektivním algoritmem. Vyskytuje-li se v dané formuli n výrokových atomů, příslušná tabulka má 2^n řádků. Velikost pravdivostní tabulky formule, která se vejde do jediného řádku, může značně přesáhnout velikost průměrné knihy!

Definice 1.1.6 *Řekneme, že výroková formule φ je* (tautologickým) důsledkem *množiny formulí T nebo že φ* vyplývá *z T, a píšeme $T \models \varphi$, jestliže φ má pravdivostní hodnotu* 1 *při každém pravdivostním ohodnocení v, které přiřazuje hodnotu* 1 *všem formulím v T. Symbolicky:*

$$T \models \varphi \;\Leftrightarrow\; \forall v(\forall \psi \in T(v(\psi) = 1) \;\Rightarrow\; v(\varphi) = 1).$$

O množině T v této souvislosti mluvíme jako o množině předpokladů *nebo o množině* axiomů. *Formule φ je* důsledkem formule ψ, *jestliže* $\{\psi\} \models \varphi$. *Formule φ a ψ jsou* ekvivalentní, *jestliže φ je důsledkem ψ a zároveň ψ je důsledkem φ.*

Znaménko $\models$ jsme již dříve použili v jiném významu. V kontextu $v \models \varphi$ vlevo od $\models$ stojí pravdivostní ohodnocení a zápis znamená, že ono ohodnocení splňuje formuli φ. V kontextu $T \models \varphi$ vlevo stojí množina formulí a znaménko $\models$ znamená důsledek. Mohlo by se zdát, že kolizi bychom se mohli vyhnout tak, že znaménko $\models$ bychom vyhradili pouze pro vztah důsledku a místo $v \models \varphi$ bychom vždy psali $v(\varphi) = 1$. Ve výrokové logice je to asi pravda, ale se znaménkem $\models$ budeme pracovat i v predikátové logice a tam je jeho užití ve více významech natolik rozšířené, že je asi měnit nelze.

Příklad 1.1.7 Předpokládejme, že množina At všech výrokových atomů je nekonečná spočetná, $\mathrm{At} = \{p_0, p_1, p_2, \dots\}$, položme $T = \{p_n \to p_m; n < m\}$ a uvažujme, které formule tvaru $p_n \to p_m$ vyplývají z T. Když $n < m$, pak $p_n \to p_m$ vyplývá z T; je zřejmé, že každý prvek jakékoliv množiny T vyplývá z T. Když $n = m$, pak $p_n \to p_m$ také vyplývá z T, neboť má pravdivostní hodnotu 1 při každém pravdivostním ohodnocení, které přiřazuje hodnotu 1 všem prvkům z T (a při každém jiném pravdivostním ohodnocení ovšem také). Když $n > m$, pak pravdivostní ohodnocení v, pro které platí $v(p_i) = 0$ pro $i \leq m$, a $v(p_i) = 1$ pro $i > m$, splňuje všechny formule v T, ale nesplňuje formuli $p_n \to p_m$. Formule $p_n \to p_m$ tedy pro $n > m$ nevyplývá z T.

Věta 1.1.8 *(a) $T \cup \{\psi\} \models \varphi$, právě když $T \models \psi \to \varphi$.*
(b) Je-li T konečná, pak $T \models \varphi$, právě když $\{\bigwedge T\} \models \varphi$, kde $\bigwedge T$ je konjunkce všech formulí v T (v libovolném pořadí).
(c) $\emptyset \models \varphi$, právě když φ je tautologie.
(d) Formule φ a ψ jsou ekvivalentní, právě když pro každé pravdivostní ohodnocení v platí $v(\varphi) = v(\psi)$.

Důkaz ponecháváme za cvičení.

Z tvrzení (a)–(c) plyne, že je-li T konečná, pak $T \models \varphi$, právě když $\bigwedge T \to \varphi$ je tautologie. To znamená, že úloha, zda daná formule vyplývá z dané *konečné* množiny předpokladů, je algoritmicky rozhodnutelná a k jejímu řešení lze užít tabulkovou metodu.

Snadno lze ověřit, že každé dvě formule umístěné ve stejném řádku následující tabulky jsou spolu ekvivalentní (pro každou volbu formulí A, B a C):

$A \vee (B \vee C)$	$(A \vee B) \vee C$	asociativní zákony
$A \,\&\, (B \,\&\, C)$	$(A \,\&\, B) \,\&\, C$	...
$A \vee (B \,\&\, C)$	$(A \vee B) \,\&\, (A \vee C)$	distributivní zákony
$A \,\&\, (B \vee C)$	$(A \,\&\, B) \vee (A \,\&\, C)$	...
$\neg(A \,\&\, B)$	$\neg A \vee \neg B$	de Morganovy zákony
$\neg(A \vee B)$	$\neg A \,\&\, \neg B$	...
$\neg\neg A$	A	zákon dvojné negace.

V posledním sloupci je u každé ekvivalence uveden tradiční název. A když už jsme u vyjmenovávání tradičních „zákonů“: $\neg(A \,\&\, \neg A)$ (přesněji řečeno fakt, že každá formule tohoto tvaru je tautologií) se nazývá *zákon sporu* a $A \vee \neg A$ se nazývá *princip vyloučeného třetího* (lze se setkat i s latinským názvem *tertium non datur*).

Domluvme se, že vzhledem k platnosti asociativního zákona budeme často vypouštět závorky ve výrazech obsahujících několik konjunkcí nebo několik disjunkcí za sebou a například místo $A \vee ((B \vee C) \vee D)$ budeme psát jen $A \vee B \vee C \vee D$.

Nazvěme *literálem* každou formuli tvaru p nebo $\neg p$, kde p je výrokový atom. Disjunkce několika literálů se nazývá *klauzule*. Řekneme, že formule A je v *konjunktivním normálním tvaru*, jestliže A je konjunkcí klauzulí. Formule A je naopak v *disjunktivním normálním tvaru*, jestliže A je disjunkcí formulí, z nichž každá je konjunkcí literálů.

Příklad 1.1.9 Formule p i $\neg p \vee q$ jsou klauzule, takže formule $p \,\&\, (\neg p \vee q)$ je v konjunktivním normálním tvaru. Formule $\neg p \vee \neg q \vee r$ je (jednočlennou) konjunkcí klauzulí a zároveň je disjunkcí tří (jednočlenných) konjunkcí literálů. Je to tedy formule, která je jak v konjunktivním, tak v disjunktivním normálním tvaru.

Věta 1.1.10 *Každá výroková formule je ekvivalentní s jistou formulí, která je v disjunktivním normálním tvaru, a také s jistou formulí, která je v konjunktivním normálním tvaru.*

Důkaz Dokážeme indukcí podle počtu výskytů logických spojek v A, že libovolná formule A je ekvivalentní s nějakou formulí v disjunktivním a také s nějakou (jinou) formulí v konjunktivním normálním tvaru. Když A neobsahuje logické spojky, pak A je atomem, a tedy formulí v konjunktivním i v disjunktivním normálním tvaru.

Není-li A atomem, pak A je tvaru $\neg B$, $B \vee C$, $B \& C$ nebo $B \to C$. Probereme všechny čtyři případy. Každá z formulí B, C obsahuje méně logických spojek než A, a dle indukčního předpokladu je tedy každá z nich ekvivalentní s formulí v konjunktivním i s formulí v disjunktivním normálním tvaru. Existují tedy klauzule $E_1, \ldots, E_n$, $E_{n+1}, \ldots, E_{n+m}$ a formule v disjunktivním normálním tvaru D takové, že B je ekvivalentní s $E_1 \,\&\, \ldots \,\&\, E_n$, dále C je ekvivalentní s $E_{n+1} \,\&\, \ldots \,\&\, E_{n+m}$ a konečně B je ekvivalentní s D.

Utvořme z D formuli D' tak, že navzájem zaměníme konjunkce a disjunkce, odstraníme všechny negace, a naopak připíšeme negaci ke každému atomu, který ji dosud neměl. Je zřejmé, že při každém pravdivostním ohodnocení mají D a D' opačné pravdivostní hodnoty. Protože D je ekvivalentní s B, znamená to, že D' je ekvivalentní s $\neg B$. Navíc D' je konjunkcí klauzulí. Dokázali jsme, že $\neg B$ je ekvivalentní s nějakou formulí v konjunktivním normálním tvaru.

Nechť A je tvaru $B \,\&\, C$. Pak A je ekvivalentní s formulí

$$E_1 \,\&\, \ldots \,\&\, E_n \,\&\, E_{n+1} \,\&\, \ldots \,\&\, E_{n+m},$$

která je v konjunktivním normálním tvaru.

Nechť A je tvaru $B \vee C$. Pak A je ekvivalentní s formulí

$$(E_1 \,\&\, \ldots \,\&\, E_n) \vee (E_{n+1} \,\&\, \ldots \,\&\, E_{n+m})$$

a snadno lze ověřit, že také s formulí $\bigwedge_{1 \le i \le n < j \le n+m} (E_i \vee E_j)$, která je v konjunktivním normálním tvaru.

Je-li A tvaru $B \to C$, pak A je ekvivalentní s $\neg B \vee C$. Víme už, že $\neg B$ je ekvivalentní s formulí v konjunktivním normálním tvaru, a z předchozího odstavce víme,

jak k disjunkci dvou formulí v konjunktivním normálním tvaru nalézt ekvivalentní formuli také v konjunktivním normálním tvaru.

Dokázali jsme, že ve všech čtyřech případech je formule A ekvivalentní s formulí v konjunktivním normálním tvaru. Ponecháváme na čtenáři, aby domyslel, že A je ekvivalentní také s formulí v disjunktivním normálním tvaru. QED

Není pravda, že konjunktivní nebo disjunktivní normální tvar formule je určen jednoznačně, a nepomůže dodat „až na pořadí členů v konjunkcích a disjunkcích". Jednoduchým příkladem je formule $(p \to q)\ \&\ (q \to r)\ \&\ (r \to p)$, na kterou nás upozornil P. Savický. Ta je ekvivalentní jak s formulí $(\neg p \vee q)\,\&\,(\neg q \vee r)\,\&\,(\neg r \vee p)$, tak s formulí $(\neg p \vee r)\ \&\ (\neg r \vee q)\ \&\ (\neg q \vee p)$.

Někdy je výhodné pracovat s menším počtem než se čtyřmi logickými spojkami. V tom případě lze jen některé z nich prohlásit za základní (tj. za opravdové symboly) a formule obsahující ty ostatní považovat za zkratkovité zápisy formulí obsahujících jen ony základní. Lze dokonce vystačit s jedinou logickou spojkou, pokud si pro tento účel zvlášť definujeme novou logickou spojku jinou než $\&$, $\vee$ a $\to$. O tom jsou některá cvičení. Někdy je naopak výhodné seznam logických symbolů ještě rozšířit, například o *ekvivalenci* $\equiv$ nebo o tzv. *logické konstanty* $\top$ a $\bot$ (pravda a nepravda, verum a falsum), které se syntakticky chovají jako atomy, ale při každém pravdivostním ohodnocení má konstanta $\top$ povinně hodnotu 1 a konstanta $\bot$ naopak hodnotu 0. Konstanty $\top$ a $\bot$ lze považovat za „nulární" logické spojky.

Je dobré si uvědomit, že mluvíme-li o jazyce matematiky, chceme-li jej zkoumat matematickými prostředky a chceme-li si přitom pomáhat symbolickými zápisy, nelze se vyhnout užití některých slov a symbolů na dvou různých úrovních. Ve výrocích o logických symbolech a formulích se mohou vyskytnout třeba implikace a kvantifikátory. Například v symbolickém zápisu v definici důsledku se vyskytují kvantifikátory $\forall v$ a $\forall \psi$, které nemají význam formálních symbolů (to přijde až v predikátové logice), ale zkratek. Lze také říci, že kvantifikátory jsou tam použity na *metamatematické* úrovni. Jen v případě implikace a ekvivalence odlišujeme graficky formální symbol od metamatematické zkratky: formální symbol je $\to$ (a případně $\equiv$, pokud jsme ekvivalenci zahrnuli do seznamu formálních symbolů), na metaúrovni píšeme $\Rightarrow$ a $\Leftrightarrow$.

Cvičení

1. Určete, které z následujících výrokových formulí jsou splnitelné a které jsou tautologie:

$((p \to q) \to q) \to q$,	$\neg p \to \neg(p \vee (p\ \&\ q))$,
$\neg p \to \neg(p \vee q)$,	$(p \to (q \vee r)) \to (q \vee (p \to r))$,
$\neg p \to \neg(p\ \&\ q)$,	$(p \to q) \to ((q \to r) \to (p \to r))$,
$p \to p\ \&\ (p \vee q)$,	$(p \to q)\ \&\ q \to p$,
$p \to p \vee (p\ \&\ q)$,	$\neg p \to (p\ \&\ q)$,
$(p \to q) \vee (q \to p)$,	$((p \to q) \to p) \to p$.

2. Formule φ je splnitelná, právě když $\neg\varphi$ není tautologie. Když $\varphi \to \chi$ i $\chi \to \psi$ jsou tautologie, pak i $\varphi \to \psi$ je tautologie. Dokažte.

3. Rozhodněte, zda platí
(a) Když φ je tautologie a ψ vznikne z φ nahrazením některých výskytů atomu p toutéž formulí χ, pak ψ je tautologie.
(b) Když φ je tautologie a ψ vznikne z φ nahrazením všech výskytů atomu p toutéž formulí χ, pak ψ je tautologie.
(c) Když φ je tautologie a ψ vznikne z φ nahrazením všech výskytů atomu p libovolnými (i různými) formulemi, pak ψ je tautologie.
(d) Když ψ_1 resp. ψ_2 vznikne z φ nahrazením některých výskytů atomu p formulí χ_1 resp. χ_2 a χ_1 a χ_2 jsou ekvivalentní, pak ψ_1 a ψ_2 jsou ekvivalentní.

4. Předpokládejte, že i ekvivalence $\equiv$ se považuje za základní logickou spojku, a navrhněte pro ni pravdivostní tabulku tak, aby platilo toto: φ je ekvivalentní s ψ, právě když formule $\varphi \equiv \psi$ je tautologie.

5. Dokažte větu 1.1.8.

6. Dokažte, že jsou-li A a B libovolné výrokové formule, pak formule $A \,\&\, B$ je ekvivalentní s formulí $\neg(A \to \neg B)$. S použitím cvičení 3 zdůvodněte, že když ψ vznikne z φ nahrazením všech podformulí tvaru $A \,\&\, B$ formulí $\neg(A \to \neg B)$, pak φ a ψ jsou ekvivalentní. Navrhněte podobné záměny i pro ostatní logické spojky a zdůvodněte, že každá formule φ je ekvivalentní s formulí ψ, která neobsahuje jiné logické spojky než
(a) $\to$ a $\neg$
(b) $\&$ a $\neg$
(c) $\vee$ a $\neg$.

7. Pro libovolnou množinu výrokových formulí Γ označme $\mathrm{Cl}(\Gamma)$ (od anglického *closure*) množinu všech tautologických důsledků množiny Γ. Rozhodněte, zda pro každou množinu formulí Γ resp. pro každé dvě množiny Γ a Δ platí
(a) $\Gamma \subseteq \mathrm{Cl}(\Gamma)$,
(b) $\mathrm{Cl}(\mathrm{Cl}(\Gamma)) = \mathrm{Cl}(\Gamma)$,
(c) $\mathrm{Cl}(\Gamma \cup \Delta) = \mathrm{Cl}(\Gamma) \cup \mathrm{Cl}(\Delta)$.
Pokud v (b) nebo v (c) je odpověď ne, rozhodněte, zda platí alespoň některá inkluze.

8. *Booleovská funkce* n proměnných je libovolná funkce f z $\{0,1\}^n$ do $\{0,1\}$. Například rovnosti
$$f(0,0) = 0, \qquad f(0,1) = 0, \qquad f(1,0) = 1, \qquad f(1,1) = 0$$
určují jednu z booleovských funkcí dvou proměnných. Kolik je booleovských funkcí n proměnných? Řekneme, že výroková formule neobsahující jiné atomy než $p_0, \ldots, p_{n-1}$ *definuje* booleovskou funkci f, jestliže pro každé pravdivostní ohodnocení v je $v(\varphi) = f(v)$ (to je napsáno trochu nepřesně, ale snad je tomu

rozumět: formule $\neg(p_0 \to p_1)$ definuje funkci dvou proměnných zmíněnou výše). Dokažte, že každou booleovskou funkci definuje některá výroková formule.

Návod. Nejprve uvažujte funkce, které mají jen jednu hodnotu 1 a jinak samé hodnoty 0. Pak uvažujte disjunkce formulí definujících takové funkce.

9. Zdůvodněte, že na předchozím cvičení lze založit alternativní důkaz tvrzení, že každá formule je ekvivalentní s nějakou formulí v disjunktivním normálním tvaru.

10. Dokažte, že není pravda, že každá formule je ekvivalentní s nějakou formulí sestavenou jen z logických spojek $\&$, $\vee$ a $\to$.

    Návod. Dokažte, že každá formule sestavená jen ze dvou atomů p_0 a p_1 pouze s užitím spojek $\&$, $\vee$ a $\to$ definuje booleovskou funkci, která má v bodě $[1,1]$ hodnotu 1. O formulích např. $\neg p_0 \vee \neg p_1$ nebo $p_0 \,\&\, \neg p_0$ to ale pravda není, a žádná z nich tedy není ekvivalentní s formulí sestavenou z p_0 a p_1 jen užitím spojek $\&$, $\vee$ a $\to$.

11. Uvažujte smyšlenou logickou spojku $\downarrow$, jejíž pravdivostní tabulka vznikne záměnou nul a jedniček v pravdivostní tabulce disjunkce:

$\downarrow$	1	0
1	0	0
0	0	1

    Tato spojka se někdy nazývá *Pierceovou šipkou* a lze ji číst „ani-ani“: $A \downarrow B$ je ekvivalentní s $\neg A \,\&\, \neg B$. Dokažte, že každá výroková formule je ekvivalentní s formulí neobsahující jinou logickou spojku než $\downarrow$.

12. Nechť φ je libovolná výroková formule. Označme $\varphi_q(\top)$ resp. $\varphi_q(\bot)$ formuli, která z ní vznikne nahrazením všech výskytů atomu q logickou konstantou $\top$ resp. $\bot$. Dokažte, že $\varphi \to \varphi_q(\top) \vee \varphi_q(\bot)$ je tautologie.

13. Dokažte, že pro klasickou výrokovou logiku platí *věta o interpolaci*, kterou lze nejsnáze formulovat pro případ, kdy se připouštějí logické konstanty $\top$ a $\bot$: jsou-li φ a ψ dvě výrokové formule takové, že $\varphi \to \psi$ je tautologie, pak existuje výroková formule ω (zvaná *interpolant* formulí φ a ψ) splňující podmínky:

    - ω obsahuje pouze atomy vyskytující se zároveň v obou formulích φ a ψ (plus případně konstanty $\top$ a $\bot$),
    - obě formule $\varphi \to \omega$ i $\omega \to \psi$ jsou tautologie.

    Návod. Nechť $q_1, \ldots, q_n$ jsou všechny atomy, které se vyskytují ve φ a nevyskytují se v ψ. Vezměte za ω disjunkci všech 2^n formulí, které vzniknou z φ dosazením konstant $\top$ a $\bot$ za atomy $q_1, \ldots, q_n$. Fakt, že $\varphi \to \omega$ je tautologie, odvoďte z předchozího cvičení. Dále si všimněte, že je-li α kterýkoliv z 2^n disjunktů formule ω, pak formuli $\alpha \to \psi$ lze získat z formule $\varphi \to \psi$ opakovaným užitím cvičení 3(b).

1.2 Věta o kompaktnosti

Předpokládejme, že T je množina, jejímiž prvky jsou uzavřené podmnožiny intervalu $[\![0,1]\!]$ chápaného jako podmnožina množiny R všech reálných čísel. Má-li každých konečně mnoho prvků množiny T neprázdný průnik, tj. platí-li $\bigcap F \neq \emptyset$ pro každou konečnou množinu $F \subseteq T$, pak existuje alespoň jedno reálné číslo, které je současně prvkem všech prvků množiny T, tj. platí $\bigcap T \neq \emptyset$.

Právě uvedené tvrzení se v topologii nazývá princip kompaktnosti, reálný interval $[\![0,1]\!]$ je z topologického hlediska kompaktní množinou. Nahradíme-li v principu kompaktnosti termíny podle následující tabulky:

uzavřená podmnožina intervalu $[\![0,1]\!]$	výroková formule
množina uzavřených množin	množina výrokových formulí
průnik množiny je neprázdný	množina je splnitelná,

dostaneme rovněž pravdivé tvrzení, které se nazývá větou o kompaktnosti ve výrokové logice. Uvádíme dvě (ekvivalentní) verze.

Věta 1.2.1 (o kompaktnosti ve výrokové logice) *(a) Je-li T množina výrokových formulí taková, že každá konečná množina $F \subseteq T$ je splnitelná, pak T je splnitelná.*
(b) Je-li T množina výrokových formulí a φ je výroková formule taková, že $T \models \varphi$, pak existuje konečná množina $F \subseteq T$ taková, že $F \models \varphi$.

Podmínka $T \models \varphi$ podle definice znamená, že množina $T \cup \{\neg\varphi\}$ není splnitelná. V tom případě a platí-li tvrzení (a), existuje konečná množina $F \subseteq T \cup \{\neg\varphi\}$ výrokových formulí, která není splnitelná. Ať už formule $\neg\varphi$ je nebo není v F, také $(F - \{\neg\varphi\}) \cup \{\neg\varphi\}$ je nesplnitelná množina. To opět podle definice důsledku znamená $F - \{\neg\varphi\} \models \varphi$. Množina $F - \{\neg\varphi\}$ je ovšem konečnou podmnožinou množiny T. Dokázali jsme, že (b) plyne z (a), a zbývá tedy dokázat (a).

Uvedeme dva různé důkazy bodu (a). K prvnímu z nich použijeme dočasný pomocný pojem konečně splnitelné množiny a pomocné tvrzení o tomto pojmu.

Řekneme, že množina S výrokových formulí je *konečně splnitelná*, jestliže každá konečná $F \subseteq S$ je splnitelná. Věta o kompaktnosti říká, že množina S je konečně splnitelná, právě když je splnitelná. Před dokončením důkazu věty o kompaktnosti se na tento fakt nespoléhejme. Po něm pojem konečné splnitelnosti ztratí smysl.

Lemma 1.2.2 *Nechť S je množina výrokových formulí a φ je výroková formule. Je-li S konečně splnitelná, pak alespoň jedna z množin $S \cup \{\varphi\}$ a $S \cup \{\neg\varphi\}$ je konečně splnitelná.*

Důkaz Kdyby ne, pak existují konečné množiny $F_1, F_2 \subseteq S$ takové, že $F_1 \cup \{\varphi\}$ a $F_2 \cup \{\neg\varphi\}$ nejsou splnitelné. Snadno lze ověřit, že v tom případě ani $F_1 \cup F_2$ není splnitelná. QED

Důkaz věty o kompaktnosti Je-li množina At všech výrokových atomů konečná nebo spočetná, je množina všech výrokových formulí nekonečná spočetná a můžeme ji seřadit do posloupnosti. Nebudeme-li trvat na indexování přirozenými čísly a připustíme i čísla ordinální, můžeme ji seřadit do posloupnosti v každém případě. Předpokládejme tedy, že ε je limitní ordinální číslo a že $\{\,\psi_\alpha\,;\,\alpha<\varepsilon\,\}$ je posloupnost všech výrokových formulí. Dále předpokládejme, že T je množina výrokových formulí, jejíž každá konečná podmnožina je splnitelná, tedy že T je konečně splnitelná. Definujme posloupnost množin $\{\,S_\alpha\,;\,\alpha<\varepsilon\,\}$ a množinu S následující rekurzí:

$$\begin{aligned} S_0 &= T, \\ S_{\alpha+1} &= \begin{cases} S_\alpha \cup \{\psi_\alpha\} & \text{když } S_\alpha \cup \{\psi_\alpha\} \text{ je konečně splnitelná} \\ S_\alpha \cup \{\neg\psi_\alpha\} & \text{jinak,} \end{cases} \\ S_\lambda &= \bigcup_{\alpha<\lambda} S_\alpha, \qquad \text{když } \lambda<\varepsilon \text{ je limitní,} \\ S &= \bigcup_{\alpha<\varepsilon} S_\alpha. \end{aligned}$$

Pro $\alpha=0$ je množina S_α konečně splnitelná podle předpokladu věty. Když S_α je konečně splnitelná, pak je podle lemmatu i $S_{\alpha+1}$ konečně splnitelná. Když λ je limitní a všechny S_α pro $\alpha<\lambda$ jsou konečně splnitelné, pak i S_λ je konečně splnitelná, neboť libovolná konečná podmnožina množiny S_λ je podmnožinou už některé S_α pro $\alpha<\lambda$. Dokázali jsme indukcí, že každá množina S_α je konečně splnitelná. Úvahou stejnou jako v případě limitního indexu lze zdůvodnit, že i celá množina S je konečně splnitelná.

Postupně dokážeme, že S má ještě následující vlastnosti:

(i) $\varphi\in S$, právě když $\neg\varphi\notin S$,

(ii) $\varphi\to\psi\in S$, právě když $\varphi\notin S$ nebo $\psi\in S$,

(iii) $\varphi\vee\psi\in S$, právě když $\varphi\in S$ nebo $\psi\in S$,

(iv) $\varphi\,\&\,\psi\in S$, právě když $\varphi\in S$ a $\psi\in S$.

(i) Kdyby platilo $\varphi\in S$ a $\neg\varphi\in S$, pak $\{\varphi,\neg\varphi\}$ by byla nesplnitelnou konečnou podmnožinou množiny S a S by nebyla konečně splnitelná. $\varphi\notin S$ a $\neg\varphi\notin S$ současně také platit nemůže: φ má v enumeraci $\{\,\psi_\alpha\,;\,\alpha<\varepsilon\,\}$ nějaký index, $\varphi=\psi_\alpha$, a už v $S_{\alpha+1}$ (a tím spíše v S) je jedna z formulí φ, $\neg\varphi$. (ii) Nechť $\varphi\in S$, $\varphi\to\psi\in S$ a $\psi\notin S$. Pak podle (i) platí $\neg\psi\in S$. Ale $\{\varphi,\varphi\to\psi,\neg\psi\}$ je nesplnitelná konečná podmnožina množiny S. (iii) Když $\varphi\vee\psi\in S$, $\varphi\notin S$ a $\psi\notin S$, pak opět podle (i) platí $\neg\varphi\in S$ a $\neg\psi\in S$. Pak ale $\{\varphi\vee\psi,\neg\varphi,\neg\psi\}$ je nesplnitelnou konečnou podmnožinou množiny S. Všechny zbývající úvahy v (ii), (iii) a (iv) jsou podobné a přenecháváme je čtenáři.

Definujme nyní funkci v z množiny všech výrokových formulí do $\{0,1\}$ předpisem

$$v(\varphi)=1 \;\Leftrightarrow\; \varphi\in S.$$

Podmínky (i)–(iv) říkají, že funkce v je pravdivostním ohodnocením. Pro všechny formule $\varphi \in T$ platí $v(\varphi) = 1$, protože platí $T \subseteq S$. Množina T je tedy splnitelnou množinou výrokových formulí. QED

V kapitole o predikátové logice se setkáme s aplikací výrokové věty o kompaktnosti a také s její predikátovou verzí. V tomto oddílu ukážeme ještě školní příklad na užití věty o kompaktnosti v oblasti mimo logiku, totiž důkaz tvrzení, že každý nekonečný graf, který nelze obarvit n barvami, obsahuje konečný podgraf, který rovněž nelze obarvit n barvami. Pak ukážeme alternativní — topologický — důkaz věty o kompaktnosti, který bude velmi snadný pro čtenáře obeznámeného se základními topologickými pojmy. Nebudeme se ale spoléhat na předběžné znalosti a všechny potřebné definice uvedeme a uvedeme také důkaz (pro naše potřeby postačující verze) Tichonovovy věty, která tvrdí, že kartézský součin kompaktních topologických prostorů je opět kompaktní topologický prostor. Zbytek tohoto oddílu lze číst selektivně a čtenář, který se nezajímá o mimologické souvislosti věty o kompaktnosti, jej může zcela vypustit.

Dvojice $\langle G, R\rangle$ je *neorientovaný graf*, jestliže R je symetrická a antireflexivní relace na množině G, tj. jestliže R splňuje podmínky $\forall x \forall y (x\ R\ y \Rightarrow y\ R\ x)$ a $\forall x \neg (x\ R\ x)$. Graf $\langle G', R'\rangle$ je *podgraf* grafu $\langle G, R\rangle$, jestliže platí inkluze $G' \subseteq G$ a $R' \subseteq \{\, [x,y]\ ;\ x \in G'\ \&\ y \in G'\ \&\ x\ R\ y \,\}$. Funkce h z G do $\{1, \ldots, n\}$ je *obarvení grafu* $\langle G, R\rangle$ *n barvami*, platí-li $\forall x \forall y (x\ R\ y \Rightarrow h(x) \neq h(y))$. Čísla $1, \ldots, n$ reprezentují n barev. Obarvení je přidělení barev vrcholům grafu tak, aby vrcholům spojeným hranou nikdy nebyla přidělena táž barva.

Příklad 1.2.3 Uvažujme tvrzení *jestliže pro každý konečný podgraf grafu $\langle G, R\rangle$ existuje jeho obarvení n barvami, pak i pro celý graf $\langle G, R\rangle$ existuje jeho obarvení n barvami.* Toto tvrzení dokážeme převedením na větu o kompaktnosti. Nechť graf $\langle G, R\rangle$ je dán. Můžeme si zvolit množinu T výrokových formulí a dokonce i množinu At výrokových atomů. Zvolme ji takto:

$$\mathrm{At} = \{\, p_{x,i}\ ;\ x \in G\ \&\ 1 \leq i \leq n \,\}.$$

Každá dvojice $[x, i]$, kde x je vrchol grafu a i je barva, má v množině At atom $p_{x,i}$, který reprezentuje tvrzení vrcholu x byla přidělena barva i. Za množinu T zvolme sjednocení následujících tří množin výrokových formulí:

$$\begin{aligned}
&\{\, p_{x,1} \vee \ldots \vee p_{x,n}\ ;\ x \in G \,\} && ;\ \text{Každý vrchol má nějakou barvu,}\\
&\{\, p_{x,i} \rightarrow \neg p_{x,j}\ ;\ i \neq j \,\} && ;\ \text{ale jen jednu,}\\
&\{\, p_{x,i} \rightarrow \neg p_{y,i}\ ;\ x\ R\ y \,\} && ;\ \text{sousední vrcholy mají různé barvy.}
\end{aligned}$$

Nechť v je libovolné pravdivostní ohodnocení splňující všechny formule množiny T. Z ohodnocení v můžeme sestrojit funkci h takto: $h(x)$ definujeme jako ono i, pro které platí $v(p_{x,i}) = 1$. Je zřejmé, že číslo i je jednoznačně určeno a že h je obarvení grafu $\langle G, R\rangle$. Zdůvodnili jsme, že je-li T splnitelná, pak graf $\langle G, R\rangle$ lze obarvit n barvami. Podobně lze zdůvodnit, že existuje-li pro libovolný konečný

podgraf grafu $\langle G, R\rangle$ obarvení n barvami, pak každá konečná část F množiny T je splnitelná. Naše tvrzení tedy bezprostředně vyplývá z věty o kompaktnosti.

Nyní směřujme ke stručnému výčtu nejzákladnějších topologických pojmů a k topologickému důkazu věty o kompaktnosti. Označme $\mathcal{P}(A)$ množinu všech podmnožin množiny A, tj. potenční množinu množiny A. Nadále předpokládejme, že A je vždy neprázdná. Množina $\mathcal{T} \subseteq \mathcal{P}(A)$ je *topologie* na A, jestliže $\emptyset \in \mathcal{T}$, $A \in \mathcal{T}$ a $\mathcal{T}$ je uzavřena na konečné průniky a na libovolná sjednocení. Je-li $\mathcal{T}$ topologie na A, pak dvojice $\langle A, \mathcal{T}\rangle$ je *topologický prostor* a prvkům topologie $\mathcal{T}$ říkáme *otevřené množiny* prostoru $\langle A, \mathcal{T}\rangle$. Množina $X \subseteq A$ je *uzavřená*, platí-li $A - X \in \mathcal{T}$, tj. je-li její komplement otevřenou množinou.

Příklad 1.2.4 Množiny $\{\emptyset, A\}$ a $\mathcal{P}(A)$ jsou krajní příklady topologií na množině A. Druhé z nich říkáme *diskrétní topologie*. Každá z množin $\emptyset$ a A je jak otevřenou, tak uzavřenou množinou libovolného prostoru $\langle A, \mathcal{T}\rangle$.

Příklad 1.2.5 Nechť $\langle A, \leq\rangle$ je (ne nutně lineárně) uspořádaná množina, tj. $\leq$ je reflexivní, tranzitivní a slabě antisymetrická relace na množině A. Prohlašme množinu $X \subseteq A$ za otevřenou, jestliže pro každé $a \in X$ platí $\{\, y \,;\, a \leq y \,\} \subseteq X$. Snadno lze ověřit, že takto definovaná množina všech otevřených množin je uzavřená na libovolná sjednocení a také na libovolné — nejen konečné — průniky, a je to tedy topologie.

Příklad 1.2.6 Nechť P je neprázdná množina. Označme 2^P množinu všech funkcí z P do dvouprvkové množiny $\{0, 1\}$:

$$2^P = \{\, f \,;\, f : P \to \{0,1\} \,\}.$$

Prohlašme množinu $X \subseteq 2^P$ za otevřenou, jestliže pro každou funkci $g \in X$ existují prvky $x_1, .., x_n \in P$ takové, že $\{\, f \,;\, f(x_1) = g(x_1)\ \&\ ..\ \&\ f(x_n) = g(x_n) \,\} \subseteq X$. Množina X je tedy otevřená, jestliže s každým prvkem g obsahuje všechny funkce, které se s funkcí g shodují na jisté konečné množině. Předpokládejme, že X a Y jsou dvě množiny funkcí otevřené v právě uvedeném smyslu. Nechť $g \in X \cap Y$. Protože $g \in X$, také všechny funkce, které se s funkcí g shodují na jisté konečné množině $\{x_1, .., x_n\}$, jsou v X. Protože $g \in Y$, také všechny funkce, které se s funkcí g shodují na jisté konečné množině $\{y_1, .., y_m\}$, jsou v Y. Pak ale všechny funkce, které se s funkcí g shodují na množině $\{x_1, .., x_n, y_1, .., y_m\}$, jsou jak v X, tak v Y. Tím je ověřeno, že průnik dvou otevřených množin je opět otevřená množina. Snadno lze ověřit, že libovolné sjednocení otevřených množin je opět otevřenou množinou. Právě definované množině otevřených množin se říká *produktová topologie* na množině 2^P. Topologický prostor $\langle 2^P, \mathcal{T}\rangle$, kde $\mathcal{T}$ je produktová topologie, značíme obvykle pouze 2^P a nazýváme *kartézskou mocninou prostoru* $\{0, 1\}$ *(vybaveného diskrétní topologií)*.

Řekneme, že topologický prostor je *kompaktní*, jestliže každá množina uzavřených množin, jejíž každá konečná část má neprázdný průnik, má neprázdný průnik. Řekneme, že množina $\mathcal{F} \subseteq \mathcal{P}(A)$ je *filtr* na množině A, jestliže

- $A \in \mathcal{F}, \quad \emptyset \notin \mathcal{F}$,
- $Y \in \mathcal{F}$, kdykoliv $X \subseteq Y$ a $X \in \mathcal{F}$,
- $\mathcal{F}$ je uzavřená na konečné průniky.

Množina $\mathcal{U} \subseteq \mathcal{P}(A)$ je *ultrafiltr* na A, jestliže $\mathcal{U}$ je filtr a jestliže navíc pro každou množinu $X \subseteq A$ platí, že jedna z množin X a $A - X$ je v $\mathcal{U}$. Je známo, že důsledkem axiomu výběru je tvrzení, že každý filtr je obsažen v nějakém ultrafiltru.

Příklad 1.2.7 Je-li A nekonečná, pak množina všech jejích podmnožin, jejichž komplement je konečný, je filtr. Je-li A libovolná, pak množina všech jejích podmnožin, které obsahují nějaký pevně zvolený prvek $a \in A$ (tj. množina všech nadmnožin množiny $\{a\}$), je ultrafiltr. Nazýváme jej *triviálním ultrafiltrem*. Každý konečný prostor je kompaktní. Vezměme za $\langle A, \leq \rangle$ množinu všech reálných čísel s obvyklým uspořádáním. Každý interval tvaru $(-\infty, a)$ je uzavřenou množinou v topologii z příkladu 1.2.5. Průnik všech takovýchto intervalů je prázdný, ale průnik libovolných konečně mnoha je neprázdný. Topologický prostor definovaný v příkladu 1.2.5 tedy v případě, kdy $\langle A, \leq \rangle$ je množina všech reálných čísel, není kompaktní.

Příklad 1.2.8 Rozmysleme si, že každá kartézská mocnina tvaru 2^P je kompaktním topologickým prostorem. Nechť $\mathcal{C}$ je nějaká množina uzavřených množin prostoru 2^P. Každý prvek množiny $\mathcal{C}$ je tedy uzavřená množina (funkcí z P do $\{0,1\}$). Předpokládejme, že každá konečná část množiny $\mathcal{C}$ má neprázdný průnik. Ověříme, že i $\bigcap \mathcal{C} \neq \emptyset$. Označme $\mathcal{F}$ množinu všech nadmnožin všech konečných průniků množin z $\mathcal{C}$. Je zřejmé, že $\mathcal{F}$ je filtr. Označme $\mathcal{U}$ (některý) ultrafiltr obsahující $\mathcal{F}$. Platí $\mathcal{C} \subseteq \mathcal{U}$.

Definujme pomocí ultrafiltru $\mathcal{U}$ funkci $g_0 : P \to \{0,1\}$ předpisem

$$g_0(x) = 1 \Leftrightarrow \{\, f \in 2^P \,;\, f(x) = 1 \,\} \in \mathcal{U}.$$

Množiny $\{\, f \in 2^P ; f(x) = 1 \}$ a $\{\, f \in 2^P ; f(x) = 0 \}$ jsou navzájem komplementární, a tedy není-li první z nich v $\mathcal{U}$, tj. platí-li $g_0(x) = 0$, musí (podle definice ultrafiltru) být v $\mathcal{U}$ druhá z nich. Tedy $\{\, f \in 2^P \,;\, f(x) = g_0(x) \,\}$ je v $\mathcal{U}$ pro každé $x \in P$. Vzhledem k uzavřenosti ultrafiltru $\mathcal{U}$ na konečné průniky platí také

$$\{\, f \in 2^P \,;\, f(x_1) = g_0(x_1) \;\&\; \ldots \;\&\; f(x_n) = g_0(x_n) \,\} \in \mathcal{U}$$

pro libovolnou konečnou množinu $\{x_1, \ldots, x_n\} \subseteq P$. Dokázali jsme, že každá otevřená množina prostoru 2^P, jejímž prvkem je funkce g_0, je v $\mathcal{U}$.

Nechť nyní $X \in \mathcal{C}$ je libovolná. Víme $X \in \mathcal{U}$. Když $g_0 \notin X$, pak $2^P - X$ je otevřená množina obsahující g_0, a tedy podle předchozího $2^P - X \in \mathcal{U}$. To ale není možné vzhledem k podmínkám v definici ultrafiltru: žádný filtr neobsahuje navzájem disjunktní množiny. Dokázali jsme $g_0 \in X$. Toto platí pro každou $X \in \mathcal{C}$. Tedy $g_0 \in \bigcap \mathcal{C}$, takže $\bigcap \mathcal{C} \neq \emptyset$.

Topologický důkaz věty o kompaktnosti Každá funkce z množiny At všech výrokových atomů do $\{0,1\}$ má jednoznačně určené rozšíření definované na množině všech výrokových formulí. To znamená, že pro účely tohoto důkazu můžeme pravdivostní ohodnocení ztotožnit s prvky prostoru 2^{At}.

Pro libovolnou formuli φ označme $\mathrm{Mod}(\varphi) = \{\, f \in 2^{\mathrm{At}} \,;\, f(\varphi) = 1 \,\}$. $\mathrm{Mod}(\varphi)$ je množina všech pravdivostních ohodnocení, která splňují formuli φ, přesněji řečeno množina všech funkcí z At do $\{0,1\}$, jejichž jednoznačně určené rozšíření na všechny výrokové formule splňuje formuli φ.

Nechť φ je libovolná výroková formule a nechť $p_1, .., p_k$ jsou všechny atomy, které se v ní vyskytují. Je-li $f \in \mathrm{Mod}(\varphi)$, tj. je-li φ splněna ohodnocením f, pak φ je také splněna každým ohodnocením g, které se s f shoduje na množině $\{p_1, .., p_k\}$. Tím je ověřeno, že každá množina tvaru $\mathrm{Mod}(\varphi)$ je otevřenou množinou prostoru 2^{At}. Každá množina tvaru $\mathrm{Mod}(\varphi)$ je však zároveň také uzavřenou množinou prostoru 2^{At}, protože je komplementem otevřené množiny $\mathrm{Mod}(\neg\varphi)$.

Předpokládejme, že T je nějaká množina výrokových formulí, jejíž každá konečná podmnožina je splnitelná. To znamená, že každá množina tvaru

$$\mathrm{Mod}(\varphi_1) \cap \, .. \, \cap \mathrm{Mod}(\varphi_n)$$

je neprázdná, pokud $\{\varphi_1, .., \varphi_n\} \subseteq T$. Splnitelnost celé množiny T znamená $\bigcap\{\, \mathrm{Mod}(\varphi) \,;\, \varphi \in T \,\} \neq \emptyset$ a plyne bezprostředně z kompaktnosti prostoru 2^{At} a uzavřenosti množin $\mathrm{Mod}(\varphi_i)$. QED

V prvním důkazu věty o kompaktnosti jsme použili předpoklad, že množinu všech výrokových formulí lze dobře uspořádat. Použili jsme tedy axiom výběru AC. V druhém, topologickém, důkazu jsme použili předpoklad

UF: Každý filtr na $\mathcal{P}(A)$, kde $A \neq \emptyset$, je obsažen v nějakém ultrafiltru,

který lze také považovat za axiom teorie množin. Bez důkazu jsme ponechali implikaci $\mathrm{AC} \to \mathrm{UF}$, ale důkaz vlastně plyne z cvičení 8. V případě, kdy množina At všech výrokových atomů je nekonečná spočetná, lze větu o kompaktnosti dokázat v teorii množin bez dodatečných axiomů.

Cvičení

1. Nechť T je množina výrokových formulí taková, že každé pravdivostní ohodnocení splňuje některou formuli v T. Pak existuje konečná množina formulí $\{\varphi_1, .., \varphi_n\} \subseteq T$ taková, že $\varphi_1 \vee \, .. \, \vee \varphi_n$ je tautologie. Dokažte.

2. Nechť $\langle A, \leq \rangle$ je lineárně uspořádaná množina, tj. $\leq$ je uspořádání na množině A, které navíc splňuje podmínku $\forall a \forall b (a \leq b \;\vee\; b \leq a)$. Nechť $(\!(c,d)\!)$ označuje množinu $\{\, a \,;\, c < a < d \,\}$, dále $(\!(c,+\infty)\!)$ označuje množinu $\{\, a \,;\, c < a \,\}$ a $(\!(-\infty,c)\!)$ označuje množinu $\{\; a \;;\; a < c \;\}$. Množinám tvaru $(\!(c,d)\!)$, $(\!(c,+\infty)\!)$ a $(\!(-\infty,c)\!)$ říkejme *otevřené intervaly*. Označme $\mathcal{T}$ množinu všech $X \subseteq A$

splňujících podmínku, že pro každé $a \in X$ existuje otevřený interval $I \subseteq X$ takový, že $a \in I$. Dokažte, že $\mathcal{T}$ je topologie. $\mathcal{T}$ se nazývá *intervalovou topologií* na uspořádané množině $\langle A, \leq \rangle$.

3. Dokažte, že množina všech reálných čísel s intervalovou topologií ani množina všech racionálních čísel z intervalu $[\![0, 1]\!]$ s intervalovou topologií nejsou kompaktní prostory.

4. Dokažte, že je-li $\mathcal{F} \subseteq \mathcal{P}(A)$ filtr a $X \subseteq A$ libovolná, pak existuje filtr, který obsahuje množinu $\mathcal{F} \cup \{X\}$ nebo množinu $\mathcal{F} \cup \{A - X\}$.

5. Ultrafiltr $\mathcal{U}$ na A je triviální, právě když $\mathcal{U}$ obsahuje nějakou konečnou množinu. Dokažte.

6. Nechť A je nekonečná množina. Množina všech částí množiny A, které mají konečný doplněk, se nazývá *Frechetův filtr* na množině A. Dokažte, že žádný ultrafiltr obsahující Frechetův filtr není triviální.

7. Znamená-li Mod totéž, co v topologickém důkazu věty o kompaktnosti, jaké vztahy platí mezi množinami $\mathrm{Mod}(\varphi \,\&\, \psi)$, $\mathrm{Mod}(\varphi \vee \psi)$, $\mathrm{Mod}(\varphi)$ a $\mathrm{Mod}(\psi)$?

8. Užijte větu o kompaktnosti pro výrokovou logiku k důkazu tvrzení, že každý filtr na libovolné množině A je obsažen v některém ultrafiltru.

   Návod. Nechť je dán filtr $\mathcal{F}$ na množině A. Zvolte množinu výrokových atomů tak, aby obsahovala atom p_X pro každou $X \subseteq A$. Atom p_X chápejte jako tvrzení množina X je prvek ultrafiltru $\mathcal{U}$, kde $\mathcal{U}$ je hledaný ultrafiltr. Definujte množinu formulí T vyjadřující fakt, že $\mathcal{U}$ je ultrafiltr obsahující filtr $\mathcal{F}$. Množina T bude mimo jiné obsahovat formuli $\neg p_X \to p_{A-X}$ pro každou $X \subseteq A$.

9. Zdůvodněte, že tvrzení

   (i) obecná věta o kompaktnosti ve výrokové logice,

   (ii) každý filtr na libovolné množině A je obsažen v některém ultrafiltru,

   (iii) každý topologický prostor tvaru 2^P je kompaktní

   jsou v teorii množin bez axiomu výběru navzájem ekvivalentní.

1.3 Hilbertovský výrokový kalkulus

V úvodním oddílu této kapitoly jsme logicky platné výrokové formule, tj. tautologie, definovali pomocí *sémantického* pojmu pravdivostního ohodnocení. Z definice tautologie jsme odvodili algoritmus zvaný tabulková metoda, který rozhoduje o tom, zda daná formule je tautologií. Viděli jsme také, že tabulková metoda není příliš efektivním algoritmem; počet pravdivostních ohodnocení, která je nutno vzít v úvahu při zpracování nějaké formule φ, roste exponenciálně s počtem atomů ve φ.

V tomto oddílu uvidíme, že tautologie lze definovat také *syntakticky*, totiž jako formule, které lze odvodit mechanickou aplikací jistých strukturálních pravidel. Jinými slovy, tautologie jsou přesně ty formule, které lze *formálně dokázat* pomocí pravidel jistého důkazového systému neboli kalkulu. Místo strukturální pravidla budeme říkat *odvozovací pravidla*; slovy „strukturální“ a „mechanická“ jsme chtěli zdůraznit, že odvozovací pravidla jsou aplikovatelná na libovolné formule předepsaného tvaru bez ohledu na jejich pravdivostní hodnoty či smysl.

Odvozovací pravidlo může vypadat například takto:

X1: $\quad \psi \to \varphi\,,\ \neg\psi \to \varphi \ /\ \varphi.$

Toto pravidlo umožňuje prohlásit za odvozenou (formálně dokázanou) formuli φ, kdykoliv se nám pro libovolnou formuli ψ podařilo (nezávisle na sobě) dokázat formule $\psi \to \varphi$ a $\neg\psi \to \varphi$. Pravidlo X1 je pravidlo se dvěma předpoklady a je aplikovatelné teprve poté, kdy byly odvozeny alespoň dvě formule. Jiná pravidla mohou mít jiný počet předpokladů. Je ale zřejmé, že abychom vůbec mohli odvodit nějakou formuli, jsou nutná také nějaká pravidla s nulovým počtem předpokladů. Těm říkáme *výrokové axiomy* a mohou být zvoleny například takto:

X2: $\quad / \ \varphi \to (\varphi \vee \psi),$

X3: $\quad / \ \varphi \to (\psi \vee \varphi).$

Snadno lze ověřit, že pravidlo X1 je *korektní* v tom smyslu, že z tautologií umožňuje odvodit opět pouze tautologie. Pravidla X2 a X3 jsou aplikovatelná kdykoliv, a rovněž umožňují odvodit pouze tautologie; jsou to tedy také korektní pravidla. Víme-li už, že všechna pravidla X1–X3 jsou korektní, můžeme ve třech krocích

1:	$\varphi \to (\varphi \vee \neg\varphi)$	; X2
2:	$\neg\varphi \to (\varphi \vee \neg\varphi)$	; X3
3:	$\varphi \vee \neg\varphi$	; X1 na 1, 2

dokázat, že každá formule tvaru $\varphi \vee \neg\varphi$ je tautologie. To jsme samozřejmě věděli; důležité ale je, že nyní jsme to dokázali bez probírání pravdivostních hodnot. Úvahu o pravdivostních hodnotách jsme totiž učinili *a priori* při zdůvodnění korektnosti pravidel X1–X3.

Kalkulus tedy chápeme jako množinu odvozovacích pravidel. Kalkulus je *korektní* vůči sémantice klasické výrokové logiky, jestliže každá formule v něm dokazatelná je tautologie. A kalkulus je *úplný*, jestliže je korektní a navíc všechny tautologie jsou v něm dokazatelné. Časem se budeme zabývat i jinými logikami, než je klasická výroková logika. V obecném případě kalkulus je korektní, jestliže neumožňuje dokázat žádnou formuli, která vzhledem k nějaké sémantice nemá být dokazatelná, a je úplný, jestliže navíc umožňuje dokázat každou formuli, která vzhledem k oné sémantice má být dokazatelná. Kalkulus s pravidly X1–X3 je korektní,

není ale úplný vůči sémantice klasické výrokové logiky. Za chvíli uvedeme kalkulus HK převzatý z Kleeneho knihy [49], o kterém dokážeme, že úplný je. Označení X1–X3 bylo jen dočasné. Pravidla X2 a X3 budou v kalkulu HK vystupovat pod jiným názvem a pravidlo X1 už používat nebudeme.

Definice 1.3.1 *Posloupnost formulí $\varphi_1, \ldots, \varphi_n$ je* důkaz (v hilbertovském kalkulu) z množiny předpokladů T*, jestliže každá formule φ_i je v T nebo je výrokovým axiomem nebo je odvozena z některých formulí φ_j pro $j < i$ pomocí některého odvozovacího pravidla. Formule φ je* dokazatelná *z množiny T (nebo též* dokazatelná v T*), jestliže existuje důkaz z množiny T takový, že φ je jeho posledním členem.* Kalkulus HK *(hilbertovský klasický) má jediné odvozovací pravidlo* modus ponens

MP: $\varphi\,,\ \varphi \to \psi\ \ /\ \ \psi$

a následující výrokové axiomy

A1: $\varphi \to (\psi \to \varphi)$,

A2: $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$,

A3: $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$,

A4: $\varphi \,\&\, \psi \to \varphi, \qquad \varphi \,\&\, \psi \to \psi$,

A5: $\varphi \to (\psi \to \varphi \,\&\, \psi)$,

A6: $\varphi \to \varphi \vee \psi, \qquad \psi \to \varphi \vee \psi$,

A7: $(\varphi \to \chi) \to ((\psi \to \chi) \to (\varphi \vee \psi \to \chi))$.

Fakt, že φ je dokazatelná z T, zapisujeme $T \vdash_{\mathrm{HK}} \varphi$ nebo jen $T \vdash \varphi$. Je-li $T = \emptyset$, píšeme jen $\vdash_{\mathrm{HK}} \varphi$ nebo $\vdash \varphi$.

Přestože jsme nezapomněli, že výrokový axiom je vlastně pravidlo s nulovým počtem předpokladů, v definici jsme poněkud nedůsledně oddělili axiomy od pravidla MP a v souvislosti s tím jsme v jejich zápisu také vynechali lomítka.

Kalkulus HK je jen jeden z celé řady kalkulů pro klasickou výrokovou logiku. V literatuře se vyskytují kalkuly s jiným seznamem axiomů a jsou myslitelné i kalkuly s jiným seznamem odvozovacích pravidel. Výrokovým kalkulům založeným na pravidle MP se také často říká *fregovské*.

Slovo důkaz tedy užíváme na dvou úrovních: (formální) důkaz jako odborný termín (posloupnost formulí taková a taková) a důkaz (metamatematický) nějakého tvrzení (o formulích, formálních důkazech, ...).

Zdůrazněme ještě, že A1–A7 nejsou jednotlivé axiomy, ale *schémata*; za φ, ψ a χ mohou být voleny libovolné formule. Každou formuli, kterou získáme volbou konkrétních formulí v nějakém schématu, nazýváme *instancí* onoho schématu.

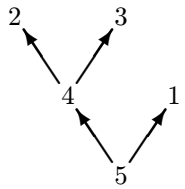
Příklad 1.3.2 Zvolíme-li libovolně formuli φ, pak následující posloupnost pěti formulí

1: $\varphi \to (\varphi \to \varphi)$; A1

2:	$(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$	; A2
3:	$\varphi \to ((\varphi \to \varphi) \to \varphi)$	; A1
4:	$(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$	; MP na 2, 3
5:	$\varphi \to \varphi$	; MP na 4, 1

je důkazem formule $\varphi \to \varphi$ z prázdné množiny předpokladů. Každá formule tvaru $\varphi \to \varphi$ je tedy v kalkulu HK dokazatelná.

Posloupnost $\varphi_1, \ldots, \varphi_n$, která je důkazem, nemusí být prostou posloupností; definice 1.3.1 připouští, že některé formule φ_i se v posloupnosti $\varphi_1, \ldots, \varphi_n$ vyskytují vícekrát. Někdy se důkaz definuje nikoliv jako posloupnost, ale jako (vrcholově) ohodnocený strom, přesněji konečný orientovaný strom, jehož vrcholům jsou přiřazeny formule tak, že formuli přiřazenou libovolnému vrcholu v lze jedním užitím odvozovacího pravidla odvodit z formulí přiřazených těm vrcholům, do kterých z vrcholu v vede hrana (definice některých pojmů z teorie grafů jsou na str. 118 a n.). I ve stromovém důkazu se ovšem táž formule může opakovat, tj. různé vrcholy mohou být ohodnoceny toutéž formulí. Zachováme-li označení formulí čísly 1 až 5, můžeme důkaz schématu $\varphi \to \varphi$ znázornit tak, jak je uvedeno na obrázku 1.3.1. K orientaci šipek na obr. 1.3.1 poznamenejme, že se snažíme držet úmluvu snad obvyklou, že cesty v orientovaných stromech vedou z kořenu směrem k listům. To v případě důkazů může vypadat neobvykle, čtenář si ale může myslet, že šipky nesledují „směr úvahy“, nýbrž ukazují na „důvody“. Mělo by být zřejmé, že pomocí stromových důkazů lze dokázat tytéž formule, které lze dokázat pomocí důkazů-posloupností.



Obrázek 1.3.1: Příklad důkazu v kalkulu HK

Důkaz schématu $\varphi \to \varphi$ je jediným případem, kdy jsme si dali práci a nějaký důkaz z prázdné množiny předpokladů jsme zapsali celý. Ve všech ostatních případech nám pomůže následující věta. Dokázat přímo dokazatelnost schématu $\varphi \to \varphi$ však bylo nutné, v důkazu věty 1.3.3 se na tento fakt budeme odvolávat.

Domluvme se, že při zapisování množin formulí budeme vypouštět složené závorky a symbol $\cup$ pro sjednocení. Zápis Γ, ψ tedy znamená $\Gamma \cup \{\psi\}$ a $\psi_1, \ldots, \psi_n \vdash \varphi$ znamená $\{\psi_1, \ldots, \psi_n\} \vdash \varphi$.

Věta 1.3.3 (o dedukci) *Nechť Γ je množina formulí a φ a ψ jsou formule takové, že $\Gamma, \psi \vdash \varphi$. Pak $\Gamma \vdash \psi \to \varphi$.*

Důkaz Podle definice důkazu existuje posloupnost $\varphi_1, \ldots, \varphi_n$ taková, že φ_n je φ a každá formule φ_i je výrokovým axiomem, nebo je odvozena z předchozích formulí pomocí pravidla MP, nebo je prvkem množiny předpokladů $\Gamma \cup \{\psi\}$. Dokážeme indukcí podle i, že každá implikace $\psi \to \varphi_i$ pro $1 \leq i \leq n$ je dokazatelná z předpokladů Γ. Nechť tedy pro všechna $j < i$ tvrzení platí a zabývejme se implikací $\psi \to \varphi_i$.

Když φ_i je ψ, pak $\psi \to \varphi_i$, tj. $\varphi_i \to \varphi_i$, je dokazatelná formule.

Když φ_i je některý výrokový axiom nebo prvek množiny Γ, pak tříčlenná posloupnost $\varphi_i \to (\psi \to \varphi_i)$, φ_i, $\psi \to \varphi_i$ je důkazem implikace $\psi \to \varphi_i$ z předpokladů Γ.

Nechť φ_i je odvozena pravidlem MP z formulí φ_j a φ_k, kde $j, k < i$. Jedna z formulí φ_j, φ_k musí být implikací takovou, že její premisa je druhá z obou formulí a závěr je φ_i. Nechť například φ_k je touto implikací a nechť $j < k$. Původní důkaz formule φ má tedy tvar

$$\ldots, \varphi_j, \ldots, \varphi_j \to \varphi_i, \ldots, \varphi_i, \ldots$$

Indukční předpoklad říká, že obě formule $\psi \to \varphi_j$ a $\psi \to (\varphi_j \to \varphi_i)$ jsou dokazatelné z množiny Γ. Zapišme oba důkazy za sebe a na konec připišme formule

$$(\psi \to (\varphi_j \to \varphi_i)) \to ((\psi \to \varphi_j) \to (\psi \to \varphi_i)), \quad (\psi \to \varphi_j) \to (\psi \to \varphi_i), \quad \psi \to \varphi_i.$$

Tím jsme získali důkaz formule $\psi \to \varphi_i$ z předpokladů Γ, neboť první z těchto tří formulí je instance schématu A2 a další dvě jsou odvozeny z předchozích členů pomocí pravidla MP. QED

Představme si nyní, že chceme zdůvodnit, že každá formule tvaru $\neg\neg\varphi \to \varphi$ je v kalkulu HK dokazatelná z prázdné množiny předpokladů. Věta o dedukci říká, že stačí zdůvodnit dokazatelnost formule φ z množiny předpokladů $\{\neg\neg\varphi\}$. Schéma A3 lze číst tak, že pokud $\neg\varphi$ vede ke sporu (tj. k závěru, že současně platí ψ i $\neg\psi$ pro některou formuli ψ), pak platí φ. A vede $\neg\varphi$ ke sporu? Ano, $\neg\varphi$ dává současně $\neg\varphi$ i $\neg\neg\varphi$, neboť jsme přijali předpoklad $\neg\neg\varphi$. Takováto hrubá úvaha a možná několik pokusů zpravidla umožňují sestrojit hledaný důkaz, v daném případě formule φ z množiny $\{\neg\neg\varphi\}$:

$$\vdots$$

1:	$\neg\varphi \to \neg\varphi$	
2:	$(\neg\varphi \to \neg\varphi) \to ((\neg\varphi \to \neg\neg\varphi) \to \varphi)$	; A3
3:	$\neg\neg\varphi \to (\neg\varphi \to \neg\neg\varphi)$	; A1
4:	$\neg\neg\varphi$	; Předpoklad
5:	$\neg\varphi \to \neg\neg\varphi$	; MP na 3, 4
6:	$(\neg\varphi \to \neg\neg\varphi) \to \varphi$	; MP na 1, 2
7:	φ	; MP na 5, 6.

Tečkami jsou znázorněny čtyři známé kroky důkazu formule $\neg\varphi \to \neg\varphi$. Abychom ukázali ještě jeden příklad na sestrojení formálního důkazu, zdůvodněme, že každá formule tvaru $\neg\psi \to (\psi \to \varphi)$ je v kalkulu HK dokazatelná. Užijeme-li větu o dedukci dvakrát, stačí zdůvodnit dokazatelnost formule φ z předpokladů $\{\psi, \neg\psi\}$. Opět lze užít schéma A3. Vede i tentokrát $\neg\varphi$ ke sporu? Ano, protože už předpoklady ψ a $\neg\psi$ tvoří dohromady spor. Tentokrát zapišme jen jakýsi „výtah“ z formálního důkazu, s vynecháním lehkých kroků (jako je například fakt, že když $\alpha \in \Gamma$ a $\Gamma \vdash \alpha \to \beta$, pak $\Gamma \vdash \beta$), zato s uvedením množiny předpokladů:

1:	$\neg\psi, \psi \vdash (\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$	; A3
2:	$\neg\psi, \psi \vdash \neg\psi \to (\neg\varphi \to \neg\psi)$	; A1
3:	$\neg\psi, \psi \vdash \psi \to (\neg\varphi \to \psi)$	; A1
4:	$\neg\psi, \psi \vdash \neg\varphi \to \neg\psi$	; 2, MP
5:	$\neg\psi, \psi \vdash \neg\varphi \to \psi$	; 3, MP
6:	$\neg\psi, \psi \vdash (\neg\varphi \to \psi) \to \varphi$	; MP na 1, 4
7:	$\neg\psi, \psi \vdash \varphi$	; MP na 5, 6
8:	$\neg\psi \quad \vdash \psi \to \varphi$	; Věta o dedukci
9:	$\vdash \neg\psi \to (\psi \to \varphi)$	; Věta o dedukci.

Lemma 1.3.4 *Následující schémata jsou dokazatelná v kalkulu HK:*

(a)	$\neg\psi \to (\psi \to \varphi)$,	*(g)*	$(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$,
(b)	$(\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi))$,	*(h)*	$(\psi \to \varphi) \to (\neg\varphi \to \neg\psi)$,
(c)	$\neg\neg\varphi \to \varphi$,	*(i)*	$\varphi \to (\neg\psi \to \neg(\varphi \to \psi))$,
(d)	$\neg\neg\neg\varphi \to \neg\varphi$,	*(j)*	$(\neg\varphi \to \varphi) \to \varphi$,
(e)	$\varphi \to \neg\neg\varphi$,	*(k)*	$(\varphi \to \neg\varphi) \to \neg\varphi$,
(f)	$(\psi \to \varphi) \to (\neg\neg\psi \to \neg\neg\varphi)$,	*(l)*	$(\psi \to \varphi) \to ((\neg\psi \to \varphi) \to \varphi)$.

Důkaz Body (a) a (c) jsme již dokázali, bod (b) je lehký, (d) je instance schématu (c). Domníváme se, že většinu zbývající práce lze ponechat na čtenáři, pro jistotu uvádíme několik rad a návodů.

Schémata jsou seřazena, někdy pomůže použít již dokázané předchozí body. Například bod (k) lze s užitím (c) a dosazením $\neg\varphi$ za φ v (j) dokázat takto:

$\varphi \to \neg\varphi, \neg\neg\varphi \vdash \varphi$	; (c)
$\varphi \to \neg\varphi, \neg\neg\varphi \vdash \neg\varphi$	; MP
$\varphi \to \neg\varphi \quad \vdash \neg\neg\varphi \to \neg\varphi$	; Věta o dedukci
$\varphi \to \neg\varphi \quad \vdash \neg\varphi$	; (j).

Víme-li už z (c) a (e), že dvojnou negaci lze podle potřeby přidat nebo odstranit, snadno dokážeme (f). Bod (h) lze dokázat z (f) a (g).

V (e) lze použít axiom A3 ve tvaru $(\neg\neg\neg\varphi\to\neg\varphi)\to((\neg\neg\neg\varphi\to\varphi)\to\neg\neg\varphi)$. Formule $\neg\neg\neg\varphi\to\neg\varphi$ je dokazatelná díky (d), formule $\neg\neg\neg\varphi\to\varphi$ je dokazatelná z předpokladu φ, takže $\neg\neg\varphi$ je dokazatelná rovněž z předpokladu φ.

Tvrzení (j) lze dokázat takto:

$$\begin{aligned}
&\vdash \neg\varphi\to(\neg\varphi\to\neg(\neg\varphi\to\varphi)) && \text{; (i)}\\
\neg\varphi &\vdash \neg(\neg\varphi\to\varphi) &&\\
&\vdash \neg\varphi\to\neg(\neg\varphi\to\varphi) && \text{; Věta o dedukci}\\
&\vdash (\neg\varphi\to\varphi)\to\varphi && \text{; (g)}
\end{aligned}$$

a konečně bod (l) lze dokázat užitím bodů (h), (b) a (j). QED

Množina předpokladů T je *sporná*, jestliže z ní lze dokázat nějakou formuli ψ i její negaci $\neg\psi$. Jinak je T *bezesporná* (*konzistentní*). Nechť T je sporná a nechť ψ je taková, že $T\vdash\psi$ a $T\vdash\neg\psi$. Podle (a) předchozího lemmatu platí $T\vdash\psi\to(\neg\psi\to\varphi)$, a tedy také $T\vdash\varphi$, a to pro libovolnou formuli φ. To znamená, že T je sporná, právě když *každá* formule je v T dokazatelná.

Je prázdná množina předpokladů bezesporná? Hned uvidíme, že ano, neboť věta o korektnosti kalkulu HK říká, že z prázdné množiny předpokladů jsou dokazatelné *pouze* tautologie, a neexistuje tautologie ψ taková, aby i $\neg\psi$ byla tautologie. Existuje algoritmus, který pro danou formuli φ rozhodne, zda φ je dokazatelná z prázdné množiny předpokladů? Ze samotné definice důkazu takový algoritmus asi odvodit nelze. Hned ale uvidíme, že odpověď je ano, neboť věta o úplnosti kalkulu HK říká, že z prázdné množiny předpokladů jsou dokazatelné *právě* tautologie, a víme, že pro rozpoznávání tautologií existuje algoritmus. Korektnost a úplnost se týká dokazatelnosti z prázdné množiny. Budeme uvažovat také *silnou korektnost* a *silnou úplnost*, které se týkají dokazatelnosti z libovolné množiny předpokladů.

Věta 1.3.5 (o úplnosti) *Formule φ je dokazatelná z prázdné množiny předpokladů, právě když φ je tautologie.*

Věta 1.3.6 (o silné úplnosti) *(a) Je-li T libovolná množina formulí, pak T je splnitelná, právě když T je bezesporná.*
(b) Je-li T množina formulí a φ libovolná formule, pak $T\vdash\varphi$, právě když $T\models\varphi$.

Implikaci $\Rightarrow$ ve větě o úplnosti se říká věta o korektnosti a implikacím $\Rightarrow$ ve větě o silné úplnosti se říká věta o silné korektnosti. Zdůrazněme, že právě věty o korektnosti jsou důležitým nástrojem, chceme-li dokázat, že nějaká formule *není* dokazatelná nebo že nějaká množina je bezesporná. Cvičení 11 ukazuje použití věty o korektnosti na kalkulus, o kterém nevíme, zda je úplný vůči dané sémantice.

Důkaz (všech tvrzení obou vět až na jedno) Začněme důkazem implikace $\Rightarrow$ v tvrzení (b) věty o silné úplnosti. Tím bude dokázána i implikace $\Rightarrow$ ve větě o úplnosti. Platí-li $T \vdash \varphi$, pak existuje důkaz $\varphi_1, \ldots, \varphi_n$ (kde φ_n je φ) formule φ z předpokladů T. Indukcí podle i dokážeme $T \models \varphi_i$. Když φ_i je výrokový axiom nebo prvek množiny T, pak vskutku $T \models \varphi_i$. Jinak je φ_i odvozena z předchozích členů φ_j a $\varphi_k = \varphi_j \to \varphi_i$ pravidlem MP. Indukční předpoklad říká $T \models \varphi_j$ a $T \models \varphi_j \to \varphi_i$. Zbývá ověřit, že pravidlo MP je *silně korektní* v tomto smyslu: když $T \models \varphi_j$ a $T \models \varphi_j \to \varphi_i$, pak $T \models \varphi_i$. To ponecháváme na čtenáři.

Zvolme nyní pevně atom p a uvažujme formuli $p \,\&\, \neg p$. Snadno lze ověřit, že $T \vdash p \,\&\, \neg p$, právě když T je sporná. Z definice důsledku plyne, že $T \models p \,\&\, \neg p$, právě když T není splnitelná. Tím jsme ověřili, že ve větě o silné úplnosti (a) vyplývá z (b).

Předpokládejme nyní, že $T \models \varphi$. Podle věty o kompaktnosti existuje konečná množina $F = \{\psi_1, \ldots, \psi_k\} \subseteq T$ taková, že $F \models \varphi$. Snadnou úvahou o pravdivostních ohodnoceních lze zjistit, že formule $\psi_1 \to (\psi_2 \to (\ldots \to (\psi_k \to \varphi)\ldots)$ je tautologie. Podle věty o úplnosti je tato formule dokazatelná z T (a z jakékoliv jiné množiny předpokladů také). Protože všechny ψ_i jsou v T, platí $T \vdash \varphi$. Použitím věty o kompaktnosti a věty o úplnosti jsme dokončili důkaz věty o silné úplnosti. Na později jsme odložili podstatný krok, totiž důkaz implikace $\Leftarrow$ ve větě o úplnosti. QED

Nechť φ je výroková formule a nechť v je pravdivostní ohodnocení. Definujme formuli φ^v jako φ v případě, kdy $v(\varphi) = 1$, a jako $\neg\varphi$ v případě, kdy $v(\varphi) = 0$. V obou případech tedy platí $v(\varphi^v) = 1$.

Lemma 1.3.7 *Nechť v je pravdivostní ohodnocení, $p_1, \ldots, p_m$ jsou výrokové atomy a φ je formule sestavená z $p_1, \ldots, p_m$ (ne všechny se skutečně musí ve φ vyskytovat). Pak φ^v je dokazatelná z množiny předpokladů $\{p_1^v, \ldots, p_m^v\}$.*

Důkaz Označme T množinu předpokladů $\{p_1^v, \ldots, p_m^v\}$ a postupujme indukcí podle složitosti formule φ. Je-li φ výrokový atom, pak φ^v je v T a platí $T \vdash \varphi^v$.

Nechť φ je tvaru $\neg\psi$ a nechť pro ψ tvrzení platí. Když $v(\psi) = 1$, pak ψ^v je ψ, dále φ^v je $\neg\neg\psi$ a z indukčního předpokladu $T \vdash \psi^v$ plyne $T \vdash \varphi^v$ díky tvrzení (e) lemmatu 1.3.4. Když $v(\psi) = 0$, pak $\varphi^v = (\neg\psi)^v = \neg\psi = \psi^v$ a není co dokazovat.

Nechť φ je tvaru $\psi \to \chi$ a nechť pro ψ i χ tvrzení platí. Když $v(\chi) = 1$, pak $\chi^v = \chi$ a $\varphi^v = \psi \to \chi$, a z indukčního předpokladu $T \vdash \chi^v$ plyne $T \vdash \varphi^v$ díky axiomu $\chi \to (\psi \to \chi)$. Když $v(\psi) = 0$, pak $\psi^v = \neg\psi$ a $\varphi^v = \psi \to \chi$, a z indukčního předpokladu $T \vdash \psi^v$ plyne $T \vdash \varphi^v$ díky bodu (a) lemmatu 1.3.4. Poslední možný případ je $v(\psi) = 1$ a zároveň $v(\chi) = 0$. Pak $\psi^v = \psi$, $\chi^v = \neg\chi$ a $\varphi^v = \neg(\psi \to \chi)$, a z indukčních předpokladů $T \vdash \psi^v$ a $T \vdash \chi^v$ plyne $T \vdash \varphi^v$ díky bodu (i) lemmatu 1.3.4.

Zbývající případy, kdy φ je konjunkcí nebo disjunkcí, přenecháváme čtenáři s tím, že je třeba také formulovat a dokázat příslušné rozšíření lemmatu 1.3.4. QED

Důkaz věty o úplnosti Nechť φ je libovolná tautologie. Chceme ověřit, že φ je dokazatelná v kalkulu HK. Nechť $p_1, \ldots, p_m$ jsou všechny výrokové atomy vyskytující se ve φ. Protože φ je tautologie, předchozí lemma říká, že

$$p_1^v, \ldots, p_m^v \vdash \varphi$$

pro každé pravdivostní ohodnocení v. Definujme pro $0 \leq k \leq m$ *elementární množinu (předpokladů) délky* k jako množinu obsahující k formulí, a to právě jednu z formulí p_i, $\neg p_i$ pro každý z atomů $p_1, \ldots, p_k$. Díky tomuto dočasnému pojmu nebudeme už muset mluvit o pravdivostních ohodnoceních. Existuje 2^k elementárních množin délky k. Uvažujme nyní tvrzení

$$\textit{Je-li } T \textit{ libovolná elementární množina délky } k\textit{, pak } T \vdash \varphi. \qquad (*_k)$$

Předchozí lemma říká, že pro $k = m$ tvrzení $(*_k)$ platí. Dokážeme (sestupnou) indukcí podle k, že $(*_k)$ platí pro každé k takové, že $0 \leq k \leq m$. Tvrzení $(*_0)$ je to, co jsme měli dokázat.

Nechť tedy $0 \leq k < m$ a T je libovolná elementární množina délky k. Indukční předpoklad říká, že platí $T, p_{k+1} \vdash \varphi$ i $T, \neg p_{k+1} \vdash \varphi$, neboť T, p_{k+1} a $T, \neg p_{k+1}$ jsou elementární množiny délky $k+1$. Věta o dedukci dává

$$T \vdash p_{k+1} \to \varphi \quad \text{a} \quad T \vdash \neg p_{k+1} \to \varphi.$$

Z toho plyne $T \vdash \varphi$ vzhledem k bodu (l) lemmatu 1.3.4. QED

Pokusme se shrnout, čeho jsme v tomto oddílu dosáhli a co se nepodařilo. Sestrojili jsme důkazový systém, který je silně úplný vzhledem k sémantice klasické výrokové logiky. Pozoruhodné je, že všechny tautologie lze odvodit užitím jen konečně mnoha logických principů vyjádřených axiomy a odvozovacími pravidly kalkulu HK. Další výhodou kalkulu HK je to, že přidáním několika pravidel a axiomů o kvantifikátorech z něj lze, jak později uvidíme, snadno získat kalkulus i pro predikátovou logiku.

K vysvětlení toho, co možná nedopadlo úplně podle očekávání, zaveďme několik pojmů. *Délku formule* φ značíme $|\varphi|$ a rozumíme jí souhrnný počet všech výskytů logických spojek a atomů ve φ. Například formule $(\neg p \to p) \to q$ má délku 6. *Délkou* $|d|$ *důkazu* d a *délkou* $|T|$ konečné *množiny* T rozumíme součet délek všech formulí v d resp. v T. Délky tedy měříme prvky množiny $\mathrm{N} = \{0, 1, 2, 3, \ldots\}$ všech přirozených čísel. O funkcích f a g z N do N řekneme, že f *neroste řádově rychleji než* g, stručně $f \in \mathcal{O}(g)$ nebo $f(n)$ *je* $\mathcal{O}(g(n))$, jestliže existují přirozená čísla c a n_0 taková, že $f(n) \leq c \cdot g(n)$ pro všechna $n \geq n_0$. Například funkce $6n^2 + 9$ je $\mathcal{O}(n^2)$, protože pro $n \geq 3$ platí $6n^2 + 9 \leq 7n^2$. Táž funkce je ovšem i $\mathcal{O}(n^3)$ atd. Řekneme-li, že každá tautologie délky n má důkaz délky $\mathcal{O}(g(n))$, pak to v souladu s touto definicí znamená, že existuje číslo c takové, že každá tautologie φ od určité délky výše má (alespoň jeden) důkaz, jehož délka je nejvýše $c \cdot g(|\varphi|)$.

Ve cvičeních vybízíme čtenáře k analýze našeho důkazu věty o úplnosti, kterou lze ověřit, že každá tautologie délky n má důkaz délky $\mathcal{O}(n^2 \cdot 2^n)$. Zajímavá a

dosud nevyřešená je otázka, zda funkci $n^2 \cdot 2^n$ lze nahradit některou funkcí rostoucí pomaleji než exponenciálně, například polynomem, tj. otázka

- *Má každá tautologie délky n důkaz v HK délky $p(n)$, kde p je vhodný polynom? Pokud ne, existuje kalkulus jiný než HK, pro který to platí?*

Tato otázka souvisí s důležitými otevřenými problémy ve výpočtové složitosti a krátce se k ní ještě vrátíme v příští kapitole. Odpověď ano by ve výpočtové složitosti měla silné a neočekávané důsledky, a je tudíž považována za nepravděpodobnou. To znamená, že za nedokázaných, ale celkem věrohodných předpokladů z výpočtové složitosti mají některé krátké tautologie jen velmi dlouhé důkazy, a platí to o jakémkoliv kalkulu. O některých kalkulech (jiných než HK) to dokonce již bylo dokázáno bez užití předpokladů z výpočtové složitosti. Nalezení formálního důkazu nějaké formule může v jednotlivých případech být rychlejší cestou k ověření, že je tautologií, než probírání všech pravdivostních ohodnocení, ale obecně, tj. pro všechny tautologie, to (asi) neplatí.

Kvantitativní analýza výsledků z logiky je oblast, která je živá a v poslední době se rychle rozvíjí. Studiu problematiky výrokových kalkulů a její souvislosti s výpočtovou složitostí je například věnována Krajíčkova kniha [50]. Zajímavé a přehledné pojednání o délkách důkazů (i v predikátové logice) je Pudlákova kapitola [69].

Cvičení

1. Zdůvodněte podrobně, že ve větě o dedukci platí i opačná implikace: když $T \vdash \psi \to \varphi$, pak $T, \psi \vdash \varphi$.

2. Dokončete důkaz lemmatu 1.3.4.

3. Množina $T, \neg\varphi$ je sporná, právě když $T \vdash \varphi$. Dokažte.

   Návod. Využijte bod (j) lemmatu 1.3.4.

4. Kromě schémat týkajících se implikace a negace, která jsou uvedena v lemmatu 1.3.4, jsou k dokončení důkazu věty o úplnosti užitečná ještě tři schémata týkající se disjunkce:

   $$\varphi \to (\varphi \vee \psi), \qquad \psi \to (\varphi \vee \psi), \qquad \neg\varphi \to (\neg\psi \to \neg(\varphi \vee \psi)).$$

   Zdůvodněte, že jsou dokazatelná v kalkulu HK. Formulujte ještě další tři potřebná schémata týkající se konjunkce a zdůvodněte i jejich dokazatelnost.

5. *Pravidlo substituce* $\varphi \,/\, \varphi_p(\chi)$ umožňuje z libovolné formule φ odvodit formuli, která z ní vznikne nahrazením všech výskytů některého atomu toutéž (libovolnou) formulí. Rozhodněte, zda pro kalkulus, který vznikne přidáním pravidla substituce ke kalkulu HK, platí věta o korektnosti a věta o silné korektnosti.

6. Zdůvodněte, že z věty o silné úplnosti plyne věta o kompaktnosti.

7. Zdůvodněte, že (b) ve větě o silné úplnosti plyne z (a).

   Návod. Využijte cvičení 3.

8. Označme HK* výrokový kalkulus, který vznikne z kalkulu HK nahrazením schématu A3 následujícím schématem A3*:

   A3*: $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$.

   Zdůvodněte, že pro kalkulus HK* platí věta o dedukci i věta o silné korektnosti.

9. Dokažte, že všechna schémata z lemmatu 1.3.4 jsou dokazatelná také v kalkulu HK*. Pro kalkulus HK* tedy platí věta o úplnosti, a tedy HK a HK* jsou ekvivalentní kalkuly.

   Návod. Postupujte jako v důkazu lemmatu 1.3.4. V (c) zdůvodněte, že místo $\vdash \neg\neg\varphi \to \varphi$ stačí dokázat $\neg\neg\varphi \vdash \neg\neg\varphi \to \varphi$. K tomu užijte A3* ve tvaru $(\neg\varphi \to \neg\neg\neg\varphi) \to (\neg\neg\varphi \to \varphi)$. V (l) dokažte

   $$\psi \to \varphi, \neg\psi \to \varphi \vdash \neg\varphi \to \varphi \qquad \text{; (h), (b),}$$

   a pak užijte (j).

10. Zdůvodněte, že každá formule neobsahující konjunkci a disjunkci je v kalkulu HK dokazatelná bez užití axiomů A4–A7.

11. Předpokládejte, že konjunkce a disjunkce se neuvažují a že implikace a negace nemají dvouhodnotové, ale následující tříhodnotové tabulky:

$\neg$	
2	0
1	0
0	2

$\to$	2	1	0
2	2	1	0
1	2	2	0
0	2	2	2

   Dokažte, že pravidlo MP je silně korektní vůči takto modifikované sémantice v tom smyslu, že z formulí, které při každém pravdivostním ohodnocení mají pravdivostní hodnotu 2, dovoluje odvodit opět pouze formuli, která při každém pravdivostním ohodnocení má hodnotu 2. Uvažujte výrokový logický systém s jediným pravidlem modus ponens a s následujícími schématy axiomů:

   $$\varphi \to (\psi \to \varphi),$$
   $$(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)),$$
   $$(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi),$$
   $$\varphi \to (\neg\varphi \to \psi).$$

   Formulujte a dokažte větu o silné korektnosti tohoto systému vůči uvedené tříhodnotové sémantice. Dokažte, že formule $(\neg p \to \neg q) \to ((\neg p \to q) \to p)$ a $\neg\neg p \to p$ nejsou v tomto systému dokazatelné.

12. Rozhodněte, které formule z lemmatu 1.3.4 jsou dokazatelné v kalkulu z cvičení 11.

    Návod. Tentokrát je asi výhodnější dokázat dřív (e) než (d) a dřív (h) než (f).

13. Zdůvodněte, že připustíme-li i konjunkci a disjunkci a přidáme-li ke kalkulu ze cvičení 11 schémata A4–A7, na nedokazatelnosti formule $\neg\neg p \to p$ a formule $(\neg p \to \neg q) \to ((\neg p \to q) \to p)$ se nic nezmění.

14. Nechť T a φ jsou takové, že $T \nvdash \varphi$. Vezměte limitní ordinální číslo ε a posloupnost $\{\psi_\alpha; \alpha < \varepsilon\}$ všech výrokových formulí a definujte posloupnost $\{S_\alpha; \alpha < \varepsilon\}$ množin výrokových formulí následující rekurzí:

$$\begin{aligned} S_0 &= T \cup \{\neg\varphi\}, \\ S_{\alpha+1} &= \begin{cases} S_\alpha \cup \{\psi_\alpha\} & \text{když } S_\alpha \cup \{\psi_\alpha\} \text{ je bezesporná} \\ S_\alpha \cup \{\neg\psi_\alpha\} & \text{jinak,} \end{cases} \\ S_\lambda &= \bigcup_{\alpha<\lambda} S_\alpha, \qquad \text{když } \lambda < \varepsilon \text{ je limitní,} \\ S &= \bigcup_{\alpha<\varepsilon} S_\alpha. \end{aligned}$$

    Dokažte, že každá množina S_α i celá S je bezesporná a že S má všechny vlastnosti (i)–(iv) z prvního důkazu věty o kompaktnosti. Dále podobně jako v onom důkazu definujte pravdivostní ohodnocení, které splňuje všechny formule množiny $T, \neg\varphi$. Tím jste dokončili přímý důkaz věty o silné úplnosti kalkulu HK.

15. Má-li libovolné ze schémat jmenovaných v lemmatu 1.3.4 délku n, pak má důkaz v HK délky $\mathcal{O}(n)$. Dokažte.

    Návod. Důkaz kterékoliv formule tvaru například $\neg\neg\varphi\to\varphi$ lze získat dosazením do jediného důkazu formule $\neg\neg p \to p$.

16. Má-li formule φ důkaz délky n z množiny T, ψ, pak formule $\psi \to \varphi$ má důkaz délky $\mathcal{O}(n) \cdot \mathcal{O}(|\psi|)$ z množiny T. Dokažte.

    Návod. Nechť $d = \varphi_1, \ldots, \varphi_r$, kde $\varphi_r = \varphi$, je důkaz formule φ z množiny T, ψ. Nechť $|d| \le n$. Musí platit $r \le n$. Můžeme předpokládat, že formule $\varphi_1, \ldots, \varphi_r$ jsou navzájem různé. Nechť d' je důkaz formule $\psi\to\varphi$ sestrojený v důkazu věty o dedukci. V místě, kde v důkazu d je formule φ_i odvozena z předchozích formulí pomocí pravidla MP, jsou v důkazu d' tři formule. Přeskupením symbolů v těchto třech formulích můžeme získat: formuli φ_i, šest výskytů formule ψ, tři výskyty formule $\varphi_j \to \varphi_i$ a sedm výskytů implikace. Protože v důkazu d se neopakují formule, můžeme říci, že každá formule φ_k důkazu d se v důkazu d' vyskytuje nejvýše sedmkrát, a to jednou nebo čtyřikrát (je-li výrokovým axiomem nebo prvkem množiny Γ) na původním místě, a pak ještě třikrát někde dále, je-li implikací $\varphi_j \to \varphi_i$ zmíněnou výše. V důkazu d' je dále nejvýše $6n$ výskytů formule ψ a nejvýše $7n$ nových implikací, jiné symboly v něm nejsou.

17. Dokažte, že je-li v pravdivostní ohodnocení a φ výroková formule sestavená z atomů $p_1, \ldots, p_m$, pak φ^v má důkaz z předpokladů $p_1^v, \ldots, p_m^v$ délky $\mathcal{O}(|\varphi|^2)$.

18. Dokažte, že je-li φ tautologie délky n, pak φ má důkaz délky $\mathcal{O}(n^2 \cdot 2^n)$.

    Návod. Uvažte, že formule délky n obsahuje nejvýše n různých atomů. J. Krajíček nás upozornil, že lze počítat o něco přesněji: tautologie délky n má nejvýše $(2n)/3$ atomů a funkce $n^2 \cdot 2^{(2n)/3}$ je v $\mathcal{O}(2^n)$.

19. Zdůvodněte, že ke každému důkazu-posloupnosti délky n existuje stromový důkaz téže formule, jehož délka je $\mathcal{O}(2^n)$.

1.4 Gentzenovský výrokový kalkulus

Věta o úplnosti pro hilbertovský kalkulus HK spolu s tabulkovou metodou zaručují existenci algoritmu, který pro každou výrokovou formuli rozhodne, je-li dokazatelná v kalkulu HK. Šlo by takový algoritmus odvodit přímo z definice důkazu, bez odvolání se na sémantiku? Možná, že o existenci důkazu dané formule v HK nebo v nějakém jiném kalkulu by šlo rozhodnout tak, že bychom se pokusili důkaz dané formule sestrojit od konce, tj. že bychom se pokusili zpětným užíváním pravidel kalkulu dospět od dané formule k axiomům. Pravidlo modus ponens kalkulu HK má bohužel pro tento účel nevýhodnou vlastnost, že dvojic ψ_1, ψ_2, z nichž lze jedním užitím pravidla MP odvodit danou formuli φ, je nekonečně mnoho.

Studium kalkulu GK, do kterého se nyní pustíme, vrhne určité světlo na otázku, jakou cenu je třeba zaplatit za kalkulus, jehož pravidla by neměla právě popsanou nevýhodnou vlastnost pravidla MP.

V kalkulu GK (gentzenovském klasickém) se na rozdíl od kalkulu HK nedokazují jednotlivé formule, ale sekventy. Někdy se proto mluví také o *sekventovém* kalkulu. *Sekvent* je definován jako dvojice konečných množin formulí. Sekvent sestávající z množin Γ a Δ zapisujeme $\langle\, \Gamma \Rightarrow \Delta \,\rangle$. Jeho zamýšlený význam je „platí-li všechny formule z Γ, pak platí i některá formule v Δ“. Znaménko $\Rightarrow$ v zápisu sekventu není metamatematickou zkratkou ani logickou spojkou, nýbrž formálním symbolem oddělujícím množiny Γ a Δ. Množině Γ v sekventu $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ říkáme *antecedent* a množině Δ *sukcedent*. Antecedent i sukcedent mohou být i prázdné. Pokračujeme v praxi vypouštění množinových symbolů $\cup$ a $\emptyset$ a složených závorek, jde-li o množiny formulí. Například místo $\langle\, \Gamma \cup \{\varphi\} \Rightarrow \emptyset \,\rangle$ píšeme jen $\langle\, \Gamma, \varphi \Rightarrow \,\rangle$. Význam sekventu $\langle\, \Gamma \Rightarrow \,\rangle$ je „nemohou současně platit všechny formule z Γ“ (tj. „množina Γ je sporná“), význam sekventu $\langle\, \Rightarrow \varphi \,\rangle$ je „platí φ“. V souladu s tím definujeme *důkaz formule* φ jako důkaz sekventu $\langle\, \Rightarrow \varphi \,\rangle$.

V literatuře se většinou lze setkat s trochu jiným způsobem zapisování sekventů. Například v [49] a [91] se nepíší lomené závorky a místo $\Rightarrow$ se píše delší jednoduchá šipka $\longrightarrow$. Spojka implikace se v literatuře o gentzenovských kalkulech často zapisuje symbolem $\supset$.

Gentzenovský (sekventový) kalkulus GK má následující odvozovací pravidla:

A: $\quad / \ \langle \Gamma, \varphi \Rightarrow \Delta, \varphi \rangle,$

W: $\quad \langle \Gamma \Rightarrow \Delta \rangle \ / \ \langle \Gamma \Rightarrow \Delta, \varphi \rangle, \qquad \langle \Gamma \Rightarrow \Delta \rangle \ / \ \langle \Gamma, \varphi \Rightarrow \Delta \rangle,$

$\vee$-r: $\quad \langle \Gamma \Rightarrow \Delta, \varphi \rangle \ / \ \langle \Gamma \Rightarrow \Delta, \varphi \vee \psi \rangle, \qquad \langle \Gamma \Rightarrow \Delta, \varphi \rangle \ / \ \langle \Gamma \Rightarrow \Delta, \psi \vee \varphi \rangle,$

&-l: $\quad \langle \Gamma, \varphi \Rightarrow \Delta \rangle \ / \ \langle \Gamma, \varphi \,\&\, \psi \Rightarrow \Delta \rangle, \qquad \langle \Gamma, \varphi \Rightarrow \Delta \rangle \ / \ \langle \Gamma, \psi \,\&\, \varphi \Rightarrow \Delta \rangle,$

&-r: $\quad \langle \Gamma \Rightarrow \Delta, \varphi \rangle, \langle \Gamma \Rightarrow \Delta, \psi \rangle \ / \ \langle \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \rangle,$

$\vee$-l: $\quad \langle \Gamma, \varphi \Rightarrow \Delta \rangle, \langle \Gamma, \psi \Rightarrow \Delta \rangle \ / \ \langle \Gamma, \varphi \vee \psi \Rightarrow \Delta \rangle,$

$\neg$-l: $\quad \langle \Gamma \Rightarrow \Delta, \varphi \rangle \ / \ \langle \Gamma, \neg\varphi \Rightarrow \Delta \rangle,$

$\neg$-r: $\quad \langle \Gamma, \varphi \Rightarrow \Delta \rangle \ / \ \langle \Gamma \Rightarrow \Delta, \neg\varphi \rangle,$

$\to$-r: $\quad \langle \Gamma, \varphi \Rightarrow \Delta, \psi \rangle \ / \ \langle \Gamma \Rightarrow \Delta, \varphi \to \psi \rangle,$

$\to$-l: $\quad \langle \Gamma \Rightarrow \Delta, \varphi \rangle, \langle \Pi, \psi \Rightarrow \Lambda \rangle \ / \ \langle \Gamma, \Pi, \varphi \to \psi \Rightarrow \Delta, \Lambda \rangle,$

Cut: $\quad \langle \Gamma \Rightarrow \Delta, \varphi \rangle, \langle \Pi, \varphi \Rightarrow \Lambda \rangle \ / \ \langle \Gamma, \Pi \Rightarrow \Delta, \Lambda \rangle.$

Vidíme, že na rozdíl od kalkulu HK, který má jen jedno pravidlo s nenulovým počtem předpokladů, má kalkulus GK naopak jen jedno pravidlo, totiž A, s nulovým počtem předpokladů. Pravidlo A umožňuje prohlásit za odvozený jakýkoliv sekvent, který má nějakou formuli současně v antecedentu i v sukcedentu. Takovému sekventu se říká *iniciální sekvent*, někdy též *axiom*.

Důkaz v kalkulu GK lze podobně jako důkaz v kalkulu HK definovat buď jako konečnou posloupnost sekventů, v níž každý (je iniciální nebo) je odvozen z předchozích pomocí některého pravidla, nebo jako konečný orientovaný strom s vrcholy ohodnocenými sekventy, v jehož listech jsou iniciální sekventy, dále každý jiný sekvent je odvozen z jednoho nebo dvou dceřinných sekventů pomocí některého pravidla a v kořenu je výsledný (*finální*) sekvent.

Jednoduchý důkaz zapsaný ve formě stromu může vypadat například takto:

$$\left.\begin{array}{r} \langle \varphi \Rightarrow \varphi \rangle \ / \ \langle \Rightarrow \underline{\varphi}, \neg\varphi \rangle \\ \langle \underline{\neg\varphi} \Rightarrow \neg\varphi \rangle \end{array}\right\} \langle \varphi \to \neg\varphi \Rightarrow \neg\varphi \rangle \ / \ \langle \Rightarrow (\varphi \to \neg\varphi) \to \neg\varphi \rangle.$$

V tomto důkazu je finální sekvent $\langle \Rightarrow (\varphi \to \neg\varphi) \to \neg\varphi \rangle$ odvozen třemi kroky ze dvou iniciálních sekventů. Vlevo nahoře je lomítkem vyznačeno použití pravidla $\neg$-r. Každé z obou pravidel pro negaci umožňuje připsat negaci ke kterékoliv formuli v antecedentu (resp. v sukcedentu) a zároveň ji přemístit na druhou stranu. Velkou složenou závorkou je vyznačeno použití pravidla $\to$-l. Toto pravidlo je použito na množiny $\Gamma = \emptyset$, $\Delta = \{\varphi\}$, $\Pi = \emptyset$ a $\Lambda = \{\neg\varphi\}$. Pravidlo $\to$-l umožňuje utvořit implikaci z formulí, z nichž závěr byl původně v antecedentu jednoho a premisa

v sukcedentu druhého sekventu. Tyto formule jsou v našem případě vyznačeny podtržením. V posledním kroku je použito pravidlo $\to$-r.

Na obrázku 1.4.1 je jiný příklad důkazu, tentokrát zapsaný ve formě stromu s kořenem dole a s kroky vyznačenými vodorovnými linkami. Snadno lze ověřit, že všechny kroky tohoto důkazu odpovídají pravidlům kalkulu GK. V okamžiku, kdy bylo použito pravidlo $\to$-l, jsme pro jistotu ony formule, ze kterých byla utvořena „nová“ implikace v antecedentu, opět vyznačili podtržením. Všimněme si podrobně posledních dvou kroků, na kterých si můžeme ukázat důležitou vlastnost kalkulu GK. V předposledním kroku je formule $\neg\psi \vee \chi$ odvozena pomocí pravidla $\vee$-r z formule $\neg\psi$ a v posledním kroku je pak táž formule odvozena podle stejného pravidla ještě jednou z formule χ. Druhé odvození téže formule ale rozhodně nebylo zbytečné, neboť současně byla odstraněna formule χ. Tím chceme upozornit na skutečnost, že zápisy tvaru Δ, ψ nebo $\Delta, \varphi \vee \psi$ připouštějí, že formule ψ resp. $\varphi \vee \psi$ je v množině Δ. Pravidlo $\vee$-r umožňuje odvodit sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta, \varphi \vee \psi \,\rangle$ ze sekventu $\langle\, \Gamma \;\Rightarrow\; \Delta, \psi \,\rangle$ jak v případě, kdy $\psi \in \Delta$, což velkou cenu nemá, tak v případě, kdy $\varphi \vee \psi \in \Delta$, což je naopak podstatné. Totéž platí o ostatních pravidlech. Není tedy úplně výstižné říci například o pravidlu $\neg$-l, že umožňuje připsat do antecedentu formuli $\neg\varphi$ za předpokladu, že v sukcedentu předchozího již dokázaného sekventu je formule φ. Přesnější je říci, že pravidlo $\neg$-l umožňuje odstranit ze sukcedentu libovolnou formuli φ za předpokladu, že formule $\neg\varphi$ je v antecedentu nebo že ji tam přidáme. Na pravidlech gentzenovského kalkulu je tedy podstatné to, že ve formálním důkazu mohou některé formule postupně zmizet. Méně podstatné je to, že nové formule se mohou postupně objevit. Kdyby šlo jen o přidání nových formulí, vystačili bychom s pravidlem W, kterému se česky říká *pravidlo oslabení*, anglicky *weakening rule*.

Formuli nebo formulím, které při použití nějakého pravidla vznikají nově nebo opětovně, se říká *principální formule* tohoto (použití) pravidla. Formuli, která při použití pravidla mizí, říkejme *vstupní* formule tohoto (použití) pravidla. Ostatní formule v sekventu, se kterými se neděje nic, jsou *postranní*. Je-li například sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta, \varphi \to \psi \,\rangle$ odvozen pravidlem $\to$-r ze sekventu $\langle\, \Gamma, \varphi \;\Rightarrow\; \Delta, \psi \,\rangle$, pak φ a ψ jsou vstupní formule, $\varphi \to \psi$ je principální a formule v Γ a v Δ jsou postranní. Jak vstupní, tak principální formule může být zároveň postranní formulí.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\langle\, \varphi, \psi \;\Rightarrow\; \varphi \,\rangle \quad \langle\, \varphi, \psi \;\Rightarrow\; \psi \,\rangle}{\langle\, \varphi, \psi \;\Rightarrow\; \varphi \,\&\, \psi \,\rangle}}{\langle\, \varphi \;\Rightarrow\; \varphi \,\&\, \psi, \neg\psi \,\rangle}}{\langle\, \Rightarrow\; \varphi \,\&\, \psi, \neg\psi, \underline{\neg\varphi} \,\rangle} \quad \langle\, \underline{\chi} \;\Rightarrow\; \chi \,\rangle}{\langle\, \neg\varphi \to \chi \;\Rightarrow\; \varphi \,\&\, \psi, \neg\psi, \chi \,\rangle}}{\langle\, \neg(\varphi \,\&\, \psi), \neg\varphi \to \chi \;\Rightarrow\; \neg\psi, \chi \,\rangle}}{\langle\, \neg(\varphi \,\&\, \psi), \neg\varphi \to \chi \;\Rightarrow\; \neg\psi \vee \chi, \chi \,\rangle}}{\langle\, \neg(\varphi \,\&\, \psi), \neg\varphi \to \chi \;\Rightarrow\; \neg\psi \vee \chi \,\rangle}$$

Obrázek 1.4.1: Příklad důkazu v gentzenovském kalkulu

Pravidlo Cut, kterému se česky říká *pravidlo řezu*, nemá žádnou principální formuli. Ostatní pravidla mají vždy jednu principální formuli, jen o pravidle A si můžeme myslet, že má dvě. Pravidlům W a Cut se říká *strukturální*, ostatní pravidla jsou *výrokově logická*. Důkaz, ve kterém není použito pravidlo Cut, se nazývá *bezřezový*. Oba dosud uvedené příklady jsou bezřezové.

Prohlédněme si ještě jeden příklad důkazu, tentokrát zapsaného ve formě posloupnosti sekventů. Na tomto příkladu si zároveň ukážeme, jak může být pravidlo Cut užitečné ke spojení dílčích výsledků do jediného důkazu. Předpokládejme, že si přejeme dokázat formuli $((\varphi \to \psi) \to \varphi) \to \varphi$. Označme ji A. Máme tedy sestrojit důkaz sekventu $\langle \Rightarrow A \rangle$. Důkaz sestrojíme formalizací následující úvahy:

(i) Platí φ nebo $\neg\varphi$.
(ii) Když φ, pak ano, platí také jakákoliv implikace tvaru $(..) \to \varphi$.
(iii) Když $\neg\varphi$, pak platí $\varphi \to \psi$.
(iv) Když $\neg\varphi$ a $\varphi \to \psi$, pak neplatí $(\varphi \to \psi) \to \varphi$.
(v) Když $\neg((\varphi \to \psi) \to \varphi)$, pak ano, platí implikace $((\varphi \to \psi) \to \varphi) \to \varphi$.

Jednotlivým krokům této neformální úvahy odpovídá následující formální důkaz. Každý z prvních třinácti členů je buď iniciálním sekventem nebo je odvozen z bezprostředně předchozího nebo dvou předchozích sekventů:

1: $\langle \varphi \Rightarrow \varphi, \psi \rangle$

2: $\langle \varphi, \neg\varphi \Rightarrow \psi \rangle$

3: $\langle \neg\varphi \Rightarrow \varphi \to \psi \rangle$; Krok (iii)

4: $\langle \varphi \to \psi \Rightarrow \varphi \to \psi \rangle$

5: $\langle \varphi \Rightarrow \varphi \rangle$

6: $\langle \varphi \to \psi, (\varphi \to \psi) \to \varphi \Rightarrow \varphi \rangle$

7: $\langle \varphi \to \psi, \neg\varphi, (\varphi \to \psi) \to \varphi \Rightarrow \rangle$

8: $\langle \varphi \to \psi, \neg\varphi \Rightarrow \neg((\varphi \to \psi) \to \varphi) \rangle$; Krok (iv)

$\vdots$

11: $\langle \neg((\varphi \to \psi) \to \varphi) \Rightarrow A \rangle$; Krok (v)

12: $\langle \varphi, (\varphi \to \psi) \to \varphi \Rightarrow \varphi \rangle$

13: $\langle \varphi \Rightarrow A \rangle$; Krok (ii).

Nyní použijeme (třikrát) pravidlo řezu a dokončíme důkaz sekventu $\langle \Rightarrow A \rangle$:

14: $\langle \varphi \to \psi, \neg\varphi \Rightarrow A \rangle$; Cut na 11, 8

15: $\langle\, \neg\varphi \Rightarrow A \,\rangle$; Cut na 14, 3

16: $\langle\, \varphi \vee \neg\varphi \Rightarrow A \,\rangle$; $\vee$-l na 15, 13

$\vdots$

21: $\langle\, \Rightarrow A \,\rangle$.

Vynechali jsme šest sekventů s čísly 9, 10 a 17–20. Čtenář, který je dovede doplnit, pravděpodobně už ví, jak gentzenovský kalkulus funguje.

Řekneme, že $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je *tautologický sekvent*, jestliže ke každému pravdivostnímu ohodnocení v, pro které platí $v(\varphi) = 1$ pro každou formuli $\varphi \in \Gamma$, existuje formule $\psi \in \Delta$ taková, že $v(\psi) = 1$. To znamená, že sekvent je tautologický, jestliže neexistuje pravdivostní ohodnocení, které přiřazuje hodnotu 1 všem formulím v antecedentu a hodnotu 0 všem formulím v sukcedentu.

Věta 1.4.1 (o úplnosti kalkulu GK) *Sekvent* $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ *je dokazatelný v kalkulu GK, právě když je tautologický.*

Důkaz Implikace $\Rightarrow$ je věta o korektnosti a lze ji dokázat indukcí podle počtu kroků v důkazu sekventu $\langle\, \Gamma \Rightarrow \Delta \,\rangle$. Je zřejmé, že každý iniciální sekvent je tautologický. Neexistuje-li pravdivostní ohodnocení v, které přiřazuje hodnotu 1 všem formulím v Γ a hodnotu 0 všem formulím v Δ, pak neexistuje ani pravdivostní ohodnocení, které přiřazuje hodnotu 1 všem formulím v Γ, Π a hodnotu 0 všem formulím v Δ, Λ, a to bez ohledu na volbu množin formulí Π a Λ. Tím je ověřena korektnost pravidla W.

Korektnost všech ostatních pravidel lze ověřit podobně, podívejme se namátkou ještě na pravidlo $\rightarrow$-r. Nechť $\langle\, \Gamma, \varphi \Rightarrow \Delta, \psi \,\rangle$ je tautologický sekvent. Máme ověřit, že v tom případě i $\langle\, \Gamma \Rightarrow \Delta, \varphi \rightarrow \psi \,\rangle$ je tautologický sekvent. Nechť tedy v je pravdivostní ohodnocení, které přiřazuje hodnotu 1 všem formulím v Γ. Když $v(\varphi) = 0$, pak $v(\varphi \rightarrow \psi) = 1$. Když $v(\varphi) = 1$, pak, protože $\langle\, \Gamma, \varphi \Rightarrow \Delta, \psi \,\rangle$ je tautologický sekvent, platí $v(\psi) = 1$ nebo $v(\chi) = 1$ pro některou formuli $\chi \in \Delta$. Když $v(\psi) = 1$, pak ovšem i $v(\varphi \rightarrow \psi) = 1$. Ve všech případech tedy v sukcedentu $\Delta, \varphi \rightarrow \psi$ existuje formule, které ohodnocení v přiřazuje hodnotu 1.

Zbývá dokázat podstatnou implikaci $\Leftarrow$ tvrzení věty. Nechť $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je tautologický sekvent. Máme dokázat, že je dokazatelný v GK. Postupujme indukcí podle souhrnného počtu (výskytů) logických spojek v množině $\Gamma \cup \Delta$.

Nechť v množině $\Gamma \cup \Delta$ nejsou žádné logické spojky, tj. jsou tam samé atomické formule. Když $\Gamma \cap \Delta = \emptyset$, lze všem formulím v Γ přiřadit hodnotu 1 a všem formulím v Δ hodnotu 0. Jinak řečeno, když $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je tautologický sekvent, pak $\Gamma \cap \Delta \neq \emptyset$ a sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je iniciální, tedy dokazatelný v GK.

Nechť nyní $\Gamma \cup \Delta$ obsahuje i neatomické formule. Zvolme libovolnou z nich a označme ji χ. Nechť $\chi \in \Gamma$. Označme $\Pi = \Gamma - \{\chi\}$, platí $\Pi, \chi = \Gamma$. Podle toho,

zda χ je tvaru $\varphi \to \psi$, $\varphi \vee \psi$, $\varphi \,\&\, \psi$ nebo $\neg\varphi$, připišme nad sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ dva (v případě negace jen jeden) nové sekventy podle následujícího návodu:

$$\frac{\begin{array}{cc}\vdots & \vdots\\ \langle\, \Pi, \psi \;\Rightarrow\; \Delta \,\rangle & \langle\, \Pi \;\Rightarrow\; \Delta, \varphi \,\rangle\end{array}}{\langle\, \Pi, \varphi \to \psi \;\Rightarrow\; \Delta \,\rangle} \qquad \frac{\begin{array}{cc}\vdots & \vdots\\ \langle\, \Pi, \varphi \;\Rightarrow\; \Delta \,\rangle & \langle\, \Pi, \psi \;\Rightarrow\; \Delta \,\rangle\end{array}}{\langle\, \Pi, \varphi \vee \psi \;\Rightarrow\; \Delta \,\rangle}$$

$$\frac{\begin{array}{c}\vdots\\ \langle\, \Pi, \varphi, \psi \;\Rightarrow\; \Delta \,\rangle\end{array}}{\begin{array}{c}\langle\, \Pi, \varphi, \varphi \,\&\, \psi \;\Rightarrow\; \Delta \,\rangle\end{array}}{\langle\, \Pi, \varphi \,\&\, \psi \;\Rightarrow\; \Delta \,\rangle} \qquad \frac{\begin{array}{c}\vdots\\ \langle\, \Pi \;\Rightarrow\; \Delta, \varphi \,\rangle\end{array}}{\langle\, \Pi, \neg\varphi \;\Rightarrow\; \Delta \,\rangle}$$

s úmyslem vytvořit postupně důkaz sekventu $\langle\, \Pi, \chi \;\Rightarrow\; \Delta \,\rangle$. Snadno lze ověřit, že je-li $\langle\, \Pi, \chi \;\Rightarrow\; \Delta \,\rangle$ tautologický sekvent, pak nově utvořené sekventy jsou také tautologické. A dále, finální sekvent $\langle\, \Pi, \chi \;\Rightarrow\; \Delta \,\rangle$ je z nově utvořených sekventů odvoditelný použitím (v případě konjunkce dvojnásobným) příslušného pravidla kalkulu GK. Ve všech případech jsme tedy zpětným užitím pravidla $\to$-l, $\vee$-l, &-l resp. $\neg$-l (v případě konjunkce dvojnásobným užitím) převedli dokazatelnost daného sekventu na dokazatelnost jednoho nebo dvou jiných tautologických sekventů. Každý z nich má nejméně o jednu logickou spojku méně, a podle indukčního předpokladu je tedy dokazatelný. Do míst označených tečkami tedy můžeme vepsat další sekventy tak, abychom dostali požadovaný důkaz sekventu $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$. V případě, kdy $\chi \in \Delta$, postupujeme analogicky: podle toho, zda χ je implikací, konjunkcí, negací nebo disjunkcí, použijeme zpětně pravidlo $\to$-r, &-r, $\neg$-r resp. dvakrát pravidlo $\vee$-r. QED

Větu o silné úplnosti kalkulu GK explicitně neformulujeme, spokojme se s následujícím komentářem. Existují nejméně dva rozumné způsoby, jak pro gentzenovský kalkulus definovat dokazatelnost z množiny předpokladů:

(i) Sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je dokazatelný z množiny předpokladů T, jestliže existuje konečná množina $\Omega \subseteq T$ taková, že sekvent $\langle\, \Omega, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je dokazatelný v GK.

(ii) Sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je dokazatelný z T, jestliže je dokazatelný v modifikovaném kalkulu, ve kterém se kromě běžných iniciálních sekventů připouštějí ještě iniciální sekventy tvaru $\langle \;\Rightarrow\; \varphi \,\rangle$, kde $\varphi \in T$.

Obě možnosti jsou ekvivalentní (cvičení). Máme-li dokazatelnost sekventu z množiny předpokladů a definujeme-li ještě vyplývání sekventu z množiny předpokladů, snadno pak domyslíme, že silná úplnost plyne z úplnosti s užitím věty o kompaktnosti, podobně jako v případě kalkulu HK.

Vraťme se ještě k našemu důkazu věty o úplnosti kalkulu GK. Důkaz daného sekventu jsme tam sestrojili zpětným použitím pravidel kalkulu GK. Ne všechna pravidla jsme v důkazu potřebovali. Obešli jsme se bez užití pravidel W a Cut a věta o úplnosti by tedy platila i pro kalkulus bez těchto dvou pravidel. Navíc, u

pravidla $\rightarrow$-l, v jehož formulaci se vyskytují čtyři množiny formulí Γ, Δ, Π a Λ, bychom vystačili s jednodušší formulací se dvěma množinami:

$$\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle, \langle\, \Gamma, \psi \Rightarrow \Delta \,\rangle \;/\; \langle\, \Gamma, \varphi \rightarrow \psi \Rightarrow \Delta \,\rangle.$$

Možnost zbavit se pravidla W a zjednodušit pravidlo $\rightarrow$-l pokládejme za nepodstatnou. Pravidlo W a obecnější formulace pravidla $\rightarrow$-l se v kalkulu GK připouštějí hlavně proto, aby bylo možné jen nevelkou modifikací získat kalkulus pro jednu z neklasických logik, což uvidíme v kapitole 5. Za pozoruhodnou pokládejme možnost zbavit se pravidla Cut.

Věta 1.4.2 (o eliminovatelnosti řezů) *Každý sekvent dokazatelný v kalkulu GK je dokazatelný i bez užití pravidla řezu.*

Všimněme si některých souvislostí věty o eliminovatelnosti řezů. Předpokládejme, že v určitém kroku důkazu byl sekvent $\mathcal{S}$ odvozen použitím nějakého logického pravidla ze sekventu $\mathcal{S}_1$ nebo ze dvou sekventů $\mathcal{S}_1$ a $\mathcal{S}_2$. Už jsme si vysvětlili, že v sekventu $\mathcal{S}_1$ nebo v sekventech $\mathcal{S}_1$ a $\mathcal{S}_2$ mohou být formule, které nejsou v $\mathcal{S}$. Zbavit se určitých formulí je vlastně cílem dokazování. Například když $\mathcal{S}_1$ je sekvent $\langle\, \Gamma, \varphi \Rightarrow \Delta, \psi \,\rangle$ a $\mathcal{S}$ je sekvent $\langle\, \Gamma \Rightarrow \Delta, \varphi \rightarrow \psi \,\rangle$, žádná z formulí φ a ψ nemusí být prvkem množiny $\Gamma \cup \Delta$. Důležité však je, že žádná z těchto dvou formulí nemůže zmizet beze stopy, obě jsou podformulemi formule $\varphi \rightarrow \psi$. Této vlastnosti pravidla $\rightarrow$-r se anglicky říká *subformula property*. Česky říkejme, že pravidlo $\rightarrow$-r *zachovává podformule*: je-li sekvent $\mathcal{S}$ odvozen jedním krokem pomocí tohoto pravidla ze sekventu $\mathcal{S}_1$, pak každá formule vyskytující se v $\mathcal{S}_1$ je *podformulí* některé formule sekventu $\mathcal{S}$ (pokud ovšem vztah „býti podformulí“ chápeme jako reflexivní; každá formule je svou vlastní podformulí). Lze ověřit, že také všechna ostatní pravidla kalkulu GK s výjimkou pravidla Cut zachovávají podformule. Z toho plyne, že každý *bezřezový* důkaz zachovává podformule v tom smyslu, že každá formule v něm se vyskytující je podformulí některé formule finálního sekventu. Je-li tedy dán sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$, pak všech sekventů sestavených z podformulí formulí v něm se vyskytujících je jen konečný počet, takže existuje algoritmus, který je všechny probere. Zatím se zabýváme a ještě se dost dlouho budeme zabývat jen klasickou logikou, pro kterou to mnoho nedává. Poznamenejme však pro budoucnost, že pro každou výrokovou logiku, pro kterou lze definovat gentzenovský kalkulus tak, aby platila věta o eliminovatelnosti řezů a aby všechna pravidla kromě pravidla Cut zachovávala podformule, existuje algoritmus, který rozhoduje, zda daný sekvent je nebo není dokazatelný.

Označme GK_0 kalkulus, jehož pravidla se shodují s pravidly kalkulu GK až na to, že se nepřipouští pravidlo Cut. Pro oba kalkuly platí věta o úplnosti, a tedy libovolný sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je dokazatelný v GK, právě když je dokazatelný v GK_0. To ale neznamená, že sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je *stejně rychle* dokazatelný v GK a v GK_0. Kalkuly GK a GK_0 jsou ekvivalentní, nemusí ale být stejně efektivní. K tomu zaveďme následující pojem. Kalkulus $\mathcal{C}_2$ *polynomiálně simuluje* kalkulus $\mathcal{C}_1$, jestliže ke každému důkazu délky n, který je důkazem nějaké formule v kalkulu $\mathcal{C}_1$, existuje

důkaz téže formule v kalkulu $\mathcal{C}_2$ délky ne větší než $p(n)$, kde p je vhodný polynom. Přitom délkou důkazu (či sekventu) se myslí souhrnný počet výskytů všech výrokových atomů a logických spojek. Lze dokázat (cvičení), že kalkuly HK a GK jsou *vzájemně polynomiálně simulovatelné*: každý z nich polynomiálně simuluje druhý. Existují i další výsledky o polynomiální simulovatelnosti kalkulů: J. Krajíček dokázal, že stromové důkazy (v kalkulu HK i v kalkulu GK) polynomiálně simulují důkazy-posloupnosti. Krajíčkův důkaz si ukážeme v oddílu 3.3. Na druhé straně lze z [11] vyčíst Takeutiho důkaz, že (alespoň v případě, kdy důkazy jsou stromy) není pravda, že kalkulus GK_0 polynomiálně simuluje kalkulus GK. To znamená, že použití pravidla řezu může některé důkazy velmi výrazně zkrátit.

Cvičení

1. Sestrojte důkazy následujících sekventů v kalkulu GK:
   $\langle\, \varphi \vee (\varphi \,\&\, \psi) \;\Rightarrow\; \varphi \,\rangle$,
   $\langle\, \varphi \vee (\psi \,\&\, \neg\psi) \;\Rightarrow\; \varphi \,\rangle$,
   $\langle\, \psi \,\&\, \neg\psi \;\Rightarrow\; \varphi \,\&\, \psi \,\&\, \neg\psi \,\rangle$,
   $\langle\, \varphi \to \psi, \neg\psi \;\Rightarrow\; \psi \to \chi \,\rangle$,
   $\langle\, \varphi \vee (\psi \,\&\, \chi) \;\Rightarrow\; (\varphi \vee \psi) \,\&\, (\varphi \vee \chi) \,\rangle$,
   $\langle\, \varphi \to \psi, \neg\psi \;\Rightarrow\; \varphi \to \chi \,\rangle$,
   $\langle\, (\varphi \vee \psi) \,\&\, (\varphi \vee \chi) \;\Rightarrow\; \varphi \vee (\psi \,\&\, \chi) \,\rangle$,
   $\langle\, \neg(\varphi \to \psi) \;\Rightarrow\; \varphi \,\rangle$.

2. Vypracujte všechny vynechané části důkazů vět o korektnosti a úplnosti kalkulu GK.

3. Definujte *hloubku* stromu jako délku nejdelší větve. Délka jednoprvkové větve je nula. Analyzujte důkaz věty o úplnosti kalkulu GK a zdůvodněte, že každý tautologický sekvent s n logickými spojkami má stromový důkaz hloubky nejvýše $2n$, ve kterém je nejvýše $2^{n+1} - 1$ sekventů.

   Návod. Mez $2^{n+1}-1$ dokažte indukcí podle n. Důkaz sekventu s $n+1$ logickými spojkami sestává z důkazu sekventu s nejvýše n logickými spojkami a jednoho nebo dvou dodatečných sekventů, nebo ze dvou důkazů sekventů s n logickými spojkami a *jen jednoho* dodatečného sekventu.

4. Každý tautologický sekvent délky n má bezřezový důkaz délky $\mathcal{O}(n \cdot 2^n)$. Dokažte.

5. Předpokládejte, že i ekvivalence $\equiv$ se považuje za základní spojku, a navrhněte pro ni pravidla zachovávající podformule tak, aby pro výsledný kalkulus platila věta o úplnosti i věta o eliminovatelnosti řezů.

6. Navrhněte modifikaci kalkulu GK pro případ, kdy se připouštějí i logické konstanty $\top$ a $\bot$.

7. Dokažte, že kalkulus GK se stromovými důkazy (s důkazy-posloupnostmi) polynomiálně simuluje kalkulus HK se stromovými důkazy (resp. s důkazy-posloupnostmi).

Návod. Každý axiom kalkulu HK lze dokázat v kalkulu GK důkazem lineární délky. Pravidlo MP lze v kalkulu GK simulovat dvěma řezy.

8. Dokažte, že ve stejném smyslu také kalkulus HK polynomiálně simuluje kalkulus GK.

   Návod. Je-li $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ sekvent takový, že $\Gamma \neq \emptyset$ a $\Delta \neq \emptyset$, definujte formuli $f(\langle\, \Gamma \Rightarrow \Delta \,\rangle)$ jako $\bigwedge \Gamma \to \bigvee \Delta$. Rozšiřte definici i na případ, kdy $\Gamma = \emptyset$ nebo $\Delta = \emptyset$. U každého pravidla $\mathcal{S}_1 \;/\; \mathcal{S}$ resp. $\mathcal{S}_1, \mathcal{S}_2 \;/\; \mathcal{S}$ pracujte s implikacemi $f(\mathcal{S}_1) \to f(\mathcal{S})$ a $f(\mathcal{S}_1) \to (f(\mathcal{S}_2) \to f(\mathcal{S}))$.

9. Představte si modifikaci kalkulu GK, ve které se pravidlo A smí použít jen tehdy, je-li jeho principální formule atomická. Dokažte, že takto modifikovaný kalkulus je ekvivalentní s původním a že jej polynomiálně simuluje.

10. Nechť T je libovolná množina výrokových formulí. Označme GK_T kalkulus, ve kterém se kromě pravidel kalkulu GK připouštějí ještě iniciální sekventy tvaru $\langle\, \Rightarrow \alpha \,\rangle$, kde $\alpha \in T$. Dokažte, že libovolná formule φ je dokazatelná v kalkulu GK_T, právě když existuje konečná množina $\Omega \subseteq T$ taková, že sekvent $\langle\, \Omega, \Gamma \Rightarrow \Delta \,\rangle$ je dokazatelný v kalkulu GK.

11. Dokažte, že pro kalkulus GK_T neplatí věta o eliminovatelnosti řezů.

    Návod. Uvažujte množinu $T = \{p \,\&\, q\}$ a důkaz atomu p.

12. Uvažujte kalkulus s logickými konstantami $\top$ a $\bot$. Nechť $\langle\, \Gamma, \Pi \Rightarrow \Delta, \Lambda \,\rangle$ je tautologický sekvent. Dokažte indukcí podle počtu kroků v jeho bezřezovém důkazu, že existuje formule ω, která je sestavena jen z atomů vyskytujících se současně v obou sekventech $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ a $\langle\, \Pi \Rightarrow \Lambda \,\rangle$ a případně logických konstant $\top$ a $\bot$, a taková, že oba sekventy $\langle\, \Gamma \Rightarrow \Delta, \omega \,\rangle$ a $\langle\, \Pi, \omega \Rightarrow \Lambda \,\rangle$ jsou tautologické.

13. Odvoďte z předchozího cvičení větu o interpolaci: jsou-li φ a ψ výrokové formule takové, že $\varphi \to \psi$ je tautologie, pak buď jedna z formulí $\neg\varphi$, ψ je tautologie, nebo existuje formule ω sestavená jen z atomů vyskytujících se zároveň v obou formulích φ, ψ taková, že $\varphi \to \omega$ i $\omega \to \psi$ jsou tautologie.

2

Algoritmy a úlohy

The distinction between recursive and recursively enumerable can be traced back to (. . .) Leibniz, when he talked of ars iudicandi *(checking the correctness of a proof) and* ars inveniendi *(finding a proof).* *(P. Odifreddi v [61])*

Úlohy obecně mohou nebo nemusí být algoritmicky rozhodnutelné, a rozhoduje-li nějaký algoritmus určitou úlohu, může mít tento algoritmus různé nároky na čas potřebný k práci a na paměťový prostor nutný pro pomocné výpočty a poznámky. Ukažme si nejprve na třech jednoduchých příkladech, co myslíme *úlohou*:

Hodnota booleovského výrazu

Dáno: Konečná posloupnost w sestavená ze znaků `(`, `)`, `+`, `*`, `0` a `1`.

Úkol: Určit, zda w je syntakticky správným booleovským výrazem, a pokud ano, určit jeho hodnotu.

Násobení

Dáno: Dvě přirozená čísla x a y.

Úkol: Určit jejich součin $x \cdot y$.

Prvočíselnost

Dáno: Přirozené číslo x.

Úkol: Určit, zda x je prvočíslo.

Booleovský výraz je definován podobnou rekurzí jako třeba syntakticky správná výroková formule (viz definice 1.1.1): `0` a `1` jsou booleovské výrazy, a dále jsou-li u a v booleovské výrazy, pak také `(`u`+`v`)` a `(`u`*`v`)` jsou booleovské výrazy. Příkladem booleovského výrazu je třeba `((1+0)+((1+1)*0))`. Hodnotou booleovského výrazu rozumíme to, co dostaneme, vyčíslíme-li operace `+` a `*` podle pravdivostních tabulek pro disjunkci resp. konjunkci uvedených na straně 14. Výrazy `(1+0)` i `(1+1)` mají tedy hodnotu 1, výraz `((1+1)*0)` má hodnotu 0, výraz `((1+0)+((1+1)*0))` má hodnotu 1.

Každá úloha je vlastně nekonečnou množinou otázek. V případě úlohy Násobení jsou to například otázky „jaký je součin čísel 7 a 5?“, „jaký je součin čísel

23 a 49?“ atd. Těmto otázkám se říká *instance* dané úlohy. Společnou vlastností všech úloh je to, že instance i příslušné odpovědi lze zapsat jako konečné posloupnosti znaků (symbolů), přičemž tyto symboly patří do předem známé konečné množiny přípustných symbolů.

Předem zvolené konečné množině symbolů se říká *abeceda*. Konečné posloupnosti prvků abecedy Σ jsou *slova abecedy* Σ nebo *slova v abecedě* Σ. Počtu výskytů symbolů ve slově w říkáme *délka* slova w a značíme jej $|w|$. Délka slova w může být libovolné přirozené číslo včetně nuly. Množina všech slov v abecedě Σ se značí Σ^*. U některých úloh můžeme uvažovat dvě abecedy, *vstupní abecedu* pro zapisování instancí a *výstupní abecedu* pro zapisování odpovědí. V případě úlohy Hodnota booleovského výrazu je vstupní abecedou množina $\{\texttt{(}, \texttt{)}, \texttt{+}, \texttt{*}, \texttt{0}, \texttt{1}\}$, za výstupní abecedu můžeme považovat množinu $\{\texttt{n}, \texttt{0}, \texttt{1}\}$, jejíž prvky reprezentují odpovědi „dané slovo w není booleovským výrazem“, „dané slovo w je booleovským výrazem s hodnotou 0“ a „dané slovo w je booleovským výrazem s hodnotou 1“. Jsou-li w_1 a w_2 slova v abecedě Σ, pak w_1w_2 značí spojení (*konkatenaci*) slov w_1 a w_2, tj. slovo vzniklé zapsáním slov w_1 a w_2 (v tomto pořadí) za sebe. Například zápis $\texttt{(}u\texttt{+}v\texttt{)}$ v definici booleovského výrazu lze tedy chápat jako konkatenaci pěti slov, z nichž tři jsou jednoznaková.

Vidíme, že úloha Hodnota booleovského výrazu je z matematického hlediska vlastně funkcí z množiny $\{\texttt{(}, \texttt{)}, \texttt{+}, \texttt{*}, \texttt{0}, \texttt{1}\}^*$ do množiny $\{\texttt{n}, \texttt{0}, \texttt{1}\}^*$ či do množiny $\{\texttt{n}, \texttt{0}, \texttt{1}\}$. Rovněž Prvočíselnost je vlastně funkcí, totiž funkcí definovanou na množině N všech přirozených čísel, která má v bodě $x \in \mathrm{N}$ hodnotu 1 nebo 0 podle toho, zda x je nebo není prvočíslo. Snadno se lze domluvit, že také Prvočíselnost je vlastně funkcí definovanou na jisté množině slov, přesněji řečeno funkcí z jisté množiny $X \subseteq \Sigma_1^*$ do jisté množiny tvaru Σ_2^*: stačí říci, že přirozené číslo je reprezentováno svým dekadickým zápisem, za vstupní abecedu Σ_1 zvolit množinu $\{\texttt{0}, \texttt{1}, \ldots, \texttt{9}\}$ obsahující deset dekadických číslic a za výstupní abecedu prohlásit množinu $\{\texttt{n}, \texttt{0}, \texttt{1}\}$, jejíž prvky reprezentují odpovědi „dané slovo w není zápisem přirozeného čísla“, „dané slovo w je zápisem složeného přirozeného čísla“ a „dané slovo w je zápisem prvočísla“. Mohli bychom se také rozhodnout, že přirozená čísla budeme zapisovat binárně (ve dvojkové soustavě), a že tedy vystačíme se vstupní abecedou $\{\texttt{0}, \texttt{1}\}$. V případě úlohy Násobení je malá potíž v tom, že instance jsou *dvojicemi* přirozených čísel. Snadným řešením této potíže je přijmout do vstupní abecedy ještě jeden znak pro oddělování přirozených čísel od sebe, řekněme středník `;`, a za vstupní slova správného formátu pak považovat slova tvaru $w_1\texttt{;}w_2$, kde w_1 a w_2 jsou zápisy přirozených čísel. Úloha Násobení je tedy vlastně funkcí z množiny $\{\texttt{;}, \texttt{0}, \texttt{1}, \ldots, \texttt{9}\}^*$ nebo z množiny $\{\texttt{;}, \texttt{0}, \texttt{1}\}^*$ do množiny $\{\texttt{n}, \texttt{0}, \texttt{1}\}$.

Úlohu tedy budeme v oddílu 2.1 definovat jako libovolnou funkci z jisté množiny X do množiny Σ_2^*, kde $X \subseteq \Sigma_1^*$ a Σ_1 a Σ_2 jsou abecedy. Funkci $g : X \to Y$, kde X a Y jsou *nějaké* množiny, budeme často také nazývat úlohou, a to tehdy, bude-li domluveno nebo bude-li zřejmé, jak se prvky množin X a Y zapisují pomocí symbolů jistých abeced. Tak jsme postupovali v případě úloh Prvočíselnost a Násobení. Samozřejmě, existuje mnoho funkcí, které úlohami nejsou. Příkladem

funkce, kterou nelze považovat za úlohu, je funkce $x \mapsto \mathrm{e}^x$, tj. mocnina se základem e, kde e je Eulerovo číslo, uvažovaná v reálném oboru.

O funkci g z X do Σ_2^*, kde $X \subseteq \Sigma_1^*$, budeme říkat, že je *algoritmicky počitatelná*, jestliže existuje algoritmus, který každý vstup $w \in X$ přepracuje na výsledek $g(w)$. Existenci takového algoritmu budeme většinou prokazovat zapsáním onoho algoritmu v programovacím jazyce RASP, který si pro tento účel zavedeme. Jazyk RASP je abstraktním programovacím jazykem v tom smyslu, že se nevztahuje k žádnému skutečnému počítači. Píšou se v něm programy pro myšlený počítač, jehož činnost je přesně definována, který ale nikdy nebyl skutečně realizován (sestaven z elektronických či jiných součástek). Takovému myšlenému počítači vybavenému příslušným programovacím jazykem se také říká *výpočtový model*. Naším primárním výpočtovým modelem tedy bude počítač RASP resp. programovací jazyk RASP.

Budeme-li chtít zdůraznit, že nám jde o algoritmické zpracování určitých syntaktických objektů (například formulí nebo důkazů), budeme k zápisu těchto syntaktických objektů užívat strojopisné písmo. To jsme také udělali na začátku při zápisu booleovských výrazů.

Časem uvidíme, že existují četné analogie mezi dokazováním a programováním. Máme-li neformální (nicméně správný a dostatečně podrobný) důkaz nějakého tvrzení, je pouze věcí zkušenosti, jak jej přepsat do formalismu kteréhokoliv logického kalkulu. To jsme už viděli na str. 43, kde jsme na základě neformální úvahy sestrojili formální důkaz formule $((\varphi \to \psi) \to \varphi) \to \varphi$, a řadu takových případů ještě uvidíme. Podobně se to má s programováním. Neformální, nicméně správný a dostatečně podrobný algoritmus může zkušený programátor přepsat do formalismu kteréhokoliv programovacího jazyka. Zkušený programátor ale také ví, že je podstatné, aby před psaním programu v daném jazyce již měl onen neformální algoritmus.

Skutečnost, že daný neformální důkaz nebo daný neformální algoritmus byl úspěšně přepsán do formalismu určitého logického kalkulu nebo do formalismu určitého programovacího jazyka, lze chápat jako potvrzení správnosti takového neformálního důkazu nebo algoritmu. Postupně však chceme čtenáře přesvědčit, že správný algoritmus lze rozpoznat i bez přepisování do daného formalismu a že obvykle lze bez přepisování do daného formalismu stanovit i to, jaké má daný algoritmus nároky na čas a paměťový prostor. Jsme přesvědčeni, že totéž platí i o dokazování. Každý, kdo má určitou zkušenost s matematickými důkazy, dovede odlišit správný důkaz od nesprávného a nepotřebuje se přitom opírat o jakýkoliv logický kalkulus. Takto také rozumíme citátu z knihy [51] uvedenému v Úvodu na str. 9: logika *není* hygienou matematiky.

V této kapitole si tedy zavedeme programovací jazyk RASP, naučíme se v něm programovat a naučíme se analyzovat programy v něm napsané. Dále se zmíníme o nejdůležitějších pojmech teorie rekurzívních funkcí a výpočtové složitosti. Tyto pojmy pak využijeme v kapitole 4 a v některých úvahách kapitoly 5. Nicméně čtenář, kterého souvislosti logiky a teoretické informatiky tolik nezajímají, by měl vědět, že téměř celou kapitolu 3 a značné části zbývajících kapitol lze číst bez znalosti problematiky z kapitoly 2. Naopak vážnější zájemce o teoretickou informatiku

upozorňujeme, že většinu obtížnějších důkazů týkajících se pojmů z kapitoly 2 jsme vypustili. O jazyce RASP, který studujeme v oddílu 2.1, musíme uznat, že je v literatuře méně běžný. Hledali jsme ale takový jazyk, ve kterém i netriviální programy lze skutečně napsat, a to tak, že mají rozumnou délku a současně není obtížné stanovit jejich časové a prostorové nároky. Některým čtenářům bude přitom určitě zřejmé, že do definice jazyka RASP uložil autor část zkušenosti, kterou kdysi získal v ČKD Polovodiče při psaní programů pro počítače firmy Digital. Některé vlastnosti našeho výpočtového modelu jsou převzaty z jazyka, který na tomtéž pracovišti navrhl a implementoval J. Pavelka se spolupracovníky.

2.1 Programování v jazyce RASP

Hlavními částmi počítače RASP jsou paměť, procesor, vstupní páska a výstupní páska. *Paměť* počítače RASP je rozdělena na *(paměťové) buňky*. Každá buňka může obsahovat (libovolně velké) celé číslo. Buněk je nekonečně mnoho a jsou číslovány celými čísly. Je-li celé číslo chápáno jako číslo paměťové buňky, říkáme mu *adresa* (oné buňky). Protože připouštíme i záporné adresy, můžeme o paměti počítače RASP říci, že je oboustranně neomezená. Obsah libovolné buňky může být interpretován jako data, tj. jako číslo, s nímž má být proveden nějaký výpočet, nebo jako adresa (jiné buňky), nebo jako číselný kód (strojový kód) nějaké *instrukce* (pro procesor).

Procesor počítače RASP pracuje v *taktech* (*krocích*), v každém taktu provádí jednu instrukci, kterou si přečetl (tj. jejíž strojový kód si přečetl) v paměti počítače. Strojový kód instrukce zabírá v paměti počítače podle druhu instrukce jednu nebo několik sousedících buněk. Procesor má schopnost uchovávat (bez použití paměti počítače) údaj, kterému se říká *čítač instrukcí* a který sestává z jednoho celého čísla. Význam čítače instrukcí je „adresa instrukce, která má být provedena v následujícím taktu“. Každý takt tedy probíhá tak, že procesor přečte z paměti strojový kód instrukce, jejíž adresu má uloženou v čítači instrukcí, přitom podle druhu instrukce zvětší obsah čítače instrukcí tak, aby obsahoval adresu bezprostředně následující instrukce, a pak přečtenou instrukci provede. Výsledkem provedení instrukce může být ještě další změna čítače instrukcí. Některé instrukce, tzv. *skokové instrukce*, totiž dělají právě (a pouze) to, že nastaví do čítače instrukcí určitou hodnotu, a to podmíněně (podle výsledku dříve provedených instrukcí), nebo nepodmíněně.

Jednoduchý příklad programu v jazyce RASP je na obrázku 2.1.1 vlevo. V tomto programu jsou užity dvě jednooperandové instrukce `jeq` a `jgt`, čtyři dvouoperandové instrukce `mov`, `cmp`, `add` a `sub` (s operandy oddělenými čárkou) a jedna instrukce bez operandů, totiž `halt`.

Předpokládáme, že máme k dispozici program zvaný *překladač* (jazyka RASP), jehož účelem je přeložit program v jazyce RASP do strojového kódu. Přeložit program znamená nahradit každou instrukci jejím strojovým kódem a určit tomuto kódu místo v paměti počítače RASP. Nezabýváme se otázkou, zda překladač výsledek své práce vhodným způsobem uloží, abychom jej kdykoliv později mohli

```
mov     #0,20
cmp     18,#0
jeq     17
add     19,20
sub     #1,18
jgt     9
halt
813
964
0
```

```
        mov     #0,Z
        cmp     X,#0
        jeq     Done
Rep:    add     Y,Z
        sub     #1,X
        jgt     Rep
Done:   halt
X:      813
Y:      964
Z:      0
```

Obrázek 2.1.1: Výpočet součinu

spustit, nebo zda jej rovnou zapíše do paměti počítače RASP a spustí jej. Pomíjíme také otázku, na jakém počítači pracuje překladač, zda rovněž na počítači RASP či na nějakém jiném, a nepokoušíme se specifikovat strojové kódy instrukcí. RASP je zkratka slov *random access stored program*. Termín „random“ v tomto případě neznamená „náhodný“, ale spíše „libovolný“: procesor může v jednom taktu přečíst nebo modifikovat libovolně vzdálenou paměťovou buňku. „Stored program“ znamená, že běžící program je umístěn v paměti počítače spolu s daty, která zpracovává. Program tedy může svou činností sám sebe modifikovat; tuto možnost ale nehodláme využívat.

Definujme, že strojový kód instrukce zabírá v paměti počítače jednu, dvě nebo tři paměťové buňky podle toho, jde-li o instrukci bez operandů, o instrukci s jedním operandem nebo o instrukci se dvěma operandy. Předpokládáme-li, že strojový kód první instrukce `mov #0,20` programu na obr. 2.1.1 vlevo je uložen na adresách `1`, `2` a `3`, snadno lze odpočítat, že například instrukce `add 19,20` je umístěna na adrese `9` a instrukce `halt` je umístěna na adrese `17`. Vše, co překladač nerozpozná jako instrukci, považuje za číslo (konstantu), kterou má rovněž uložit do paměti. To znamená, že v případě programu z obr. 2.1.1 překladač za strojový kód instrukce `halt` uloží čísla 813, 964 a 0, a to na adresy `18`, `19` a `20`.

Důležitou vlastností překladače jazyka RASP je schopnost pracovat se symbolickými odkazy. Libovolná instrukce může být označena *návěštím*, které je v zápisu programu umístěno vlevo před instrukcí na tomtéž řádku a které je od ní odděleno dvojtečkou. Překladač při překladu programu určí hodnotu každého návěští, a to stejným způsobem, jako když jsme před chvilkou určili, že adresa instrukce `halt` z programu na obr. 2.1.1 je `17`. Vyskytne-li se návěští v operandu některé instrukce, překladač místo něj použije jeho hodnotu, tj. adresu instrukce, která je oním návěštím označena. Vpravo na obrázku 2.1.1 je týž program jako vlevo, jsou v něm ale použity symbolické odkazy. Návěštími jsou označeny i buňky s adresami `18`, `19` a `20`, které neobsahují opravdové instrukce. To je ovšem také povoleno. Je zřejmé, že můžeme-li užívat symbolické odkazy, nemusíme odpočítávat instrukce, abychom zjistili, na jaké adrese je co uloženo, a nemusíme dokonce ani vědět, kolik paměťových buněk je třeba k uložení strojových kódů jednotlivých instrukcí.

Význam instrukce `add Y,Z` je „přičti k číslu uloženému na adrese `Z` číslo uložené na adrese `Y`“ (neboli „sečti čísla uložená na adresách `Y` a `Z` a ulož výsledek na adresu `Z`“), význam instrukce `sub #1,X` je „odečti jedničku od čísla uloženého na adrese `X`“. Instrukce `jgt Rep` je *podmíněný skok*; její význam je „pokračuj na adrese `Rep` (tj. na adrese `9`), byl-li výsledek naposled provedené aritmetické instrukce (v našem případě instrukce `sub`) větší než nula“. Tyto tři instrukce tedy pracují tak, že přičtou k obsahu buňky `Z` obsah buňky `Y` tolikrát, kolik udávalo číslo původně uložené v buňce `X`. Poté je provedena instrukce `halt`, jejíž význam je „hotovo, skonči“. Před prvním provedením instrukce `add` umístěné na adrese `Rep` program provede instrukci `mov #0,Z`, která znamená „ulož nulu na adresu `Z`“. Tato instrukce je zbytečná, neboť nulu na adresu `Z` uložil již překladač (tj. obsah adresy `Z` byl staticky inicializován pomocí zápisu `Z: 0`). Účelem instrukce `cmp` (*compare*, porovnej) je zjistit, zda první z obou činitelů je nulový. Pokud ano, program přeskočí tři instrukce uložené na adresách `Rep` až `Rep+7` (tj. podmíněný skok `jeq Done` se provede) a skončí svou činnost provedením instrukce `halt`. Tím jsme zdůvodnili, že program z obrázku 2.1.1 vypočte součin nezáporných čísel uložených v buňkách `X` a `Y` a uloží jej do buňky `Z`.

Procesor počítače RASP při své činnosti udržuje kromě čítače instrukcí dva tzv. *podmínkové bity* Z a G. Nastavení určité hodnoty podmínkových bitů je vedlejším (a někdy jediným) efektem provedení kterékoliv aritmetické instrukce. Podle nastavení podmínkových bitů se pak řídí činnost skokových instrukcí. Bit Z je nebo není nastaven podle toho, byl-li výsledek naposled provedené aritmetické instrukce nulový (*zero*). Bit G je nebo není nastaven podle toho, byl-li výsledek naposled provedené aritmetické instrukce větší než nula (*greater*). Přesný význam instrukce `jgt` ⟨*lab*⟩ (*jump if greater*) tedy je „pokračuj na adrese ⟨*lab*⟩, je-li bit G nastaven (tj. má-li hodnotu 1), jinak pokračuj bezprostředně následující instrukcí“. Instrukce `jeq` (*jump if equal*) má analogický význam, řídí se bitem Z. Kromě dvou podmíněně skokových instrukcí máme v jazyce RASP ještě *nepodmíněný skok* `jmp`, ten se provede vždy bez ohledu na hodnoty podmínkových bitů. Žádná ze skokových instrukcí nemění hodnoty podmínkových bitů, takže podmíněně skoková instrukce může smysluplně následovat po jiné skokové instrukci, čili není nutné, aby před provedením skokové instrukce bezprostředně předcházelo provedení aritmetické instrukce. Tuto možnost budeme (muset) využívat.

Jazyk RASP má *aritmetické instrukce* `mov` (*move*, přenes), `cmp` (porovnej), `add` (přičti), `sub` (odečti), `neg` (*negate*, změň znaménko) a `shr` (*shift right*, děl dvěma). K aritmetickým instrukcím počítejme i instrukce `read` a `write`, o kterých bude řeč později. Význam instrukce `mov` jsme již definovali. Je-li například v paměťové buňce `X` uloženo číslo 5, po provedení instrukce `mov X,R` je hodnota 5 jak v buňce `X`, tak v buňce `R`, a dále bit G je nastaven (má hodnotu 1) a bit Z není nastaven (má hodnotu 0), protože číslo 5 je kladné a není nulové. Význam instrukcí `add`, `sub` a `neg` je zřejmý. Instrukci `sub` by samozřejmě bylo možné simulovat pomocí dvojice `neg` a `add`. Tím se ale nezabýváme, nesnažíme se, aby náš programovací jazyk byl za každou cenu co nejúspornější. Instrukce `cmp` nastaví podmínkové bity stejně, jako by je nastavila instrukce `sub` s prohozenými operandy. Například je-li opět v `X` číslo 5

```
      mov     #0,Z
      cmp     X,#0
      jeq     Done
      jgt     I1B
      neg     X
      neg     Y
I1B:
L1A:
      mov     X,Q
      shr     X
      sub     X,Q
      sub     X,Q
      jeq     I2B
      add     Y,Z
I2B:  add     Y,Y
      cmp     X,#0
      jgt     L1A
Done: halt
```

```
      mov     #0,Z
      if      X eq #0 then goto Done
      ;
      if      le then
        neg     X
        neg     Y
      endif
      loop
        mov     X,Q
        shr     X
        sub     X,Q
        sub     X,Q
        if      ne then add Y,Z
      ;
        add     Y,Y
      endloop X le #0
      ;
Done: halt
```

Obrázek 2.1.2: Jiný program pro výpočet součinu

a v `Y` číslo 4, instrukce `sub X,Y` uloží do buňky `Y` novou hodnotu -1 a vynuluje bity Z a G, kdežto instrukce `cmp X,Y` ponechá obsah buněk `X` a `Y` beze změny a nastaví bit G a vynuluje bit Z, protože výsledek 1 (který se nikam nezapisuje) odčítání $5 - 4$ je kladný a není nulový. Mnemonika instrukce `shr` je odvozena od představy, že číslo je v paměťové buňce počítače reprezentováno svým binárním zápisem (tj. posloupností nul a jedniček); dělení dvěma pak znamená nejnižší bit zahodit a všechny ostatní bity posunout o jedno místo doprava. Je-li například v buňce `X` uložena hodnota 4, 0 nebo -3, pak po provedení instrukce `shr X` tam je 2, 0 resp. -1.

Na obrázku 2.1.2 vlevo je uveden program, který počítá součin jiným způsobem než program z obrázku 2.1.1, totiž s využitím tzv. školního algoritmu pro násobení, který je naznačen na obrázku 2.3.6 na straně 133. Program opět očekává vstupní data v buňkách `X` a `Y`, svůj výsledek nakonec zapíše do buňky `Z`. Navíc užívá pomocnou buňku `Q`. Představujme si, že paměťové buňky `X`, `Y`, `Z` a `Q` jsou umístěny těsně za závěrečnou instrukcí `halt`; jejich alokaci (tj. deklaraci návěští `X`, `Y`, `Z` a `Q` a určení počátečního obsahu příslušných buněk) jsme pro stručnost vynechali.

Program nejprve inicializuje obsah buňky `Z`. Testováním, zda obsah buňky `X` je nenulový, pak zjistí, zda je třeba dělat cokoliv dalšího. Na rozdíl od programu z obrázku 2.1.1 se nespoléhá na to, že vstupy uložené v `X` a `Y` jsou nezáporné: je-li první činitel záporný, využije rovnost $x \cdot y = (-x) \cdot (-y)$ a pomocí dvou instrukcí `neg` změní jejich znaménka. Všimněme si, že instrukce `jgt I1B` využívá fakt, že předchozí instrukce `jeq Done` nezměnila podmínkové bity nastavené instrukcí `cmp X,#0` (po pravdě řečeno, zjišťování, zda obsah buňky `X` je nenulový, není pro správné fun-

gování programu nezbytné). Program dále provádí opakovaně instrukce na adresách `L1A` až `Done-2`. Vysvětleme si smysl těchto instrukcí podrobněji.

Označme u, v a z obsahy buněk `X`, `Y` a `Z` v kterémkoliv okamžiku výpočtu. Označme x a y vstupní data, tj. počáteční obsahy buněk `X` a `Y`. Nechť dále n je počet cifer v binárním zápisu čísla x a nechť j označuje počet, kolikrát byla dosud provedena instrukce `shr X`. Tvrdíme, že vždy před provedením instrukce `mov X,Q` a také vždy v okamžiku provedení instrukce `jgt L1A` platí

$$u = x \operatorname{div} 2^j, \qquad v = y \cdot 2^j, \qquad z = y \cdot (x \bmod 2^j), \tag{$*$}$$

kde $(x \operatorname{div} 2^j)$ označuje výsledek celočíselného dělení čísla x číslem 2^j, tj. číslo, jehož binární zápis vznikne z binárního zápisu čísla x odstraněním j nejnižších číslic, a $(x \bmod 2^j)$ označuje zbytek po dělení čísla x číslem 2^j, tj. číslo, jehož binární zápis naopak vznikne z j nejnižších číslic binárního zápisu čísla x odstraněním případných zbytečných nul na začátku. Pro $j = 0$ rovnosti $(*)$ platí: před prvním provedením instrukce `mov X,Q` máme $u = x$, $v = y$, $(x \bmod 2^0) = 0$ a $z = 0$. Platnost prvních dvou rovností i pro $j > 0$ je zřejmá, neboť instrukce `shr X` vždy dělí u dvěma a instrukce `add Y,Y` násobí v dvěma. Třetí rovnost se snadno dokáže indukcí podle j. Když $(x \operatorname{div} 2^j)$ čili u je sudé, pak $(x \bmod 2^{j+1}) = (x \bmod 2^j)$, dvojnásobné odečtení čísla $(u \operatorname{div} 2)$ od u dá nulu a z se nemění. Když naopak číslo $(x \operatorname{div} 2^j)$ je liché, čili když $(j+1)$-ní nejnižší číslice v binárním zápisu čísla x je `1`, pak dvojnásobné odečtení čísla $(u \operatorname{div} 2)$ od u dá nenulový výsledek, instrukce `add Y,Z` se provede, nová hodnota z je $v + z$, tj. $y \cdot 2^j + y \cdot (x \bmod 2^j)$, a platí $(x \bmod 2^{j+1}) = 2^j + (x \bmod 2^j)$. Po n-násobném provedení instrukce `shr X` je u nulové, skok `jgt L1A` se neprovede, $(x \bmod 2^n)$ je x, platí $z = y \cdot x$ a program skončí činnost provedením instrukce `halt`. Program z obrázku 2.1.2 tedy správně spočítá součin kterýchkoliv dvou celých čísel.

V instrukcích programů jsme zatím vystačili se dvěma druhy operandů, přímými a běžnými. *Přímý operand* má tvar `#`⟨*výraz*⟩ a jeho hodnotou je hodnota výrazu ⟨*výraz*⟩. Kdyby například v kontextu programu z obr. 2.1.1 byly použity operandy `#Done+3` nebo `#Z`, oba by měly tutéž hodnotu 20. *Běžný operand* má tvar ⟨*výraz*⟩ a jeho hodnotou je číslo uložené na adrese, která je hodnotou výrazu ⟨*výraz*⟩. Například, opět v kontextu programu z obr. 2.1.1, operand `Done+3` má zpočátku hodnotu 0 a v okamžiku provedení instrukce `halt` je jeho hodnotou součin obou vstupních čísel. Kromě přímých a běžných operandů připouští jazyk RASP ještě operandy vzdálené. *Vzdálený operand* může mít tvar `@`⟨*výraz1*⟩`(`⟨*výraz2*⟩`)`, `@(`⟨*výraz*⟩`)+` nebo `-@(`⟨*výraz*⟩`)`. Hodnotou operandu `@`⟨*výraz1*⟩`(`⟨*výraz2*⟩`)` je číslo, které je uloženo na adrese, která vznikne přičtením čísla ⟨*výraz1*⟩ k číslu uloženému na adrese ⟨*výraz2*⟩. Přitom toto sčítání procesor provádí interně, bez modifikace obsahu adresy ⟨*výraz2*⟩ a podmínkových bitů. Například je-li návěští `Done` přiřazena hodnota 17 a je-li v určitém stadiu výpočtu v `X` uloženo číslo 2, pak operandy `@Done+1(X)` a `Done+3` mají tutéž hodnotu, totiž číslo uložené na adrese `Done+3`. Hodnotou operandu `@(`⟨*výraz*⟩`)+` je číslo, jehož adresa je uložená na adrese ⟨*výraz*⟩. Znaménko plus znamená, že po přečtení obsahu adresy ⟨*výraz*⟩ je tento obsah zvětšen o jedničku. Přitom modifikace obsahu adresy ⟨*výraz*⟩ nemá vliv na hodnoty

podmínkových bitů. Je-li například v `X` číslo 140, instrukce `mov #-4,@(X)+` zvětší obsah buňky `X` na 141, uloží číslo −4 na adresu `140` a vynuluje bity Z a G (protože číslo −4 je nenulové a nekladné). Operand `-@(`⟨*výraz*⟩`)` procesor vyhodnotí tak, že sníží obsah adresy ⟨*výraz*⟩ o jedničku (opět beze změny podmínkových bitů), a pak onen obsah použije jako adresu hodnoty operandu. Domluvme se, že místo `@0(`⟨*výraz2*⟩`)` je dovoleno psát pouze `@(`⟨*výraz2*⟩`)`.

Vzdálené operandy usnadňují práci se složitějšími datovými strukturami, než jsou jednotlivá čísla. Například pracujeme-li se seznamem čísel, která jsou uložena na adresách `Tab`, `Tab+1`, `Tab+2` atd., můžeme se rozhodnout, že obsah adresy `X` bude sloužit jako ukazatel do tohoto seznamu. Provedení instrukce `mov #Tab,X` pak znamená, že ukazatel `X` byl nasměrován na začátek našeho seznamu. Je-li kdykoliv později provedena instrukce `mov @(X)+,Y`, znamená to, že program si do `Y` uložil jeden prvek seznamu a přesměroval ukazatel `X` na prvek těsně následující.

Jednou z velmi užitečných standardních datových struktur je zásobník. *Zásobník* je seznam, jehož délka se může měnit odebíráním položek a přidáváním nových položek. O položce naposled uložené do zásobníku se říká, že je umístěna na *vrcholu* zásobníku. Ze zásobníku může být odebrána pouze položka umístěná na vrcholu. To znamená, že položka uložená do zásobníku může být odebrána pouze tehdy, byly-li odebrány všechny položky, které do zásobníku byly uloženy později než ona.

Zásobník je obvyklé realizovat jako souvislou část paměti plus ukazatel (*zásobníkový ukazatel*), který vždy obsahuje adresu vrcholu zásobníku. V jazyce RASP předpokládáme, že zásobníkovým ukazatelem je paměťová buňka `SP` (*stack pointer*) a že vrchol zásobníku má nižší adresu než všechny ostatní prvky. Při uložení nového prvku do zásobníku tedy musí být snížen obsah adresy `SP`, a naopak zvýšení obsahu adresy `SP` znamená odebrání prvku (prvků) ze zásobníku. Návěští `SP` se nemusí deklarovat, překladač mu automaticky přiřadí hodnotu 0. To znamená, že paměťová buňka `0` slouží jako zásobníkový ukazatel.

Zásobník se dobře hodí k implementaci volání podprogramů. Například součástí programu z obrázku 2.1.3 je podprogram `Cnv`. V hlavním programu začínajícím na adrese `Sta` se vyskytují dvě instrukce `jmp Cnv`, neboli podprogram `Cnv` je volán ze dvou různých míst. Vždy před provedením instrukce `jmp Cnv` je ale pomocí instrukce `mov #C1,-@(SP)` resp. `mov #C2,-@(SP)` uložena do zásobníku tzv. *návratová adresa*, čili informace o tom, kde má činnost hlavního programu po návratu z podprogramu pokračovat. Uvnitř podprogramu se předpokládá, že na vrcholu zásobníku je uložena návratová adresa; ta se uplatní v okamžiku, kdy je ze zásobníku odebrána provedením instrukce `jmp @(SP)+` na adrese `L1C`. Zásobník se užívá také k implementaci lokálních dat podprogramu, což v programu z obrázků 2.1.3 a 2.1.4 nebylo třeba, a k předávání parametrů podprogramu, což, jak si za chvíli vysvětlíme, se v tomto programu skutečně děje.

Programy z obrázků 2.1.1 a 2.1.2 nejsou zcela kompletní. Pominuli jsme totiž otázku, jak se vstupní čísla, která se mají násobit, octnou v buňkách `X` a `Y`. Obecněji řečeno, pominuli jsme *vstupní a výstupní operace*. Neřekli jsme také, kde je určeno, že program začíná práci provedením instrukce na adrese `1`. Vysvětleme si nejprve to druhé, začátek činnosti programu.

K tomu, že překladač určí strojový kód každé instrukce a stanoví mu místo v paměti počítače RASP, nyní dodejme, že při obsazování paměti začíná od adresy `0`. Start programu probíhá tak, že obsah adresy `0` je vynulován (tím je inicializován zásobníkový ukazatel) a program je spuštěn od instrukce, jejíž adresa byla předtím (před vynulováním) umístěna na adrese `0`. Stanovením obsahu adresy `0` tedy při psaní programu určujeme startovací adresu programu, čili iniciální hodnotu čítače instrukcí (nikoliv iniciální hodnotu zásobníkového ukazatele, ta je vždy nulová). Například v programu z obr. 2.1.3 je umístěním čísla `Sta` na adresu `0` (tj. do prvního řádku programu) určeno, že program má svou činnost začít provedením instrukce `mov #C1,-@(SP)` na adrese `Sta`. Adresa `0`, tj. adresa `SP`, v tom okamžiku obsahuje číslo 0. Ukládání položek do zásobníku pak znamená ukládat je na (nižší a nižší) záporné adresy. Nulový obsah buňky `0` znamená prázdný zásobník.

Data, která má program zpracovat, jsou uložena na vstupní pásce. *Vstupní páska* je rozdělena na pole, která jsou očíslována celými nezápornými čísly. Pole vstupní pásky mohou obsahovat znaky. Máme k dispozici *kódovou tabulku*, která znakům přiřazuje celé nezáporné číselné kódy. Kódová tabulka je něco jako tabulka ASCII; skutečnou tabulku ASCII jsme nepoužili pouze proto, že v ní nejsou zahrnuty některé znaky důležité pro logiku, například logické spojky. Předpokládáme, že kódová tabulka obsahuje znaky všech abeced, které jsme kdy potřebovali či budeme potřebovat, a že kdyby snad ne, můžeme ji rozšířit o další znaky. Jeden ze znaků je *mezera*, kterou lze podle potřeby zapisovat jako „ “ nebo jako „␣“, žádným zvláštním číselným kódem ani ničím jiným však významná není. Vstupní páska je nekonečná, ale jen v konečně mnoha počátečních polích jsou znaky. Ve všech zbývajících polích vstupní pásky je *koncová značka* ∎, kterou nepokládáme za znak (nemůže být prvkem žádné abecedy) a která má kód -1. Čtení znaků ze vstupní pásky se děje pomocí instrukce `read`. Tato instrukce má dva operandy: druhý operand určuje, kam se má do paměti uložit číselný kód znaku umístěného v poli, které je určeno prvním operandem. Například instrukce `read 2,-@(SP)` uloží do zásobníku číselný kód znaku umístěného ve třetím (počítáme od nuly) poli vstupní pásky. Obsah vstupní pásky se během činnosti počítače nemůže měnit. Témuž programu mohou ovšem být ke zpracování předložena různá data, tj. různé obsahy vstupní pásky.

Opačný význam než vstupní páska má *výstupní páska*, na tu program může zapsat výstupní data. Výstupní páska je také rozčleněna na pole číslovaná přirozenými čísly. Při zahájení činnosti programu je výstupní páska prázdná, tj. obsahuje samé koncové značky. Zapisování znaků na výstupní pásku se děje instrukcí `write`. První operand instrukce `write` udává číselný kód znaku, druhý udává pole výstupní pásky, na které má být tento znak zapsán. Abychom se při psaní programu nemuseli zabývat číselnými kódy znaků, připouští překladač jazyka RASP výrazy tvaru ‘⟨*znak*⟩ (levý apostrof následovaný jedním znakem). Hodnotou výrazu ‘⟨*znak*⟩ je číselný kód znaku ⟨*znak*⟩. Například je-li v paměťové buňce `I` číslo 0, instrukce `write X,@(I)+` zapíše do nejlevějšího pole výstupní pásky znak, jehož číselný kód je uložen v buňce `X`. Je-li později provedena instrukce `write #‘7,@(I)+` a nebyl-li mezitím změněn obsah buňky `I`, je do druhého nejle-

```
      Sta
Cnv:  mov     @(SP),-@(SP)
      mov     #0,@1(SP)
L1A:
      read    @(Inp)+,X
      sub     #'0,X
      jgt     I1A
      jeq     I1A
      jmp     L1C
I1A:  cmp     X,#1
      jgt     L1C
      add     @1(SP),@1(SP)
      add     X,@1(SP)
      jmp     L1A
L1C:  jmp     @(SP)+
Inp:  0
Out:  0
X:    0
Sta:  mov     #C1,-@(SP)
      jmp     Cnv
C1:   mov     #C2,-@(SP)
      jmp     Cnv
C2:   add     @(SP)+,@(SP)
```

```
      Sta
Cnv:  mov     @(SP),-@(SP)
      mov     #0,@1(SP)
      loop
        read    @(Inp)+,X
        sub     #'0,X
        if      lt then exit
;
;
        if      X gt #1 then exit
;
        add     @1(SP),@1(SP)
        add     X,@1(SP)
      endloop
      ret
Inp:  0
Out:  0
X:    0
Sta:  call    Cnv
;
      call    Cnv
;
      add     @(SP)+,@(SP)
```

Obrázek 2.1.3: Kompletní program pro výpočet součtu, první část

vějšího pole vstupní pásky (tj. do pole s číslem 1) zapsán znak `7`. Program může do určitého pole výstupní pásky zapisovat i opakovaně, a to jak (různé) znaky, tak koncovou značku. Program ale nemá možnost číst po sobě znaky, které zapsal na výstupní pásku.

Po provedení instrukce `read` ⟨*op1*⟩`,`⟨*op2*⟩ či `write` ⟨*op1*⟩`,`⟨*op2*⟩, kterým je čten nebo zapisován znak s číselným kódem x, mají bity Z a G tutéž hodnotu, jako kdyby bylo číslo x přenášeno instrukcí `mov`.

Nyní si můžeme podrobněji prohlédnout program na obrázcích 2.1.3 a 2.1.4. Program sečte dvě přirozená čísla, o nichž předpokládá, že jsou na vstupní pásce zapsaná ve dvojkové soustavě a oddělená jedním znakem různým od znaků `0` a `1`. Program užívá buňku `X` jako pomocnou proměnnou. Dále užívá buňky `Inp` a `Out` jako vstupní a výstupní ukazatel, tj. jako ukazatel do vstupní resp. výstupní pásky. Zpočátku každý z ukazatelů ukazuje na nejlevější pole své pásky, tj. na pole s číslem 0.

Program volá „konverzní“ podprogram `Cnv`, od kterého očekává, že určí hodnotu jednoho sčítance a uloží ji na vrchol zásobníku. Protože máme dva sčítance, podprogram `Cnv` je volán dvakrát. Po druhém volání jsou v zásobníku dvě položky (tj. v buňce `SP` je číslo -2). Instrukce `add @(SP)+,@(SP)` na adrese `C2` dělá vlastně

```
      mov     @(SP)+,X                    mov     @(SP)+,X
L2A:                                      loop
      mov     X,-@(SP)                      mov     X,-@(SP)
      shr     X                             shr     X
      sub     X,@(SP)                       sub     X,@(SP)
      sub     X,@(SP)                       sub     X,@(SP)
      add     #‘0,@(SP)                     add     #‘0,@(SP)
      cmp     X,#0                        endloop X eq #0
      jeq     L2C                 ;
      jmp     L2A                 ;
L2C:                              ;
L3A:                                      loop
      write   @(SP)+,@(Out)+                write   @(SP)+,@(Out)+
      cmp     SP,#0                       endloop SP eq #0
      jeq     L3C                 ;
      jmp     L3A                 ;
L3C:  halt                                halt
```

Obrázek 2.1.4: Kompletní program pro výpočet součtu, dokončení

vše podstatné: jednu ze dvou položek ze zásobníku odebere a druhou nahradí jejich součtem. Připomeňme, že `@(SP)` znamená totéž co `@0(SP)`. Nyní se věnujme podprogramu `Cnv`. Podprogram nejprve provede instrukci `mov @(SP),-@(SP)`. Tím je zásobník prodloužen o jednu položku, stále však platí, že na vrcholu je uložena návratová adresa. Výsledek v svého výpočtu čili výstupní parametr podprogram uloží do buňky, kde byla návratová adresa původně a kterou lze nyní adresovat jako `@1(SP)`. Až podprogram svou činnost skončí, tj. až bude návratová adresa ze zásobníku odebrána instrukcí `jmp @(SP)+`, výstupní parametr v se octne na vrcholu zásobníku. Zpočátku platí $v = 0$. Každým provedením instrukce `read @(Inp)+,X` je přečten jeden znak ze vstupní pásky a vstupní ukazatel je přesměrován na následující znak. Zjistí-li se, že právě přečtený znak není číslice `0` ani `1`, čtení znaků končí a vstupní ukazatel je správně nastaven pro případné druhé volání podprogramu `Cnv`. V opačném případě, tj. jestliže byla přečtena číslice, číslo v uložené v buňce `@1(SP)` je pomocí dvou instrukcí `add` nahrazeno číslem $2v$ nebo $2v+1$ podle toho, zda přečtená číslice byla `0` nebo `1`. Podprogram předpokládá, že číselný kód znaku `1` je o jedničku větší než číselný kód znaku `0`. To znamená, že provedením instrukce `sub #‘0,X` je číselný kód znaku `0` nebo `1` převeden na číslo 0 resp. 1.

Poté, co program přečetl oba vstupy a sečetl je instrukcí `add @(SP)+,@(SP)`, provádí „výstupní konverzi“, tj. převádí výstup z číselné do znakové podoby. To je vidět na obrázku 2.1.4. Číslice výsledku jsou nejprve uloženy do zásobníku, a teprve pak, v obráceném pořadí, zapsány na výstupní pásku. Všimněme si ještě, že program nemá žádné nároky na formát vstupních dat: nevadí mu, začíná-li zápis nenulového čísla nulami, prázdnou posloupnost číslic považuje za zápis čísla 0, znaky případně umístěné na vstupní pásce za oběma sčítanci ignoruje.

Činnost programu pracujícího na počítači RASP může skončit provedením instrukce `halt`, ale také detekováním chybového stavu. Chybový stav může například nastat provedením instrukcí `mov #X,Y` a `jmp Y`, neboť pravděpodobně ne každé číslo `X` je strojovým kódem nějaké instrukce. Jiným příkladem chybového stavu je pokus zapsat na výstupní pásku do pole se záporným číslem nebo číst ze vstupní pásky z pole se záporným číslem. Můžeme si představovat, že zastaví-li se procesor provedením instrukce `halt`, na jeho panelu se rozsvítí zelené signální světlo, kdežto zastaví-li se po detekování chyby, na panelu se rozsvítí červené signální světlo. Během práce počítače jsou obě světla zhasnutá. Zastavení procesoru a rozsvícení červeného signálního světla lze z programu dosáhnout provedením instrukce `error`. To je poslední instrukce jazyka RASP, o které jsme se dosud nezmínili. Daný program může instrukci `error` dát libovolný předem dohodnutý význam. Rozsvícení červeného světla může například indikovat nesprávný formát vstupních dat. Má-li program pouze dva možné výstupy (ANO a NE), je také možné stanovit, že na výstupní pásku se nic nezapisuje a že výsledkem činnosti programu je pouze rozsvícení toho nebo onoho signálního světla. V tom případě provedení instrukce `error` neznamená žádnou „chybu“.

Shrňme a nepatrně rozšiřme své poznatky o jazyce RASP a o počítači RASP. Program v jazyce RASP se člení na řádky. Každý řádek může mít tři pole. Pole návěští končí dvojtečkou, pole komentáře začíná středníkem, zbývající (střední) část řádku je pole instrukce. Pole komentáře slouží pouze pro pisatele nebo čtenáře programu, překladač jazyka RASP je ignoruje. Pole instrukce může obsahovat výraz, nebo skutečnou instrukci. Výraz je sestaven z návěští, čísel a výrazů tvaru `‘`⟨*znak*⟩ pomocí znamének. Příklady výrazů jsou `Res-Tab+4`, `‘A+64` nebo `-4`. Je-li v nějakém řádku programu uvedeno návěští a přitom chybí pole instrukce, návěští se vztahuje k nejbližšímu následujícímu řádku s neprázdným polem instrukce. Není-li v poli instrukce výraz, může tam být skutečná instrukce. Výraz se v programu může vyskytnout samostatně, tj. jako jediný obsah pole instrukce, nebo jako součást operandu instrukce. Překladač jazyka RASP převádí výrazy na jejich hodnoty a instrukce na jejich strojové kódy a určuje jim místo v paměti počítače RASP. V jazyce RASP máme celkem třináct instrukcí. Je to osm aritmetických instrukcí, které mohou měnit obsah paměti i podmínkové bity, nemohou ale měnit čítač instrukcí v tom smyslu, že po provedení aritmetické instrukce je vždy provedena ta instrukce, která v paměti bezprostředně následuje. Dále máme tři skokové instrukce, ty mohou měnit čítač instrukcí, nemění ale podmínkové bity a nemění ani obsah paměti až na výjimku, že při vyhodnocení vzdáleného operandu takové instrukce může dojít ke zvětšení nebo zmenšení obsahu určité paměťové buňky o jedničku. A konečně máme instrukce `halt` a `error`. Dvě posledně jmenované instrukce jsou instrukce bez operandů, instrukce `add`, `sub`, `cmp`, `mov`, `read` a `write` jsou instrukce se dvěma operandy, zbývající instrukce `neg`, `shr`, `jeq`, `jgt` a `jmp` mají jeden operand. Operandy jsou přímé, běžné a vzdálené. Operand jednooperandové instrukce a druhý operand dvouoperandové instrukce musí být běžný nebo vzdálený s výjimkou instrukce `cmp`, jejíž druhý operand může být i přímý. První operand dvouoperandové instrukce může být libovolný s výjimkou instrukce `read`,

jejíž první operand může být pouze běžný nebo vzdálený. Překladač jazyka RASP převádí výrazy na jejich hodnoty a instrukce na jejich strojové kódy a určuje jim místo v paměti počítače RASP. Činnost programu začíná přenesením obsahu paměťové buňky `0` do čítače instrukcí a jejím vynulováním. Činnost programu končí provedením jedné z instrukcí `halt` nebo `error` nebo detekováním chybového stavu. Pro určitost definujme, že v okamžiku startu počítače jsou oba podmínkové bity nulové a že instrukce `halt` a `error` podmínkové bity nemění. Není zaručeno, že každý program při zpracování libovolných dat někdy skončí. Například program z obrázku 2.1.1 dospěje k výsledku právě tehdy, je-li počáteční obsah buňky `X` nezáporný. V opačném případě program pracuje donekonečna, tj. *zacyklí se*. Počítač RASP pracuje s čísly, s okolím ale komunikuje pomocí znaků zapsaných na vstupní a výstupní pásce a pomocí dvou signálních světel. Obsah vstupní pásky se během činnosti programu nemění.

Označení RASP jsme převzali z knihy [1]. V této knize se kromě počítače RASP užívá také (hlavně) počítač RAM (*random access machine*). Modely RAM a RASP mají tutéž množinu instrukcí, liší se ale tím, že program počítače RAM není uložen v paměti. Pro model RASP jsme se rozhodli proto, že implementace volání podprogramů, kterou považujeme za dost důležitou, by na počítači RAM byla mnohem méně přirozená. Počítače RAM se uvažují také v knihách [62] a [52]. Na rozdíl od všech tří knih jsme připustili, aby aritmetické operace probíhaly ve všech paměťových buňkách, nikoli jen v jedné k tomu určené. Připustili jsme také paměť se zápornými adresami. Ani jedno totiž nic nestojí a přitom to značně usnadňuje programování. Stejně jako v knize [62] a na rozdíl od knih [1] a [52] jsme mezi instrukce jazyka nepřijali instrukce pro násobení a dělení. Ty by totiž nic podstatného nepřinesly, ale komplikovaly by úvahy, které povedeme dále, o časové a paměťové náročnosti úloh a programů.

V pravých částech obrázků 2.1.2, 2.1.3 a 2.1.4 jsou tytéž programy přepsány s použitím „konstruktů“ `call`, `if`–`endif` a `loop`–`endloop`. Tyto konstrukty nejsou novými instrukcemi, nýbrž textovými zkratkami, pod nimiž se skrývají fragmenty programů, tj. instrukce a návěští. Takovýmto textovým zkratkám se zpravidla říká *makra*. Užití maker může někdy zkrátit zápis programu, jejich hlavní význam je ale v tom, že naznačují „logiku programu“, čili zpřehledňují význam skokových instrukcí. Značně také omezují potřebu návěští. O textu, který se skrývá pod určitým makrem, říkáme, že je oním makrem generován. Nadále budeme makra při psaní programů hojně využívat a budeme se spoléhat na to, že čtenář, který si pečlivě prohlédl obrázky 2.1.2 až 2.1.4, dovede kterýkoliv program obsahující makra přepsat na program bez maker.

Vysvětleme si nyní podrobněji syntax a význam (některých) maker. Nejprve se zabývejme makrem `if`. Podmínka ⟨*cnd*⟩ umístěná mezi `if` a `then` může mít tvar ⟨*op1*⟩ ⟨*rel*⟩ ⟨*op2*⟩ nebo tvar ⟨*rel*⟩. Jako „relační znaménko“ ⟨*rel*⟩ se připouštějí mnemoniky `gt` a `eq`, které jsou opsány z mnemonik podmíněně skokových instrukcí, dále k nim komplementární mnemoniky `le` (*less or equal*, menší nebo rovno) a `ne` (*not equal*, nerovno), a konečně `lt` (*less than*, menší než) a `ge` (*greater or equal*, větší nebo rovno). Makro `if` generuje jednu až tři skokové instrukce a případně

```
      loop                                  ; Všechny znaky
        read    @(Inp)+,X                   ; Přečti další znak
        if      lt  then exit               ; Koncová značka
        mov     X,-@(SP)                    ; Vše kromě pravé závorky
        if      X ne #‘)  then repeat       ; pouze ulož do zásobníku
        add     #1,SP                       ; Odeber pravou závorku
        if      @3(SP) ne #‘(  then error  ; Zkontroluj uložené
        if      @2(SP) ne #‘0  then         ; znaky
          if      @2(SP) ne #‘1  then error
        endif
        mov     @(SP)+,X                    ; Pravý operand
        mov     @(SP)+,Op                   ; Znaménko operace
        if      X eq #‘0  then
          if      Op eq #‘+  then goto Res ; 0+x=x
          if      Op ne #‘*  then error
          mov     #‘0,@(SP)                 ; 0*x=0
        else                                ; Pravý operand není nula
          if      X ne #‘1   then error     ; Musí to být jednička
          if      Op eq #‘*  then goto Res ; 1*x=x
          if      Op ne #‘+  then error
          mov     #‘1,@(SP)                 ; 1+x=1
        endif
Res:    mov     @(SP)+,@(SP)                ; Jeden znak místo pěti
      endloop                               ; Po zpracování
      if      SP ne #-1  then error         ; vstupu musí být v zá-
      if      @(SP) eq #‘0  then goto Done ; sobníku jediný znak,
      if      @(SP) ne #‘1  then error      ; nula nebo jednička,
Done: write   @(SP)+,0                      ; který je výsledkem
      halt
```

Obrázek 2.1.5: Výpočet hodnoty booleovského výrazu

jedno návěští. Má-li podmínka ⟨*cnd*⟩ složitější tvar ⟨*op1*⟩ ⟨*rel*⟩ ⟨*op2*⟩, makro `if` generuje ještě instrukci `cmp` ⟨*op1*⟩`,`⟨*op2*⟩. V opačném případě, má-li podmínka ⟨*cnd*⟩ tvar pouze ⟨*rel*⟩, se předpokládá, že podmínkové bity byly nastaveny instrukcemi předcházejícími řádek s makrem `if`. Mezi `if` a `endif` může, ale nemusí být použito `else`. Kdyby mezi `if` a `endif` nebylo `else` a byl by tam pouze jeden řádek, je povoleno psát jednořádkový `if` s instrukcí zapsanou za `then` a bez užití makra `endif`.

Makra `loop` a `endloop` vymezují cyklus. Za `loop` i za `endloop` může následovat podmínka ⟨*cnd*⟩ téhož tvaru jako v makru `if`. Na rozdíl od makra `if` je jak podmínka za `loop`, tak podmínka za `endloop` nepovinná. Podmínka za `loop` je podmínkou pro vstup do cyklu, podmínka za `endloop` je podmínkou pro opuštění cyklu. Dvojice `loop` a `endloop` ⟨*cnd*⟩ odpovídá konstruktu `repeat`–`until` v jazyce

```
Get:  mov     @(SP),-@(SP)                ; Posuň návratovou adresu
      read    @(Inp)+,@1(SP)              ; V @1(SP) bude výsledek
      if      @1(SP) eq #‘0  then  ret    ; Hotovo, když jen
      if      @1(SP) eq #‘1  then  ret    ; jedna číslice
      if      @1(SP) ne #‘(  then  error  ; Jinak je nutná závorka
      call    Get                         ; Čti levý podvýraz,
      read    @(Inp)+,-@(SP)              ; operační znaménko
      call    Get                         ; a pravý podvýraz
      if      @1(SP) eq #‘+ then          ; Logický součet
        if      @0(SP) eq #‘1  then  mov #‘1,@2(SP)
      else                                ; Logický součin
        if      @1(SP) ne #‘*  then  error ; nebo nesprávný formát
        if      @0(SP) eq #‘0  then  mov #‘0,@2(SP)
      endif
      read    @(Inp)+,-@(SP)              ; Následovat musí
      if      @(SP)+ ne #‘)  then  error  ; pravá závorka
      add     #2,SP                       ; Dvě položky už zbytečné
      mov     @(SP)+,@1(SP)               ; třetí je výsledek
      ret                                 ; Hotovo, zpět
Sta:  call    Get                         ; Přečti celý výraz
      read    @(Inp)+,-@(SP)              ; Následovat musí
      if      @(SP)+ ge #‘0  then  error  ; koncová značka
      write   @(SP)+,0                    ; Zapiš výsledek
      halt                                ; Hotovo
```

Obrázek 2.1.6: Hodnota booleovského výrazu pomocí rekurzívního volání

Pascal. Dvojice `loop` ⟨*cnd*⟩ a `endloop` (bez podmínky) odpovídá konstruktu `while`. V cyklu mezi `loop` a `endloop` se může vyskytnout konstrukt `exit`, kterým lze nařídit předčasné opuštění cyklu, a konstrukt `repeat`, kterým lze naopak nařídit opakování cyklu od počátku. Konstruktu `repeat` tedy přisuzujeme zcela jiný význam, než má v jazyce Pascal. Konstrukty `exit` a `repeat`, a rovněž `goto`, se mohou vyskytnout také za `then` v jednořádkovém `if`. Význam maker `call` a `ret` je z obrázků 2.1.3 a 2.1.4 zřejmý.

Program z obrázku 2.1.5 určuje hodnotu booleovského výrazu. V zápisu programu jsme vynechali řádky, které si čtenář jistě umí představit: deklaraci startovací adresy a alokaci pomocných buněk `X`, `Op` a `Inp`. Program pracuje tak, že všechny znaky booleovského výrazu zapsaného na vstupní pásce beze změny ukládá do zásobníku a pozastaví se pouze v případě, kdy přečtený znak je pravá závorka. V tom okamžiku musí platit, že pět nejvyšších položek na vrcholu zásobníku jsou znaky levá závorka, číslice `0` nebo `1`, znaménko `+` nebo `*`, číslice `0` nebo `1`, a pravá závorka. Není-li tomu tak, program skončí činnost provedením instrukce `error`. Je-li tomu tak, program těchto pět znaků nahradí znakem `0` nebo `1`, a pak pokračuje ve čtení vstupního výrazu.

Program z obrázku 2.1.6 také určuje hodnotu booleovského výrazu, postupuje ale jinak než program z obr. 2.1.5, užívá *rekurzívní volání podprogramů*. Program začíná svou činnost na adrese `Sta`, znaky ze vstupní pásky jsou opět čteny pomocí ukazatele `Inp`. Od podprogramu `Get` se očekává, že určí hodnotu výrazu, na jehož nejlevější znak ukazuje buňka `Inp`, uloží ji do zásobníku a přesměruje ukazatel `Inp` těsně za onen výraz. Pokud se po volání umístěném na adrese `Sta` zjistí, že na vstupní pásce jsou ještě další (nadbytečné) znaky, program ohlásí chybu provedením instrukce `error`. Pokud podprogram `Get` zjistí nesprávný formát booleovského výrazu, nevrací žádný chybový parametr, nýbrž sám provede instrukci `error`. Podprogram `Get` začíná svou činnost podobně jako podprogram `Cnv` z obrázku 2.1.3, posunutím návratové adresy utvoří v zásobníku prostor pro uložení svého výstupního parametru a přečte jeden znak ze vstupní pásky. Pokud je přečtený znak číslice `0` nebo `1`, nemusí dělat již nic dalšího. V opačném případě by na pásce měl být zapsán složený výraz, který sestává ze dvou podvýrazů spojených znakem `+` nebo `*` a obklopených závorkami. Hodnoty obou podvýrazů zjistí dvojnásobným voláním podprogramu `Get`, čili rekurzívním voláním sebe sama. Po druhém volání podprogramu `Get` v osmém řádku programu, a to až do provedení instrukce `add #2,SP`, lze hodnoty obou podvýrazů adresovat jako `@2(SP)` a `@0(SP)`, kdežto `@1(SP)` je operační znaménko. Zbytek je podobný jako v programu z obr. 2.1.5.

Nyní směřujme k definici počitatelnosti úloh a k definici časových a paměťových nároků programu. Víme, že pouze konečný počáteční úsek vstupní pásky obsahuje znaky a že celý zbývající úsek vstupní pásky je vyplněn koncovými značkami. Slovu zapsanému v onom počátečním úseku říkejme *vstup programu*, délka tohoto slova je *délka vstupu*. Délka vstupu w je tedy nejmenším číslem n takovým, že v poli s indexem n a všech dalších polích vstupní pásky jsou koncové značky. Výstupní páska je zpočátku prázdná, tj. obsahuje samé koncové značky, obsah některých polí ale program během své činnosti může změnit. V okamžiku, kdy se program zastaví (a rozsvítí některé signální světlo), jsou jen v konečně mnoha polích výstupní pásky zapsány znaky. V každém taktu totiž program mohl změnit obsah nejvýše jednoho pole. Zastaví-li se program provedením instrukce `halt`, pak za *výstup programu* pokládáme slovo, které je v tom okamžiku na výstupní pásce zapsáno vlevo od nejlevějšího pole obsahujícího koncovou značku. Nevylučujeme, že vpravo od tohoto pole jsou na výstupní pásce zapsány ještě další znaky; ty ale k výstupu nepočítáme. Zastaví-li se program rozsvícením červeného světla (tj. provedením instrukce `error` nebo detekováním chybového stavu), nebo nezastaví-li se vůbec (tj. zacyklí-li se), pokládáme výstup programu za nedefinovaný.

Nechť Σ_1 a Σ_2 jsou abecedy a nechť $X \subseteq \Sigma_1^*$ a $g : X \to \Sigma_2^*$. Řekneme, že *program P počítá funkci g*, jestliže (i) program P při zpracování libovolného vstupu $w \in \Sigma_1^*$ poskytne výstup právě tehdy, platí-li $w \in X$, a (ii) pokud to nastane, je výstupem slovo $g(w)$. Program P je tedy povinen dát výstup $g(w)$, kdykoliv $w \in X$, a nedat žádný výstup (tj. zastavit se rozsvícením červeného signálního světla nebo se nezastavit vůbec), platí-li $w \in \Sigma_1^* - X$. Řekneme, že *funkce g* z X do Σ_2^* je *počitatelná (na počítači RASP)*, existuje-li program v jazyce RASP, který ji počítá.

Například program z obrázku 2.1.5 počítá funkci definovanou na množině všech booleovských výrazů, která každému booleovskému výrazu přiřazuje jeho hodnotu. Je snadné pozměnit tento program na program počítající funkci (úlohu) HODNOTA BOOLEOVSKÉHO VÝRAZU definovanou v úvodu této kapitoly. Znamená to upravit jej tak, aby místo provedení kterékoliv ze svých instrukcí `error` zapsal do nultého pole výstupní pásky dohodnutý znak (v úvodu kapitoly to byl znak `n`), a pak provedl instrukci `halt`. Dále nevelkou úpravou programu z obrázků 2.1.3 a 2.1.4 lze získat program, který počítá funkci $[x, y] \mapsto x + y$, tj. který počítá součet přirozených čísel. Znamená to zapracovat do něj kontrolu, která připustí pouze vstupy tvaru $w_1;w_2$, kde w_1 a w_2 jsou binární zápisy přirozených čísel, a odmítne (provedením instrukce `error`) všechny ostatní vstupy. Přidáme-li k programu z obrázku 2.1.1 nebo k programu z obrázku 2.1.2 kontrolu formátu vstupních dat a vstupní a výstupní konverze, dostaneme v obou případech program, který počítá součin přirozených čísel. Programy (přesněji řečeno fragmenty programů či algoritmy) z obrázků 2.1.1 a 2.1.2 tedy představují dvě různá zdůvodnění, proč NÁSOBENÍ je funkce počitatelná na počítači RASP. Několik dalších počitatelných funkcí je uvedeno ve cvičeních.

Nechť P je program a nechť f je funkce z N do N. Řekneme, že *program P pracuje v čase f*, jestliže při zpracování libovolného vstupu délky nejvýše n se program P zastaví po provedení nejvýše $f(n)$ kroků. Řekneme, že úloha $g : X \to \Sigma_2^*$, kde $X \subseteq \Sigma_1^*$, je *počitatelná (na počítači RASP) v čase f*, jestliže existuje program, který ji počítá a který pracuje v čase f.

Například v podprogramu `Cnv` na obrázku 2.1.3 je cyklus, tj. vícenásobně prováděná sekvence instrukcí omezená makry `loop` a `endloop`. Při zpracování vstupu délky n se tento cyklus provádí $(n + 1)$-krát (naposled při přečtení první koncové značky za vstupním slovem). To znamená, že každá z deseti instrukcí cyklu se provede nejvýše $(n + 1)$-krát. Výstup programu má nejvýše $(n + 1)$ znaků (normálně je jich nejvýše $n - 1$, pouze při zpracování prázdného vstupu jich je $n + 1$). To znamená, že také každá z nejvýše dvanácti instrukcí dvou cyklů hlavního programu (na obr. 2.1.4) se provádí nejvýše $(n + 1)$-krát. V podprogramu `Cnv` jsou tři instrukce umístěné mimo cyklus a každá z nich se provádí dvakrát, v hlavním programu je sedm instrukcí umístěných mimo oba cykly. Dohromady se tedy provede nejvýše $10(n + 1) + 12(n + 1) + 6 + 7$ instrukcí. Tím jsme zdůvodnili, že náš program pro výpočet součtu počítá v čase f, kde $f(n) = 22n + 35$. V dalším výkladu budeme pokud možno dodržovat zvyklost, že počet znaků vstupu se značí n a že funkce vyjadřující časové nebo paměťové nároky programu se zapisuje výrazem (v n). Náš program tedy pracuje v čase $22n + 35$.

Také časové nároky programu z obr. 2.1.5 lze snadno odhadnout: v programu je 49 instrukcí a při zpracování vstupu délky n se každá z nich provede nejvýše $(n + 1)$-krát. Program tedy pracuje v čase $49(n + 1)$. V obou případech by šlo počítat i precizněji. To ale nemáme v úmyslu. Naopak, v dalším textu se většinou nebudeme zajímat o přesnou hodnotu multiplikativních konstant a spokojíme se také s odhady, které platí až na konečně mnoho výjimek. Pro tento účel jsme v oddílu 1.3 (viz str. 36) zavedli tuto definici: funkce f je v $\mathcal{O}(g)$, jestliže existuje

konstanta c taková, že $f(n) \leq c \cdot g(n)$ pro všechna dost velká n. Zatím jsme tedy zjistili, že jak náš program pro výpočet součtu, tak program z obr. 2.1.5 pro výpočet hodnoty booleovského výrazu pracuje v čase (f, kde f je funkce v) $\mathcal{O}(n)$. Na tomto tvrzení by se nic nezměnilo, kdybychom programy upravili tak, jak je naznačeno výše, tj. kdybychom do programu pro sčítání zapracovali kontrolu formátu vstupních dat a kdybychom program z obr. 2.1.5 upravili tak, aby se vždy dopracoval k rozsvícení zeleného světla. Jak součet přirozených čísel, tak určování hodnoty booleovského výrazu jsou tedy funkce počitatelné na počítači RASP v *lineárním čase*.

Když v binárním zápisu čísla x je n cifer, může být potřeba až $2^n - 1$ odčítání jedničky, než je x přepracováno na nulu. To znamená, že kdybychom fragment programu uvedený na obr. 2.1.1 doplnili na kompletní program, o výsledném programu počítajícím funkci $[x, y] \mapsto x \cdot y$ bychom nemohli říci nic lepšího, než že pracuje v čase 2^n. Protože funkce $n \mapsto 2^n$ roste dosti rychle, rychleji než všechny funkce tvaru $n \mapsto n^k$ (tj. rychleji než všechny polynomy), program pro výpočet součinu přirozených čísel založený na algoritmu z obr. 2.1.1 nelze považovat za příliš efektivní.

Je-li naproti tomu v buňce `X` číslo, jehož zápis má n cifer, dospějeme již po n-násobném provedení instrukce `shr X` k nule. Cyklus v algoritmu na obrázku 2.1.2 se tedy provádí pouze tolikrát, kolik cifer je v zápisu prvního činitele x. Kdybychom tento algoritmus doplnili na kompletní program přidáním kontroly formátu vstupních dat a vstupních a výstupních konverzí, dostali bychom program pro výpočet součinu přirozených čísel, který pracuje v čase $\mathcal{O}(n)$. Díky algoritmu z obr. 2.1.2 tedy můžeme tvrdit, že úloha NÁSOBENÍ je na počítači RASP počitatelná v lineárním čase. Algoritmus z obrázku 2.1.1 není pro tento účel nijak užitečný.

Přikročme k úvahám o prostorové (paměťové) náročnosti programů a úloh. Nejprve definujme funkci ℓ z N do N předpisem $\ell(x) = \lceil \log(x+1) \rceil$, kde log je dvojkový logaritmus a $z \mapsto \lceil z \rceil$ je horní celá část, tj. funkce, která každému (řekněme reálnému) číslu z přiřadí nejmenší celé číslo j takové, že $z \leq j$. Funkce ℓ se nazývá *délková funkce* nebo také *celočíselný logaritmus*. Je-li $x \in \mathrm{N}$ a $x > 0$, pak $\ell(x)$ udává počet cifer v binárním zápisu čísla x. Místo $\ell(x)$ se v literatuře často píše $|x|$ (což je v souladu s označením $|w|$ pro délku slova w). Toho se ale držet nebudeme, označení $|x|$, je-li x číslo, si vyhradíme pro absolutní hodnotu čísla x.

Definujme *konfiguraci* počítače RASP jako slovo tvaru

$$d_1 d_2 d_3 d_4 b \texttt{,} a \texttt{,} c_1 \texttt{,} \ldots \texttt{,} c_k, \qquad (*)$$

kde d_1 až d_4 jsou číslice `0` nebo `1`, slova b, a a $c_2, \ldots, c_{k-1}$ jsou binární zápisy celých čísel a slova c_1 a c_k jsou binární zápisy nenulových celých čísel. Konfigurace je tedy slovem v abecedě $\{\texttt{-}, \texttt{,}, \texttt{0}, \texttt{1}\}$, přičemž minus slouží k zapisování záporných čísel a čárka slouží k oddělování čísel od sebe. Jednotlivé části konfigurace interpretujeme následovně. Číslice d_1 (číslice d_2) je `1` právě tehdy, je-li rozsvíceno zelené resp. červené signální světlo. Číslice d_3 a d_4 udávají hodnoty podmínkových bitů Z a G. Slovo b udává hodnotu čítače instrukcí, slovo c_1 udává obsah paměťové buňky, jejíž adresu udává slovo a, slova $c_2, \ldots, c_k$ udávají obsahy $(k-1)$ bezprostředně následujících paměťových buněk. O ostatních paměťových buňkách (s adresami nižšími

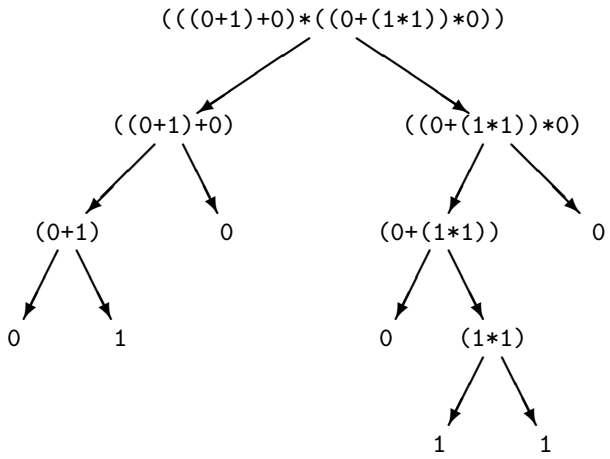
než a a vyššími než $a + k - 1$) se rozumí, že obsahují nuly. Celá konfigurace tedy udává informaci o stavu počítače RASP v určitém okamžiku jeho činnosti. Je-li C konfigurace tvaru $(*)$, pak slovem C a obsahem w vstupní pásky je jednoznačně určeno, co v daném okamžiku počítač udělá: neudělá nic, má-li některý z bitů d_1 a d_2 hodnotu 1 (v tom případě došlo k zastavení počítače už v konfiguraci C), nebo přejde do jednoznačně určené konfigurace D, která se od konfigurace C může lišit v hodnotách bitů d_1 až d_4, v hodnotě čítače instrukcí a dále v obsahu nejvýše tří paměťových buněk (neboť každá instrukce modifikuje obsah nejvýše jedné paměťové buňky, ale při vyhodnocení případných vzdálených operandů může být obsah dalších nejvýše dvou paměťových buněk zvětšen nebo zmenšen o jedničku). Takto jednoznačně určené konfiguraci D říkejme konfigurace *odvozená* z konfigurace C a z obsahu w vstupní pásky. Konfiguraci, ve které má některý z bitů d_1 a d_2 hodnotu 1 (takže neexistuje konfigurace z ní odvozená), říkejme *koncová* konfigurace. Definujme konfiguraci *počáteční* vzhledem k programu P jako konfiguraci, ve které jsou bity $d_1, \ldots, d_4$ nulové, čítač instrukcí má tu hodnotu, kterou překladač při překladu programu P uložil na adresu `0`, adresa `0` má nulový obsah a všechny ostatní paměťové buňky mají ten obsah, který jim určil překladač při překladu programu P. Řekneme, že posloupnost $C_0, \ldots, C_m$ konfigurací je *výpočet programu P ze vstupu w*, jestliže C_0 je konfigurace počáteční vzhledem k programu P, každá konfigurace C_{i+1} je odvozená z konfigurace C_i a slova w a konfigurace C_m je koncová. Všimněme si, že je-li $C_0, \ldots, C_m$ výpočet programu ze vstupu w, pak číslo m je počet kroků, které počítač vykonal při zpracování vstupu w. Dále si všimněme, že připouštíme pouze výpočty, které skončily zastavením procesoru. „Výpočet“, který probíhal donekonečna, neuznáváme za výpočet.

Nechť $C_0, \ldots, C_m$ je výpočet programu P ze vstupu w. Definujme *velikost paměti použité programem P při zpracování vstupu w* jako číslo $\max_i |C_i|$. Délku konfigurace tedy pokládáme za velikost paměti použité programem v příslušném kroku výpočtu, celkovou velikost paměti použité při zpracování vstupu w definujeme jako maximální velikost paměti použité v kterémkoliv kroku výpočtu. Nechť P je program a nechť f je funkce z N do N. Řekneme, že *program P pracuje v prostoru f*, jestliže pro každé n platí, že program P se dopočítá při zpracování libovolného vstupu délky nejvýše n a použije při tom paměť velikosti nejvýše $f(n)$. Řekneme, že úloha $g : X \to \Sigma_2^*$, kde $X \subseteq \Sigma_1^*$, je *počitatelná (na počítači RASP) v prostoru f*, jestliže existuje program, který ji počítá a který pracuje v prostoru f.

Vraťme se znovu k programu pro výpočet součtu z obrázků 2.1.3 a 2.1.4. Předpokládejme, že programu je předložen vstup tvaru $w_1\,;w_2$, kde w_1 a w_2 jsou binární zápisy čísel x a y. Nechť délka tohoto vstupu je nejvýše n. V okamžiku před provedením instrukce `add @(SP)+,@(SP)` jsou v zásobníku uloženy dvě položky, x a y, nejnižší paměťová buňka s nenulovým obsahem má adresu -2, číslo -2 je také v buňce `SP` čili v buňce `0`, a v buňce `Inp` je číslo $n + 1$. Počítač se tedy nachází v konfiguraci tvaru

$$\ldots,\texttt{-10},w_2,w_1,\texttt{-10},\ldots,w_3,\ldots,$$

kde w_3 je binární zápis čísla $n + 1$ uloženého v buňce `Inp`. Platí $|w_1| + |w_2| \leq n$



Obrázek 2.1.7: Rekurzívní volání podprogramu

a $|w_3| = \ell(n+1) \leq \ell(n)+1$. Souhrnná délka všech ostatních částí konfigurace (naznačených tečkami) nezávisí na n. Druhé maximum, pokud jde o velikost obsazené paměti, nastane v okamžiku před prvním provedením instrukce `write`. Tehdy jsou v zásobníku uloženy číselné kódy všech znaků, které mají být zapsány na výstupní pásku. Znamená to nejvýše n čísel, jejichž binární zápisy mají souhrnnou délku nejvýše $c \cdot n$, kde konstanta c je dána kódovou tabulkou. Protože funkce $c \cdot n$, n i $\ell(n)+1$ jsou v $\mathcal{O}(n)$ (i jejich součet je v $\mathcal{O}(n)$), můžeme říci, že program pracuje v prostoru $\mathcal{O}(n)$. Funkce sčítání přirozených čísel je tedy na počítači RASP počitatelná v *lineárním prostoru*.

Podobnou analýzou programu z obr. 2.1.5 lze ověřit, že také úloha Hodnota booleovského výrazu je počitatelná v lineárním prostoru. I úloha Násobení je počitatelná v lineárním prostoru a je přitom jedno, zda si pro analýzu paměťových nároků vybereme algoritmus z obr. 2.1.2 nebo časově mnohem méně efektivní algoritmus z obr. 2.1.1.

Také program z obrázku 2.1.6 pracuje v prostoru $\mathcal{O}(n)$. Protože s podobnými programy, založenými na rekurzívním volání podprogramů, se ještě setkáme, zdůvodněme tento fakt raději podrobněji. Předpokládejme, že programu je ke zpracování předložen výraz w délky n. K určení hodnoty výrazu w program volá podprogram `Get`. Podprogram `Get` při každém svém volání přečte jeden znak ze vstupní pásky a má za úkol stanovit hodnotu podvýrazu výrazu w, který začíná oním znakem. Než to udělá, může dojít k dalším (vnořeným) voláním podprogramu `Get`. V každém okamžiku výpočtu tedy může být rozpracováno několik „kopií“ podprogramu `Get`. Celý výpočet si můžeme představit jako strom, jehož vrcholům odpovídají jednotlivé kopie. Z vrcholu v_1 vede hrana do vrcholu v_2, jestliže kopie odpovídající vrcholu v_2 je volána z kopie odpovídající vrcholu v_1. Pro případ, kdy vstupní výraz w je `(((0+1)+0)*((0+(1*1))*0))`, je tento strom znázorněn na obr. 2.1.7. Pro stanovení hodnoty výrazu w je třeba znát hodnoty

```
GLE:  read    -@(Aux),X                    ; Vezmi předchozí znak
      if      X eq #‘0 then ret            ; Hotovo, je-li to
      if      X eq #‘1 then ret            ; 0 nebo 1
      if      X ne #‘) then error          ; Jinak to musí být )
      mov     #1,Dp                        ; Inicializuj hloubku
      loop                                 ; Jdi doleva
        read    -@(Aux),X                  ; a nalezni
        if      X eq #‘) then add #1,Dp    ; levou závorku,
        if      X eq #‘( then sub #1,Dp    ; která je
      endloop Dp eq #0                     ; v patřičné hloubce
      ret
Sta:  loop
        mov     Ptr,Aux                    ; Přečti další znak
        read    @(Ptr)+,X                  ; Aux ukazuje na,
        if      lt then exit               ; Ptr za onen znak
        if      v X je kód jednoho ze znaků (, +, *, 0, 1  then repeat
        if      X ne #‘) then error        ; Když ), najdi
        call    GLE                        ; začátek 2. podvýrazu
        read    -@(Aux),X                  ; Vlevo musí být + nebo *
        if      v X není kód znaku + ani *  then error
        call    GLE                        ; Začátek 1. podvýrazu
        read    -@(Aux),X                  ; Vlevo musí být
        if      X ne #‘( then error        ; levá závorka
      endloop
      call    GLE                          ; Levý konec celku
      if      Aux ne #0 then error         ; musí být v poli nula
      halt
```

Obrázek 2.1.8: Paměťově úsporné rozpoznávání booleovských výrazů

výrazů `((0+1)+0)` a `((0+(1*1))*0)`, pro stanovení hodnoty výrazu `((0+1)+0)` je třeba znát hodnoty výrazů `(0+1)` a `0` atd.

V době, kdy je volána kopie odpovídající vrcholu v, jsou ještě rozpracovány kopie odpovídající vrcholům ležícím na cestě z kořenu stromu do vrcholu v. Paměťový prostor, který je v tomto okamžiku obsazen, lze odhadnout jako součet velikostí „lokálních dat“ všech těchto kopií. Lokální data každé kopie sestávají ze dvou nebo tří položek uložených v zásobníku: paměťová buňka adresovaná jako `@1(SP)` je rezervována pro budoucí výsledek činnosti podprogramu, druhá položka je návratová adresa, případná třetí je dílčí výsledek získaný prvním voláním vnořené kopie. Každá z těchto položek je omezená konstantou, rozpracovaných kopií je nejvýše n. Program z obr. 2.1.6 tedy opravdu pracuje v prostoru $\mathcal{O}(n)$. Do budoucna si pamatujme, že výpočet podprogramu, který rekurzívně volá sám sebe, si lze přestavit jako průchod stromem, jehož vrcholy odpovídají různým kopiím tohoto podprogramu. Čas potřebný pro výpočet souvisí s celkovým počtem

vrcholů ve stromu, prostor potřebný pro výpočet souvisí s délkou nejdelší větve stromu. U programu z obr. 2.1.6 ale mezi počtem vrcholů a maximální délkou větve není velký rozdíl, obojí je odhadnuto číslem n a žádný podstatně lepší odhad neexistuje.

Má-li vstup w nějakého programu P délku n, potřebuje program P nejméně n kroků, aby přečetl všechny znaky slova w. Z tohoto důvodu budeme tvrzení, že určitý program P pracuje v čase $\mathcal{O}(n)$, pokládat za maximum toho, čeho lze dosáhnout. O programy, jejichž časové nároky rostou pomaleji než lineárně, nebudeme usilovat. Na druhé straně může být někdy užitečné a žádoucí napsat program, jehož *prostorové* nároky jsou výrazně menší než lineární. Příklad takového programu je na obrázku 2.1.8. Tento program o každém slově $w \in \{\texttt{(}, \texttt{)}, \texttt{+}, \texttt{*}, \texttt{0}, \texttt{1}\}^*$ rozhodne, je-li booleovským výrazem. Na rozdíl od programů z obrázků 2.1.5 a 2.1.6 se ale nezabývá *hodnotami* booleovských výrazů. Program čte ze vstupní pásky znaky jeden po druhém, ale v každém okamžiku má v paměti pouze jeden znak vstupního slova w. Vždy, když narazí na pravou závorku, hledá *k ní příslušnou* levou závorku. Udělá to tak, že si uloží jedničku do buňky `Dp`, jde doleva, při každém výskytu pravé závorky k buňce `Dp` přičítá jedničku, při každém výskytu levé závorky od buňky `Dp` odečítá jedničku. „Příslušná“ levá závorka se vyznačuje tím, že je-li v souvislosti s jejím přečtením odečtena jednička od buňky `Dp`, poprvé dojde k tomu, že výsledek je nula. Označme i obsah buňky `Ptr`. Tvrdíme, že vždy v okamžiku provedení instrukce `mov Ptr,Aux` platí: *ke každé pravé závorce umístěné na vstupní pásce v poli s indexem menším než i existuje někde vlevo od ní k ní příslušná levá závorka a tyto dvě závorky spolu se znaky umístěnými mezi nimi tvoří booleovský výraz.* Toto tvrzení lze snadno dokázat indukcí podle i. Dále lze ověřit, že řekne-li program NE, tj. provede-li kteroukoliv ze svých pěti instrukcí `error`, nebo pokusí-li se číst z pole se záporným indexem (čili „spadne z pásky“), pak má pravdu, vstupní slovo w skutečně není booleovským výrazem (viz též cvičení 6–8). Je-li přečtena koncová značka a předchozí znak byla pravá závorka, program prostřednictvím posledního volání podprogramu `GLE` (get left end) nalezne k ní příslušnou levou závorku. I v tomto okamžiku ovšem platí, že tyto dvě závorky spolu s textem mezi nimi tvoří booleovský výraz. Je-li příslušná levá závorka v poli s indexem nula, program skončí provedením instrukce `halt`. A opět má pravdu, celé vstupní slovo w je booleovským výrazem.

Tento program je napsán tak, že nic nezapisuje na výstupní pásku a odpověď ANO či NE (daný vstup je či není booleovským výrazem) dá najevo rozsvícením zeleného resp. červeného signálního světla. Snadno bychom jej ale upravili tak, aby žádný výpočet nekončil rozsvícením červeného světla a aby odpověď ANO či NE dal program najevo zápisem (třeba jednoznakových slov `a` či `n`) na výstupní pásku. Takováto úprava by nic (podstatného) neměnila na jeho časových a paměťových nárocích.

V dalším textu se často spokojíme s tím, že místo programu podáme pouze neformální algoritmus, a budeme se spoléhat na to, že čtenář by jej dovedl přepsat do jazyka RASP. Algoritmus pro rozpoznávání booleovských výrazů, tj. neformální verze programu z obr. 2.1.8, může vypadat například takto:

S užitím hlavního ukazatele Ptr čti znaky jeden po druhém, pozastav se pouze u pravé závorky a u koncové značky. Ostatní přípustné znaky jsou `(`, `+`, `*`, `0`, `1`, ty pouze zkontroluj.

Je-li přečtený znak pravá závorka, pak užij pomocný ukazatel Aux, a

- ukaž si na těsně předchozí znak. Není-li to `0` ani `1`, musí to být pravá závorka. V tom případě si ukaž na k ní příslušnou levou závorku.
- ukaž si na těsně předchozí znak. Musí to být `+` nebo `*`.
- ukaž si na těsně předchozí znak. Není-li to `0` ani `1`, musí to být pravá závorka. V tom případě si ukaž na k ní příslušnou levou závorku.
- ukaž si na těsně předchozí znak. Musí to být levá závorka.

Je-li přečtena koncová značka, pak

- ukaž si na těsně předchozí znak. Není-li to `0` ani `1`, musí to být pravá závorka. V tom případě si ukaž na k ní příslušnou levou závorku.
- zkontroluj, že ukazatel nyní ukazuje na nulté pole vstupní pásky, a skonči.

Má-li náš algoritmus (tj. program z obr. 2.1.8) zpracovat vstup délky n, pak při každém přečtení pravé závorky, což nastane řádově n-krát, musí vykonat řádově n kroků, aby nalezl k ní příslušnou levou závorku. Program tedy pracuje v čase $\mathcal{O}(n^2)$. Program užívá pouze tři paměťové buňky, jejichž obsah závisí na n, totiž buňky `Inp`, `Aux` a `Dp`. Na zápis těchto tří čísel je tedy třeba nejvýše $3\ell(n)+3$ znaků. Program z obr. 2.1.8 tedy pracuje v prostoru $\mathcal{O}(\ell(n))$. Říká se také, že pracuje v *logaritmickém prostoru*. Místo našeho $\mathcal{O}(\ell(n))$ se často píše $\mathcal{O}(\log n)$.

Nyní máme jednu z více příležitostí doložit tezi, že algoritmicky zajímavé úlohy se často vyskytují v logice. Vezměme v úvahu následující úlohy.

Pravdivostní hodnota výrokové formule

Dáno: Výroková formule A a pravdivostní ohodnocení v.

Úkol: Určit, zda ohodnocení v splňuje formuli A.

Sat

Dáno: Výroková formule A.

Úkol: Určit, zda formule A je splnitelná.

Taut

Dáno: Výroková formule A.

Úkol: Určit, zda formule A je výroková tautologie.

U těchto úloh bychom mohli uvažovat tři hodnoty. Například u úlohy Sat by to byly hodnoty „A není výroková formule“, „A je splnitelná výroková formule“ a „A je nesplnitelná výroková formule“. Tak ale nepostupujeme, dvě z těchto hodnot vždy ztotožňujeme. Všechny tři úlohy definujeme jako dvouhodnotové. Odpověď NE tedy například opět v případě úlohy Sat znamená „A není výroková formule nebo

A je nesplnitelná výroková formule“. Takovéto ztotožnění si můžeme dovolit proto, že nijak neuzavírá ani nekomplikuje cestu zpátky ke třem hodnotám. Kdybychom trvali na tom, že chceme vědět, co konkrétně znamená NE (například zda „A není výroková formule“ či „A je nesplnitelná výroková formule“), neznamenalo by to (jak se dále ukáže) žádné podstatně větší časové ani paměťové nároky.

Než budeme uvažovat o algoritmech počítajících tyto úlohy, je třeba zvolit abecedu Σ a stanovit, v jakém formátu budeme na vstupní pásku počítače RASP zapisovat výrokové formule a případně pravdivostní ohodnocení. V kapitole 1 jsme vystačili s tím, že výrokové formule jsou sestaveny pomocí logických spojek z výrokových atomů, přičemž výrokové atomy tvoří abstraktní množinu, na kterou neklademe žádné zvláštní požadavky a která může být i nespočetná. Pro tento okamžik a pro všechny situace, kdy budeme uvažovat o algoritmech zpracovávajících výrokové formule, přijměme dodatečnou úmluvu, že množina všech výrokových atomů je nekonečná spočetná a že $a_0, a_1, a_2, \ldots$ je prostá posloupnost všech jejích prvků. Protože abeceda Σ musí být konečná, ale výrokových atomů je nekonečně mnoho, nemůžeme výrokové atomy považovat za jednotlivé (dále nedělitelné) symboly a musíme se i u nich rozhodnout, jak je budeme zapisovat. Nejjednodušší je zapisovat atom a_i jako znak `a` následovaný zápisem čísla i. Přitom může být stanoveno, že zápis čísla i je dekadický, binární, unární (kdy číslo i je zapsáno pomocí i stejných znaků) nebo ještě jiný. Například atom a_9 je při dekadickém zapisování indexů reprezentován slovem `a9`, při binárním slovem `a1001` a při unárním slovem `a|||||||||`.

Lze snadno zdůvodnit, že mezi binárním a dekadickým zapisováním indexů není vlastně žádný rozdíl, neboť existují rychlé a paměťově úsporné algoritmy, které převedou zápis formule A, v němž jsou indexy zapsány dekadicky (nebo binárně), na zápis téže formule, v němž jsou zapsány naopak binárně (resp. dekadicky). V situacích, které uvažujeme v této knize, by dokonce ani volba unárního zapisování indexů nic podstatného neměnila. Nicméně pro určitost se domluvme, že indexy (u atomů ve výrokových formulích a v dalších kapitolách také u proměnných v predikátových formulích) se zapisují binárně. Kdykoliv tedy uvažujeme o algoritmickém zpracování syntaktických objektů, výroková formule je pro nás slovem sestaveným z pomocných symbolů `(`, `)` a `a`, logických spojek `→`, `¬`, `&` a `∨` a z číslic `0` a `1`.

Než popíšeme algoritmus pro výpočet pravdivostní hodnoty formule při daném pravdivostním ohodnocení, musíme také stanovit způsob zapisování pravdivostních ohodnocení. Máme-li jen jednu formuli A, má každé pravdivostní ohodnocení jen konečně mnoho důležitých hodnot, tj. takových hodnot, které mají vliv na pravdivostní hodnotu formule A. Můžeme se tedy domluvit, že pravdivostní ohodnocení v je pro nás konečný seznam dvojic tvaru $[i, k]$, kde $k \in \{0, 1\}$. Význam dvojice $[i, k]$ je „atom a_i má hodnotu k“. O atomech, kterým hodnota není explicitně přiřazena, se rozumí, že mají hodnotu 0. Zápis dvojice $[i, k]$ sestává z binárních zápisů čísel i a k oddělených středníkem. Jednotlivé dvojice od sebe navzájem i od formule A oddělujeme rovněž středníkem. Například obsah vstupní pásky tvaru

(	(	a	1	1	0	→	a	1	)	→	a	1	)	;	1	1	0	;	1	■	···

(∗)

reprezentuje otázku, zda výroková formule $((a_6 \to a_1) \to a_1)$ je splněna ohodnocením, které výrokový atom a_6 ohodnocuje jedničkou a všechny ostatní atomy nulou. Jak už bylo dohodnuto, plný obdélník ■ označuje koncovou značku. Tři tečky naznačují, že ve všech ostatních polích vstupní pásky jsou také koncové značky.

Ukážeme si dva různé algoritmy počítající úlohu PRAVDIVOSTNÍ HODNOTA VÝROKOVÉ FORMULE. Oba začínají svou činnost tím, že vstup tvaru $(*)$ celý přečtou, převedou jej do paměti a přepracují jej přitom na tvar

···	12	‘(	‘(	‘a	6	‘¬	‘a	1	‘)	‘¬	‘a	1	‘)	2	1	0	6	1	···

$(**)$

Číslo 12 říká, že paměťová reprezentace vstupní formule A je uložena v následujících dvanácti paměťových buňkách. Paměťová reprezentace se v podstatě shoduje s původní formulí až na to, že znaky jsou převedeny na číselné kódy (to je naznačeno levými apostrofy) a binární zápisy indexů jsou převedeny (konvertovány) na čísla. Zbývající pětice paměťových buněk obsahující čísla 2, 1, 0, 6 a 1 reprezentuje informaci, že v pravdivostním ohodnocení v jsou dvě důležité hodnoty: atom a_1 je ohodnocen nulou a atom a_6 jedničkou. Datová struktura, která zaujímá souvislou část paměti a v níž první paměťová buňka obsahuje informaci o počtu zbývajících paměťových buněk, se zpravidla nazývá *záznam*. O datové struktuře $(**)$ tedy můžeme mluvit jako o dvou (bezprostředně za sebou následujících) záznamech. První reprezentuje vstupní formuli A, druhý reprezentuje vstupní pravdivostní ohodnocení v. Jednoduchý příklad, jak může nějaký program P pracovat se strukturou tvaru $(**)$, je tento: ukazuje-li buňka `X` na začátek této struktury (tj. na pole obsahující údaj o délce prvního záznamu), pak po provedení instrukcí `mov X,Y` a `add @(Y)+,Y` ukazuje buňka `Y` na druhý záznam, tj. na reprezentaci pravdivostního ohodnocení.

Formulujme první z našich dvou algoritmů, které počítají úlohu PRAVDIVOSTNÍ HODNOTA VÝROKOVÉ FORMULE.

> Přečti ze vstupní pásky vstupní data A a v a zkontroluj jejich formát. Je-li nesprávný, řekni NE a skonči. Jinak přepracuj vstupní data na datovou strukturu dohodnutého tvaru (sestávající ze dvou na sebe navazujících záznamů) a zapiš ji do volné paměti za koncem programu.

Kontrolou formátu rozumíme ověření, že A je skutečně výrokovou formulí a že ohodnocení v neobsahuje sporné údaje, tj. že pro žádné i neobsahuje současně dvojice $[i, 0]$ a $[i, 1]$. Zápis výrokové formule se velmi podobá booleovskému výrazu, jen místo znamének `+` a `*` obsahuje logické spojky `¬`, `&` a `v`, místo symbolů `0` a `1` obsahuje zápisy výrokových atomů a před výrokovým atomem (čili před znakem `a`) a před levou závorkou může obsahovat libovolné množství znaků `¬`. To znamená, že kontrolu, zda A je výrokovou formulí, lze provést algoritmem, který získáme přizpůsobením některého z našich programů zpracovávajících booleovské výrazy (z obr. 2.1.5 nebo 2.1.8), a na tuto kontrolu je potřeba čas $\mathcal{O}(n)$ nebo $\mathcal{O}(n^2)$ a prostor $\mathcal{O}(n)$ nebo $\mathcal{O}(\ell(n))$, kde n je délka vstupních dat. Řekněme, že druhý záznam naší datové struktury, tj. přepis vstupního ohodnocení v, si přejeme mít ve tvaru $r, i_1, k_1, .., i_r, k_r$, kde $i_1, .., i_r$ je rostoucí posloupnost přirozených čísel

taková, že $a_{i_1}, \ldots, a_{i_r}$ je seznam všech atomů vyskytujících se ve formuli A. Na vytvoření tohoto záznamu také postačuje čas $\mathcal{O}(n^2)$. Celá právě utvořená struktura má velikost $\mathcal{O}(n)$. Po této úvodní fázi, čili po přečtení vstupu a inicializaci datových struktur, náš algoritmus pokračuje analogicky jako program z obr. 2.1.5:

> Čti z prvního záznamu právě utvořené datové struktury znaky jeden po druhém. Znaky (, ¬, ¬, & a ∨ ukládej beze změny do zásobníku.
>
> Přečteš-li znak a, přečti i celý zbytek zápisu výrokového atomu a_i a nalezni v druhém záznamu dvojici $[i, k]$, tj. nalezni hodnotu k, kterou ohodnocení v přiřazuje atomu a_i. Odstraň ze zásobníku všechny negace bezprostředně předcházející zápis atomu a_i. Ulož k do zásobníku. Byl-li počet odstraněných negací lichý, nahraď pravdivostní hodnotu k právě uloženou do zásobníku hodnotou k ní opačnou.
>
> Přečteš-li pravou závorku, pak tato závorka spolu se čtyřmi nejvyššími položkami v zásobníku tvoří „výraz“ (sestávající ze dvou pravdivostních hodnot spojených logickou spojkou a obklopených závorkami), jehož hodnotu k určuje pravdivostní tabulka příslušné logické spojky. Odstraň ze zásobníku tyto čtyři položky, odstraň všechny bezprostředně předcházející negace a ulož do zásobníku pravdivostní hodnotu k nebo hodnotu k ní opačnou podle toho, zda počet odstraněných negací byl sudý nebo lichý.
>
> Po přečtení celé formule musí být v zásobníku jediná položka, výsledná pravdivostní hodnota. Podle toho, je-li to jednička nebo nula, řekni ANO nebo NE a skonči.

Přitom můžeme předpokládat, že ANO nebo NE se řekne zapsáním jednoznakového slova a či n na výstupní pásku. V této druhé části algoritmu, kde jsou postupně čteny znaky z datové struktury umístěné za koncem programu, je časově nejnáročnější ten případ, kdy je přečten výrokový atom. Tehdy program potřebuje $\mathcal{O}(n)$ kroků, aby v paměťové reprezentaci ohodnocení v vyhledal příslušnou hodnotu, a tento případ může nastat řádově n-krát. Vidíme, že program postupně provádí několik akcí, z nichž na každou stačí čas $\mathcal{O}(n^2)$; pracuje tedy v čase $\mathcal{O}(n^2)$. Protože paměťová reprezentace vstupních dat i maximální velikost prostoru použitého v zásobníku je $\mathcal{O}(n)$, program pracuje v prostoru $\mathcal{O}(n)$.

Druhý z našich dvou algoritmů pro počítání úlohy PRAVDIVOSTNÍ HODNOTA VÝROKOVÉ FORMULE využívá rekurzívní volání podprogramu:

> Přečti ze vstupní pásky vstupní data A a v. Zkontroluj jejich formát, a je-li nesprávný, řekni NE a skonči. Zapiš je v domluveném tvaru (tj. ve tvaru dvou záznamů) do zásobníku. Volej podprogram `Eval`. Podle toho, vrátí-li výsledek ano nebo ne, řekni ANO nebo NE a skonči.

Tato část programu je podobná tomu, co se dělo v posledních pěti řádcích programu z obr. 2.1.6. Rozdíl je v tom, že podprogram `Get` měl za úkol zpracovat jistý podvýraz výrazu umístěného na vstupní pásce, kdežto náš podprogram `Eval` má za

úkol vyhodnotit data (formuli plus ohodnocení), která jsou umístěna v zásobníku. Tato data podprogram nazývá „A“ a „v“. Jedná se ale o „lokální“ označení v tom smyslu, že každá kopie podprogramu `Eval` má na vrcholu zásobníku svá vlastní data A a v. Předpokládáme, že během určování, zda ohodnocení v splňuje formuli A, podprogram `Eval` tato data ze zásobníku odstraní a že výsledek ano nebo ne vrátí tak, jak jsme zvyklí, uložením výstupního parametru `'0` nebo `'1` do zásobníku. Podprogram `Eval` pracuje takto:

> Pokud formule A, čili první ze dvou záznamů uložených v zásobníku, je reprezentací atomu a_i, nalezni v druhém záznamu hodnotu k, kterou ohodnocení v přiřazuje atomu a_i. Odstraň A a v ze zásobníku a vrať výsledek ano nebo ne podle toho, zda $k = 1$ nebo $k = 0$.
>
> Pokud formule A začíná levou závorkou, může mít jeden z tvarů $(B\&C)$, $(B\vee C)$ nebo $(B\to C)$. Má-li tvar $(B\&C)$, pak: ulož do zásobníku data B a v, volej podprogram `Eval` a zapamatuj si výsledek, ulož do zásobníku data C a v, znovu volej podprogram `Eval`, zapamatuj si výsledek. Odstraň A a v ze zásobníku a vrať výsledek ano, byly-li oba zapamatované výsledky ano, jinak vrať výsledek ne.
>
> Pokud formule A má tvar $(B\vee C)$ nebo $(B\to C)$, postupuj analogicky, jen místo pravdivostní tabulky konjunkce užij pravdivostní tabulku disjunkce resp. implikace.
>
> Pokud formule A má tvar $\neg B$, postupuj rovněž analogicky, podprogram `Eval` volej na data B a v a užij pravdivostní tabulku negace.

U tohoto programu lze opět snadno odhadnout, že pracuje v čase $\mathcal{O}(n^2)$. Víme, že výpočet takovéhoto podprogramu rekurzívně volajícího sama sebe lze chápat jako průchod stromem, v němž vrcholy odpovídají jednotlivým kopiím podprogramu, a že prostor potřebný pro výpočet lze odhadnout jako součet velikostí lokálních dat všech kopií podél jedné větve stromu. Každá větev má délku nejvýše n a lokální data každé kopie (tj. formule A a ohodnocení v v zásobníku) mají velikost $\mathcal{O}(n)$. Algoritmus tedy pracuje v prostoru $\mathcal{O}(n^2)$.

Máme tedy dva různé algoritmy pro určování pravdivostní hodnoty dané formule při daném pravdivostním ohodnocení. Význam prvního je v tom, že na něm lze založit algoritmy pro počítání úloh SAT a TAUT. Význam druhého je v tom, že jeho modifikací lze získat algoritmus pro počítání úlohy QBF, kterou popíšeme za chvíli. Algoritmus pro úlohu SAT vypadá takto:

> Přečti ze vstupní pásky formuli A. Zkontroluj její formát, a je-li nesprávný, řekni NE a skonči. Zapiš ji v domluveném tvaru do volné paměti za koncem programu. Za ni zapiš (v dohodnutém formátu reprezentaci) ohodnocení v, které všem atomům formule A přiřazuje nuly.
>
> Zjisti, zda ohodnocení v splňuje formuli A. Pokud ano, řekni ANO, formule A je splnitelná, a skonči. Jinak nalezni v ohodnocení v poslední dvojici tvaru $[i, 0]$. Pokud taková dvojice neexistuje, tj. všem atomům je přiřazena hodnota 1,

> řekni NE, formule A není splnitelná, a skonči. Jinak nahraď dvojici $[i, 0]$ dvojicí $[i, 1]$, druhé členy všech následujících dvojic změň na nuly a pokračuj znovu od zjišťování, zda ohodnocení v splňuje formuli A.

Tento algoritmus tedy probírá všechna pravdivostní ohodnocení v a zjišťuje, zda některé splňuje formuli A. Počet všech pravdivostních ohodnocení, tj. všech funkcí z množiny, která má nejvýše n prvků, do množiny $\{0, 1\}$, lze odhadnout číslem 2^n. Protože na zpracování každého ohodnocení je potřeba čas $\mathcal{O}(n^2)$, náš algoritmus pracuje v čase $\mathcal{O}(n^2 \cdot 2^n)$. Lze také říci, že pracuje v čase $2^{\mathcal{O}(n)}$, protože funkce $n^2 \cdot 2^n$ je v $\mathcal{O}(2^{2n})$. Algoritmus pracuje v prostoru $\mathcal{O}(n)$, v každém okamžiku totiž drží v paměti pouze jedno pravdivostní ohodnocení.

Algoritmus počítající úlohu TAUT lze získat naprosto analogicky a bude to algoritmus, pro který budou platit stejné odhady na čas i prostor.

Kvantifikované výrokové formule jsou výrokové formule, ve kterých se kromě logických spojek připouštějí také výrokové kvantifikátory $\forall p$ a $\exists p$. Každá výroková formule je tedy zároveň kvantifikovanou výrokovou formulí. Navíc je-li A kvantifikovaná výroková formule a p libovolný výrokový atom, pak i $\forall pA$ a $\exists pA$ jsou kvantifikované výrokové formule. Je-li v pravdivostní ohodnocení, pak $v(p/0)$ označuje ohodnocení, které atomu p přiřazuje hodnotu 0 a na všech ostatních atomech se shoduje s ohodnocením v. Podobně $v(p/1)$ je ohodnocení, které atomu p přiřazuje hodnotu 1 a jinak se shoduje s ohodnocením v. V dvojici $v(p/0)$ a $v(p/1)$ se ovšem pouze (a právě) jedno ohodnocení liší od původního ohodnocení v.

Formule $\forall pA$ je splněna ohodnocením v, právě když formule A je splněna oběma ohodnoceními $v(p/0)$ a $v(p/1)$. Formule $\exists pA$ je splněna ohodnocením v, právě když formule A je splněna některým z ohodnocení $v(p/0)$ a $v(p/1)$. Ostatní logické symboly (logické spojky) vyskytující se v kvantifikovaných výrokových formulích mají obvyklý význam.

Například kvantifikovaná výroková formule $\exists q(p \,\&\, q)$ je splněna ohodnocením v, právě když $v(p) = 1$. Formule $\exists p(p \vee q)$ a $\forall p \exists q((p \to q) \,\&\, (q \to p))$ jsou splněny každým ohodnocením v.

Nesnažíme se tvrdit, že výrokové kvantifikátory mají zřejmý intuitivní význam ani že jsou důležité pro logiku. Postupně si ale ozřejmíme, že úloha QBF (*quantified boolean formulae*) má dost velký význam v teoretické informatice:

QBF

Dáno: Kvantifikovaná výroková formule A a pravdivostní ohodnocení v.

Úkol: Určit, zda ohodnocení v splňuje formuli A.

Užijeme-li značení z cvičení 12 oddílu 1.1, můžeme říci, že každá formule $\forall pA$ je ekvivalentní s formulí $A_p(\top) \,\&\, A_p(\bot)$, kdežto formule $\exists pA$ je ekvivalentní s formulí $A_p(\top) \vee A_p(\bot)$. To znamená, že každá kvantifikovaná výroková formule je ekvivalentní s formulí neobsahující výrokové kvantifikátory, a lze si rozmyslet, že je tomu tak bez ohledu na to, zda symboly $\top$ a $\bot$ byly přijaty mezi základní logické symboly. Potíž je ale v tom, že odstraněním výrokových kvantifikátorů se formule může až exponenciálně prodloužit. Algoritmus, který by úlohu QBF počítal tak,

```
boolean function E(A, v)
    if A = (B & C)  then return [E(B, v) and E(C, v)]
    if A = (B ∨ C)  then return [E(B, v) or E(C, v)]
    if A = (B → C)  then return [not E(B, v) or E(C, v)]
    if A = ¬B       then return [not E(B, v)]
    if A = ∀a_i B   then return [E(B, v(i/1)) and E(B, v(i/0))]
    if A = ∃a_i B   then return [E(B, v(i/1)) or E(B, v(i/0))]
    if A = a_i      then return v(i)
endfunction
```

Obrázek 2.1.9: Algoritmus pro úlohu QBF

že by danou formuli nejprve převedl na ekvivalentní formuli bez výrokových kvantifikátorů, by tudíž měl vysoké nároky na paměťový prostor. Existuje ale úspornější algoritmus pro počítání úlohy QBF a lze jej získat tak, že k našemu druhému (rekurzívnímu) algoritmu pro určování pravdivostní hodnoty výrokové formule přidáme část, která se zabývá výrokovými kvantifikátory:

> Pokud formule A má jeden z tvarů $\forall a_i B$ nebo $\exists a_i B$, pak: ulož do zásobníku data B a $v(i/0)$, volej podprogram `Eval` a zapamatuj si výsledek, ulož do zásobníku data B a $v(i/1)$, znovu volej podprogram `Eval`, zapamatuj si výsledek. Odstraň A a v ze zásobníku. Měla-li formule A tvar $\forall a_i B$, vrať výsledek ano, byly-li oba zapamatované výsledky ano, jinak vrať výsledek ne. Měla-li tvar $\exists a_i B$, vrať výsledek ano, byl-li alespoň jeden ze zapamatovaných výsledků ano, jinak vrať výsledek ne.

V zápisu algoritmu píšeme $v(i/0)$ a $v(i/1)$ místo důslednějšího $v(a_i/0)$ a $v(a_i/1)$, což je snad přijatelné vzhledem k tomu, jak jsme definovali reprezentaci pravdivostního ohodnocení. Tato modifikace původního algoritmu má stejné nároky na paměťový prostor. Úlohu QBF lze tedy počítat v prostoru $\mathcal{O}(n^2)$. Pro znalce dodejme, že jsou známy ještě úspornější algoritmy; to však pro náš text nemá význam.

Na obrázku 2.1.9 jsme podstatnou část našeho algoritmu, totiž jeho podprogram `Eval`, přejmenovali na „E“ a zapsali jsme jej ve smyšleném vyšším programovacím jazyce, tj. pomocí dosud nepoužitých programových konstruktů (maker). Zápis $E(A, v)$ v prvním řádku udává, jak se podprogram jmenuje (tj. jaké návěští se má vygenerovat) a jaké vstupní parametry má podprogram očekávat v zásobníku. Slovem `function` je řečeno, že zápis $E(..)$ se v místech, odkud je podprogram volán, může vyskytnout ve výrazech. Protože podprogram v některých případech volá sám sebe, vyskytují se i v něm samém takové výrazy (vymezené hranatými závorkami), například `[not` $E(B, v)$`]`. Slovo `boolean` znamená, že zápis $E(..)$ se může s jinými takovými výrazy kombinovat pomocí `and`, `or` a `not`. Zápis `return` V znamená ulož do zásobníku na patřičné místo hodnotu výstupního parametru V a pokračuj těsně za místem, odkud byl podprogram E volán. Za místem, odkud byl podprogram E volán, se musí počítat s tím, že v zásobníku je jedna nová položka, výsledek činnosti podprogramu E.

Máme tedy algoritmus, který počítá úlohu PRAVDIVOSTNÍ HODNOTA VÝROKOVÉ FORMULE a který pracuje v čase $\mathcal{O}(n^2)$ a v prostoru $\mathcal{O}(n^2)$. Dále máme jeho rozšířenou verzi, která počítá úlohu QBF, pracuje v čase $2^{\mathcal{O}(n)}$ (cvičení), ale rovněž vystačí s prostorem $\mathcal{O}(n^2)$. Nejdůležitější částí obou algoritmů je podprogram, který rekurzívně volá sám sebe a který jsme v obou případech pojmenovali `Eval`. Všimněme si ještě, že každá kopie podprogramu `Eval` má v zásobníku vlastní lokální data sestávající ze dvou záznamů, totiž formuli A a ohodnocení v. V případě prvního algoritmu se ale ohodnocení v nikdy nemění, všechny kopie podprogramu `Eval` mají v zásobníku totéž ohodnocení v. V případě úlohy QBF se ohodnocení v mění. Formule A se ovšem mění v obou případech, v obou programech je formule A dělena na jednodušší a jednodušší formule, dokud se nedospěje k výrokovým atomům.

Nechť Σ je konečná abeceda a nechť g je funkce definovaná na množině Σ^* všech slov v abecedě Σ. Má-li funkce g pouze dvě hodnoty (ANO či NE), mluvíme o ní jako o *rozhodovací úloze*. Úlohy PRAVDIVOSTNÍ HODNOTA VÝROKOVÉ FORMULE, SAT a TAUT jsou příklady rozhodovacích úloh. Také úlohy HODNOTA BOOLEOVSKÉHO VÝRAZU a PRVOČÍSELNOST lze chápat jako rozhodovací úlohy. Rozhodovací úlohu g můžeme ztotožnit s množinou všech těch $w \in \Sigma^*$, pro která $g(w)$ je ANO. Například úlohu TAUT lze považovat buď za dvouhodnotovou funkci definovanou na množině $\{\mathtt{\neg}, \neg, \mathtt{\&}, \mathtt{v}, \mathtt{a}, \mathtt{0}, \mathtt{1}, \mathtt{(}, \mathtt{)}\}^*$ (která každému w přiřazuje hodnotu ANO nebo NE podle toho, je-li w tautologií), nebo za množinu všech slov $w \in \{\mathtt{\neg}, \neg, \mathtt{\&}, \mathtt{v}, \mathtt{a}, \mathtt{0}, \mathtt{1}, \mathtt{(}, \mathtt{)}\}^*$, která jsou tautologiemi. Podobně PRVOČÍSELNOST lze chápat jako množinu všech slov v abecedě $\{\mathtt{0}, \mathtt{1}\}$, která jsou zápisem prvočísla. Řekneme, že program P *rozhoduje* úlohu $A \subseteq \Sigma^*$, jestliže pro libovolné slovo $w \in \Sigma^*$ platí, že program P se dopočítá při zpracování vstupu w a navíc skončí svou činnost rozsvícením zeleného světla právě tehdy, platí-li $w \in A$. Jinak řečeno, rozhoduje-li program P určitou úlohu, pak jakýkoliv jeho výstup interpretujeme jako ANO, kdežto neposkytnutí výstupu interpretujeme jako NE. Program se ale na žádném vstupu nesmí zacyklit. Je zřejmé, že program, který ANO či NE řekne rozsvícením zeleného či červeného signálního světla, lze snadno upravit na program, který vždy dospěje k rozsvícení zeleného světla a ANO či NE dá najevo příslušným zápisem na výstupní pásku (čili na program, který dle naší definice počítá funkci definovanou na množině všech slov dané abecedy). Opačná úprava je také možná, ale nebudeme ji potřebovat.

Rozhodovací úloha je *rozhodnutelná* (na počítači RASP), jestliže existuje program, který ji rozhoduje. Ve zřejmém smyslu mluvíme také o *rozhodnutelnosti v čase* a o *rozhodnutelnosti v prostoru*. Rozhodovacím úlohám se v literatuře často také říká *jazyky*. My ale budeme termín „jazyk“ od příští kapitoly používat v jiném významu.

Naše dosavadní úvahy o algoritmické rozhodnutelnosti úloh vyskytujících se ve výrokové logice a o jejich složitosti můžeme shrnout do následující věty.

Věta 2.1.1 *Úlohy* SAT, TAUT *a* QBF *jsou algoritmicky rozhodnutelné. Existují programy pro počítač RASP, které rozhodují úlohu* SAT *resp.* TAUT *a které pracují v čase* $2^{\mathcal{O}(n)}$ *a v prostoru* $\mathcal{O}(n)$. *Existuje program, který rozhoduje úlohu* QBF *a který pracuje v čase* $2^{\mathcal{O}(n)}$ *a v prostoru* $\mathcal{O}(n^2)$.

Algoritmus, jehož časové nároky rostou exponenciálně s délkou vstupu, nelze považovat za příliš efektivní ani za prakticky užitečný. O otázce, zda pro úlohy SAT, TAUT a QBF existují lepší algoritmy, a o významu všech tří úloh se zmíníme v oddílu 2.3. V tomto oddílu ještě naznačíme, jak může vypadat úloha, která na počítači RASP není rozhodnutelná, tj. kterou nelze rozhodovat *žádným* programem bez ohledu na efektivnost.

Řekneme, že program P *přijímá* rozhodovací úlohu $A \subseteq \Sigma^*$, jestliže pro libovolné slovo $w \in \Sigma^*$ platí, že P poskytne výstup při zpracování vstupu w, právě když $w \in A$. Program, který přijímá úlohu A, má tedy povinnost skončit provedením instrukce `error` nebo se zacyklit (nedopočítat se) při zpracování libovolného slova $w \in \Sigma^* - A$, a naopak dopočítat se a dát nějaký (libovolný) výstup při zpracování libovolného slova $w \in A$.

Lemma 2.1.2 *(a) Nechť rozhodovací úloha $A \subseteq \Sigma^*$ je rozhodnutelná na počítači RASP. Pak i její komplement $\Sigma^* - A$ je rozhodnutelný na počítači RASP.*
(b) Je-li úloha $A \subseteq \Sigma^*$ rozhodnutelná na počítači RASP, pak existuje program v jazyce RASP, který úlohu A přijímá.

Důkaz je zřejmý. V programu, který se dopočítá na každém vstupu, totiž můžeme zaměnit instrukce `halt` a `error`, a získat tak program, který rozhoduje komplement dané úlohy. Dále je zřejmé, že program, který určitou úlohu rozhoduje, tutéž úlohu současně i přijímá. QED

Zvolme minimální abecedu Σ_0, která postačuje k zapsání libovolného programu v jazyce RASP. Mysleme si na chvíli, že programy píšeme bez komentářů a že tedy znaku středník můžeme dát nový význam. Dále si mysleme, že překladač jazyka RASP nerozlišuje mezi malými a velkými písmeny. Do abecedy Σ_0 tedy zahrňme znaky `@`, `#`, `-`, `+`, `(`, `)`, dále čárku, levý apostrof, tečku a středník, číslice `0` až `9` a konečně všechna malá latinská písmena a mezeru. Znak tečka slouží k oddělení instrukcí v zápisu programu, tj. stojí všude tam, kde by se v „normálním“ zápisu programu přešlo na nový řádek. Definujme úlohu

PROBLÉM ZASTAVENÍ

Dáno: Program P (zapsaný bez maker a komentářů a tak, že jednotlivé instrukce jsou odděleny tečkou) a slovo w v abecedě $\Sigma_0 - \{;\}$.

Úkol: Rozhodnout, zda program P se dopočítá (zastaví), je-li mu ke zpracování předložen vstup w.

Domluvme se, že program P a slovo w jsou na vstupní pásce počítače odděleny znakem středník. Komplement úlohy PROBLÉM ZASTAVENÍ tedy obsahuje slova v abecedě Σ_0, která neobsahují středník, dále slova, která obsahují více než jeden středník, pak slova tvaru $P;w$, kde P a w neobsahují středník a P není zápisem programu, a konečně (hlavně) slova $P;w$, kde P je zápisem programu (takže neobsahuje středník) a w je takové slovo v abecedě $\Sigma_0 - \{;\}$, při jehož zpracování se program P zacyklí.

Věta 2.1.3 *(a) Existuje program v jazyce RASP, který přijímá úlohu* Problém zastavení.
(b) Neexistuje program v jazyce RASP, který přijímá komplement úlohy Problém zastavení. *Úloha* Problém zastavení *tedy není na počítači RASP rozhodnutelná.*

K tvrzení (b) poznamenejme, že jeho druhá část plyne z první, využijeme-li lemma 2.1.2. Větu 2.1.3 ponecháváme bez důkazu, něco k ní ale ještě řekneme v oddílu 2.2. Podrobný důkaz tvrzení 2.1.3(a), ale pro jiný výpočtový model, totiž pro Turingovy stroje, je uveden ve skriptech [15].

Některé úlohy tedy nejsou rozhodnutelné (počitatelné) na počítači RASP. Pokud nějaká rozhodovací úloha rozhodnutelná není, může se stát, že existuje program, který ji alespoň přijímá. O takovém programu samozřejmě netvrdíme, že je užitečný v programátorské praxi. Za zajímavý ale pokládáme fakt, že některé úlohy nemají ani to, tj. že o dané úloze je někdy možné dokázat, že nejenže není rozhodnutelná, ale že dokonce ani neexistuje program, který ji přijímá. „Přijímatelnost" tedy považujeme za důležitý teoretický nástroj pro klasifikaci (nerozhodnutelných) úloh.

Cvičení

1. Booleovský výraz v prefixovém formátu je definován takto: `0` a `1` jsou booleovské výrazy v prefixovém formátu, a dále jsou-li u a v booleovské výrazy v prefixovém formátu, pak i `+`uv a `*`uv jsou výrazy v prefixovém formátu. Například výrazům `(1+(1*0))` a `((1+0)+((1+1)*0))` odpovídají výrazy `+1*10` a `++10*+110` v prefixovém formátu. Při zapisování výrazů v prefixovém formátu se tedy neužívají závorky a operační znaménko se píše před operandy místo mezi ně. Napište program v jazyce RASP pro určování hodnoty booleovského výrazu v prefixovém formátu.

2. Zdůvodněte bez programování detailů, že existuje program pro počítač RASP, který počítá dělení dvou přirozených čísel a který pracuje v čase $\mathcal{O}(n)$.

3. Eukleidův algoritmus pro výpočet největšího společného dělitele přirozených čísel pracuje tak, že konstruuje posloupnost $d_0 \geq d_1 > d_2 > \ldots$ přirozených čísel. Iniciálně je d_0 větší a d_1 menší z čísel, ke kterým má být nalezen největší společný dělitel. Jsou-li již sestrojena čísla $d_0 \geq d_1 > d_2 > .. > d_{i+1}$ a $d_{i+1} = 0$, algoritmus končí a d_i je výsledek. Je-li $d_{i+1} \neq 0$, k posloupnosti je přidán nový člen d_{i+2} definovaný jako zbytek po dělení čísla d_i číslem d_{i+1}. Zdůvodněte, že tento algoritmus pro každou dvojici čísel správně určí jejich největší společný dělitel.

4. Zdůvodněte na základě předchozích dvou cvičení, že existuje program pro počítač RASP, který počítá největší společný dělitel dvou přirozených čísel a který pracuje v prostoru $\mathcal{O}(n)$ a čase $\mathcal{O}(n^2)$.

Návod. Zdůvodněte, že pro každé tři po sobě jdoucí členy d_i, d_{i+1}, d_{i+2} v posloupnosti definované v předchozím cvičení platí $d_i \geq d_{i+1} + d_{i+2}$ a $d_i \geq 2d_{i+2}$.

5. Navrhněte program pro počítač RASP, který pro každé přirozené číslo x určí, zda x je prvočíslem (tj. který počítá úlohu Prvočíselnost). Stanovte prostorové a časové nároky vašeho programu.

   Návod. Spokojte se s tímto výsledkem: prostor $\mathcal{O}(n)$, čas $2^{\mathcal{O}(n)}$.

6. Jsou-li u a v booleovské výrazy a w_1 a w_2 slova v abecedě $\{\texttt{(}, \texttt{)}, \texttt{+}, \texttt{*}, \texttt{0}, \texttt{1}\}$ taková, že $w_1 u = w_2 v$ nebo $u w_1 = v w_2$, pak $u = v$ a $w_1 = w_2$. Dokažte.

   Návod. Postupujte indukcí podle součtu počtu znaků ve výrazech u a v. Užijte opakovaně fakt, že jsou-li w_1', w_2' a w slova taková, že $w_1' w = w_2' w$, pak $w_1' = w_2'$.

7. Nechť w a v jsou slova v $\{\texttt{(}, \texttt{)}, \texttt{+}, \texttt{*}, \texttt{0}, \texttt{1}\}$ taková, že wv`)` a v jsou booleovské výrazy. Pak slovo w má délku alespoň 3, jeho prvním znakem je levá závorka, posledním znakem je `+` nebo `*`, předposledním znakem je `0`, `1`, nebo `)`. Dokažte.

8. V komentáři k programu z obr. 2.1.8 bylo definováno, co je levá závorka příslušná k dané pravé závorce. Zdůvodněte, že (i) ke každé pravé závorce libovolného slova w v abecedě $\{\texttt{(}, \texttt{)}, \texttt{+}, \texttt{*}, \texttt{0}, \texttt{1}\}$ existuje nejvýše jedna k ní příslušná levá závorka, (ii) je-li navíc w booleovským výrazem, pak ke každé pravé závorce slova w existuje (právě jedna) k ní příslušná levá závorka, a (iii) je-li navíc w výrazem různým od `0` a `1`, pak poslední znak slova w je pravá závorka a první znak k ní příslušná levá závorka.

9. Napište (jinak neužitečný) program, který pracuje v čase $\mathcal{O}(n)$, ale při zpracování libovolného vstupu délky n použije paměť velikosti nejméně 2^n.

   Návod. Každá konfigurace při naší definici udává obsah souvislého pole paměťových buněk. Paměťové buňky, do kterých program během své činnosti něco zapíše, nemusí tvořit souvislé pole.

10. Zdůvodněte, že každá z funkcí $n \mapsto n^k \cdot 2^n$ je v $\mathcal{O}(2^{2n})$.

11. Zdůvodněte, že náš program pro rozhodování úlohy QBF pracuje v čase $2^{\mathcal{O}(n)}$.

2.2 Základní pojmy z teorie rekurzívních funkcí

V tomto oddílu se budeme zabývat funkcemi, jejichž argumenty i funkční hodnoty jsou přirozená čísla. Začněme dvěma jednoduchými příklady. Snadno lze ukázat (indukcí podle x), že existuje právě jedna funkce f, splňující (pro všechna x) podmínky

$$f(0) = 1, \qquad f(x+1) = (x+1) \cdot f(x). \tag{1}$$

Jde o funkci $x \mapsto x!$, tj. o funkci faktoriál. Také podmínky

$$f(0) = 1, \qquad f(1) = 1, \qquad f(x+2) = f(x+1) + f(x) \tag{2}$$

jednoznačně určují funkci z N do N. Její hodnoty například v bodech 0 až 5 jsou 1, 1, 2, 3, 5 a 8 a říká se jí Fibonacciho funkce. Společnou vlastností předpisů (1) a (2) je to, že nedávají přímou odpověď na otázku, jaká je hodnota funkce f v určitém bodě x, nýbrž převádějí ji na otázku, jaká je hodnota funkce f v nějakém jiném bodě nebo bodech. Chceme-li na základě předpisu (2) určit hodnotu funkce f například v bodě 17, potřebujeme znát její hodnoty v bodech 15 a 16; tyto hodnoty pak máme sečíst. Přitom je důležité, že tyto nové otázky, na které je převedena původní otázka po hodnotě v bodě x, se vždy týkají čísel *menších* než x. Díky tomu můžeme předpis tvaru (1) nebo (2) užít k *výpočtu* hodnoty funkce v libovolném bodě x: máme-li určit hodnotu například opět v bodě 17, určíme nejprve postupně hodnoty ve všech bodech 0 až 16.

Předpisům tvaru (1) a (2) se obecně říká rekurzívní definice funkce a o funkci, která je takovým předpisem určena, se říká, že je definována (odvozena) *rekurzí*. Náš plán je definovat přesně jednu z variant rekurze, totiž primitivní rekurzi, a pak definovat částečně rekurzívní funkce jako funkce, které lze odvodit opakovaným užitím primitivní rekurze a ještě dalších dvou operací. Částečně rekurzívní funkce budou naším druhým výpočtovým modelem.

Domluvme se, že platí-li $\psi : X \to Y$, tj. zobrazuje-li funkce ψ množinu X do množiny Y, množině X říkáme *definiční obor* funkce ψ a píšeme $X = \mathrm{Dom}(\psi)$. Pro pozdější použití definujme množinu $\mathrm{Rng}(\psi)$, *obor hodnot funkce* ψ, jako množinu $\{\, z \,;\, \exists x(\psi(x) = z) \,\}$. Dále se domluvme, z jakého univerza funkcí chceme vyčlenit částečně rekurzívní funkce:

Definice 2.2.1 *Funkce ψ je* částečná funkce *k proměnných, platí-li $\psi : X \to \mathrm{N}$, kde $X \subseteq \mathrm{N}^k$. Částečná funkce ψ, která je funkcí k proměnných, je* totální, *jestliže platí* $\mathrm{Dom}(\psi) = \mathrm{N}^k$.

Místo $[x_1, .., x_k] \in \mathrm{Dom}(\psi)$ budeme psát $!\psi(x_1, .., x_k)$. Zápis $!\psi(x_1, .., x_k)$ čteme „funkce ψ je definována v bodě $[x_1, .., x_k]$“ nebo také „funkce ψ konverguje v bodě $[x_1, .., x_k]$“. V souladu s tím se zápis $\neg!\psi(x_1, .., x_k)$ někdy čte „funkce ψ diverguje v bodě $[x_1, .., x_k]$“. Za částečnou funkcí ψ se často budeme snažit vidět nějaký program, který ji počítá, a je-li z její funkční hodnota v bodě $[x_1, .., x_k]$, bude užitečné si představovat, že z je výstup, který onen program vydal, jestliže mu byl mu ke zpracování předložen vstup $[x_1, .., x_k]$. Zápis $!\psi(x_1, .., x_k)$ se proto čte také „funkce ψ se dopočítá v bodě $[x_1, .., x_k]$“, kdežto zápis $\neg!\psi(x_1, .., x_k)$ se čte „funkce ψ se zacyklí v bodě $[x_1, .., x_k]$“.

Domluvme se, že je-li počet k členů nějaké k-tice zřejmý nebo nepodstatný, nebudeme jej vyznačovat a k-tici označíme podtrženým písmenem. Tuto úmluvu budeme vydatně využívat v celém zbývajícím textu. Je-li tedy například ψ částečná funkce k proměnných, pak ψ je totální, platí-li $\forall x_1 \,..\, \forall x_k !\psi(\underline{x})$.

Uvidíme, že je-li ψ částečně rekurzívní funkce k proměnných a definujeme-li totální funkci f předpisem $f(\underline{x}) = \psi(\underline{x})$ pro $[x_1, .., x_k] \in \mathrm{Dom}(\psi)$ a $f(\underline{x}) = 0$ pro $[x_1, .., x_k] \notin \mathrm{Dom}(\psi)$ (tj. dodefinujeme-li funkci ψ nulou), pak funkce f nemusí být částečně rekurzívní. Může se dokonce stát, že funkce ψ (jako množina $(k+1)$-tic)

není podmnožinou žádné totální částečné rekurzívní funkce stejného počtu k proměnných. Toto je důvod, proč uvažujeme i netotální částečné funkce.

Částečné funkce značíme malými latinskými písmeny f, g, h, ... nebo malými řeckými písmeny. Nebude-li ale o funkci označené latinským písmenem řečeno jinak, rozumí se, že jde o totální funkci.

Řekneme, že funkce φ, která má $k+1$ proměnných, je odvozena z funkcí ψ a χ, které mají k resp. $k+2$ proměnných, operací *primitivní rekurze*, jestliže pro všechna $x, y_1, \ldots, y_k$ a z platí

$$\begin{aligned} \varphi(0, \underline{y}) = z &\Leftrightarrow \psi(\underline{y}) = z, \\ \varphi(x+1, \underline{y}) = z &\Leftrightarrow !\varphi(x, \underline{y}) \ \&\ \chi(\varphi(x, \underline{y}), x, \underline{y}) = z. \end{aligned} \tag{3}$$

Příklad 2.2.2 Sčítání přirozených čísel, tj. funkce $f(x, y) = x + y$ s definičním oborem N^2, je odvozena primitivní rekurzí z funkcí g a h, o kterých platí $g(y) = y$ a $h(v, x, y) = v + 1$.

Indukcí lze snadno dokázat, že jsou-li φ, ψ a χ jako v (3) a platí-li $!\varphi(x, \underline{y})$, pak platí i $!\varphi(v, \underline{y})$ pro všechna $v < x$.

Zápis $\psi(\underline{y}) = z$ v (3) znamená, že funkce ψ je definována v bodě $[y_1, \ldots, y_k]$ a její hodnota v tomto bodě je z. Stejný význam mají i ostatní rovnosti v (3) a dále. Zápis $\psi(\underline{y}) \neq z$ by tedy znamenal, že funkce ψ buď není definována v bodě $[y_1, \ldots, y_k]$, nebo že její hodnota v tomto bodě je jiná než z.

Řekneme, že funkce φ, která má k proměnných, je odvozena z funkce χ, která má m proměnných, a z funkcí $\psi_1, \ldots, \psi_m$, které mají shodně k proměnných, operací *substituce*, jestliže pro všechna $x_1, \ldots, x_k$ a z platí

$$\varphi(\underline{x}) = z \Leftrightarrow !\psi_1(\underline{x}) \ \&\ \ldots \ \&\ !\psi_m(\underline{x}) \ \&\ \chi(\psi_1(\underline{x}), \ldots, \psi_m(\underline{x})) = z. \tag{4}$$

Funkce φ je tedy definována v bodě $[x_1, \ldots, x_k]$ právě tehdy, jsou-li v $[x_1, \ldots, x_k]$ definovány všechny funkce ψ_i a je-li navíc funkce χ definována v bodě $[\psi_1(\underline{x}), \ldots, \psi_m(\underline{x})]$.

Pro operaci substituce (říká se také operace dosazení nebo operace skládání funkcí) se užívá znak $\circ$. Fakt, že φ je z χ a $\psi_1, \ldots, \psi_m$ odvozena substitucí, se zapisuje $\varphi = \chi \circ [\psi_1, \ldots, \psi_m]$. Je-li $m = 1$, tj. je-li φ odvozena substitucí z funkce χ jedné proměnné a z jedné funkce ψ, píšeme $\varphi = \chi \circ \psi$.

Běžně užívaný zápis pro podmínku (4) je

$$\varphi(\underline{x}) \simeq \chi(\psi_1(\underline{x}), \ldots, \psi_m(\underline{x})),$$

přičemž znak $\simeq$ má tento význam: levá strana je definována jako hodnota výrazu na pravé straně, pokud je tento výraz definován; není-li definován, ani levá strana není definována.

Řekneme, že funkce φ, která má k proměnných, je z funkce ψ, která má $k+1$ proměnných, odvozena operací *minimalizace*, jestliže pro všechna $x_1, \ldots, x_k$ a z platí

$$\varphi(\underline{x}) = z \Leftrightarrow \psi(\underline{x}, z) = 0 \ \&\ \forall y{<}z\,(!\psi(\underline{x}, y) \ \&\ \psi(\underline{x}, y) \neq 0). \tag{5}$$

Běžně užívaný zápis pro podmínku (5) je

$$\varphi(\underline{x}) \simeq \mu y(\psi(\underline{x}, y) = 0),$$

písmeno μ odkazuje ke slovu „minimum“.

Příklad 2.2.3 Předpokládejme, že pro totální funkci g dvou proměnných platí $g(x, y) = 0$, je-li $x < 2^y$, a $g(x, y) \neq 0$ jinak. Užijeme-li na funkci g operaci minimalizace, dostaneme tutéž funkci, kterou jsme v minulém oddílu označili ℓ a nazvali celočíselným logaritmem.

Příklad 2.2.4 Předpokládejme, že pro funkci ψ, která je funkcí k proměnných, a určitou k-tici $[x_1, \ldots, x_k]$ platí $\psi(\underline{x}, 0) = 1$, $\neg!\psi(\underline{x}, 1)$ a $\psi(\underline{x}, 2) = 0$. Je-li φ odvozena z ψ operací minimalizace, platí $\neg!\varphi(\underline{x})$.

Vidíme tedy, že $\mu y(\psi(\underline{x}, y) = 0)$ nemusí být totéž co $\min\{\, y \,;\, \psi(\underline{x}, y) = 0 \,\}$. V situaci z příkladu 2.2.4 platí $\neg!\mu y(\psi(\underline{x}, y) = 0)$, ale $\min\{\, y \,;\, \psi(\underline{x}, y) = 0 \,\} = 2$.

Je-li φ odvozena z ψ minimalizací a platí-li $\varphi(\underline{x}) = z$, definice operace minimalizace požaduje, aby platilo i $!\psi(\underline{x}, v)$ pro všechna $v \leq z$. Tento požadavek je v souladu s naší snahou vidět za každou částečnou funkcí nějaký program a za kteroukoliv její hodnotou z vidět výpočet onoho programu, jehož výstupem je z. Výpočet funkce φ odvozené z ψ minimalizací se může zacyklit tak, že není nalezeno z splňující $\psi(\underline{x}, z) = 0$, ale také tak, že výpočet funkce ψ se zacyklí na nějakém vstupu $[\underline{x}, v]$ dříve, než by bylo nalezeno takové z.

Definice 2.2.5 *(a)* Základní funkce *jsou funkce* s, z *a* i^k_j *pro* $1 \leq j \leq k$, *kde*

$$\mathrm{s}(x) = x + 1, \qquad \mathrm{z}(x) = 0, \qquad \mathrm{i}^k_j(x_1, \ldots, x_k) = x_j$$

pro každé x *resp. pro každou* k*-tici* $[x_1, \ldots, x_k]$.
(b) Částečná funkce je částečně rekurzívní*, jestliže ji lze odvodit ze základních funkcí pomocí operací primitivní rekurze, substituce a minimalizace.*
(c) Částečná funkce je rekurzívní *(nebo* obecně rekurzívní*), jestliže je částečně rekurzívní a totální.*
(d) Částečná funkce je primitivně rekurzívní*, jestliže ji lze odvodit ze základních funkcí pomocí operací primitivní rekurze a substituce.*
(e) Množinu všech částečně rekurzívních, rekurzívních a primitivně rekurzívních funkcí značíme FPartR*,* FOR *resp.* FPR*.*

Operace minimalizace je jediná z našich tří operací, jejíž užití na totální funkci může dát netotální funkci. Výsledkem užití primitivní rekurze nebo substituce na totální funkce je vždy opět totální funkce. Protože základní funkce jsou totální, všechny primitivně rekurzívní funkce jsou automaticky totální a platí inkluze $\mathsf{FPR} \subseteq \mathsf{FOR} \subseteq \mathsf{FPartR}$. Když je funkce f odvozena z (totálních) funkcí g a h primitivní rekurzí nebo když je f odvozena z (totálních) funkcí h a $g_1, \ldots, g_m$ substitucí,

můžeme podmínky (3) a (4) přepsat na

$$f(0,\underline{y}) = g(\underline{y}), \qquad f(x+1,\underline{y}) = h(f(x,\underline{y}),x,\underline{y}), \tag{3'}$$
$$f(\underline{x}) = h(g_1(\underline{x}),\ldots,g_m(\underline{x})). \tag{4'}$$

Primitivně rekurzívní funkce jsou tedy ty funkce, které jsou ze základních odvoditelné pomocí „totálních variant“ operací primitivní rekurze a substituce vyjádřených podmínkami (3′) a (4′).

Příklad 2.2.6 Funkce $\mathrm{s}\circ(\mathrm{z}\circ\mathrm{i}_1^2)$ je konstanta dvou proměnných s hodnotou 1. Funkce $\mathrm{s}\circ(\mathrm{s}\circ(\mathrm{s}\circ\mathrm{z}))$ je konstanta jedné proměnné s hodnotou 3. Obě tyto funkce jsou primitivně rekurzívní. Podobně lze zdůvodnit, že konstanta s libovolnou hodnotou a s libovolným počtem proměnných je primitivně rekurzívní.

Příklad 2.2.7 Pro funkce g a h z příkladu 2.2.2 platí $g = \mathrm{i}_1^1$ a $h = \mathrm{s}\circ\mathrm{i}_1^3$. Platí tedy $g \in \mathit{FPR}$ a $h \in \mathit{FPR}$. Protože funkce $f(x+y) = x+y$ je z g a h odvozena primitivní rekurzí, platí i $f \in \mathit{FPR}$. Sčítání přirozených čísel je tedy primitivně rekurzívní funkcí.

Podobně bychom mohli zdůvodnit, že také funkce $[x,y] \mapsto x\cdot y$ a $[x,y] \mapsto y^x$ jsou primitivně rekurzívní. Pro zdůvodnění, že třeba také funkce $x \mapsto x!$ je primitivně rekurzívní, je výhodné užít následující variantu (6) primitivní rekurze.

Lemma 2.2.8 *Nechť h je primitivně rekurzívní funkce dvou proměnných a nechť pro číslo c a pro každé x platí*

$$f(0) = c, \qquad f(x+1) = h(f(x),x). \tag{6}$$

Pak f je primitivně rekurzívní funkce.

Důkaz Definujme funkci h' předpisem $h'(v,x,y) = h(v,x)$. Platí $h' = h\circ[\mathrm{i}_1^3,\mathrm{i}_2^3]$, tedy h' je primitivně rekurzívní. Označme g' konstantu jedné proměnné s hodnotou c. Pro funkci f', která je z g' a h' odvozena primitivní rekurzí, platí

$$f'(0,y) = c, \qquad f'(x+1,y) = h'(f'(x,y),x,y) = h(f'(x,y),x).$$

Funkci f lze z f' odvodit například takto: $f = f'\circ[\mathrm{i}_1^1,\mathrm{z}]$. QED

Operace primitivní rekurze umožňuje pro $m \geq 1$ odvodit funkci $m+1$ proměnných ze dvou funkcí, z nichž jedna je funkcí m proměnných a druhá je funkcí $m+2$ proměnných. Lemma 2.2.8 říká, že omezení $m \geq 1$ není příliš podstatné. Snadno lze také dokázat (podobným důkazem nebo převedením na tvrzení lemmatu 2.2.8), že je-li h primitivně rekurzívní funkce jedné proměnné a splňuje-li f podmínky

$$f(0) = c, \qquad f(x+1) = h(f(x)), \tag{7}$$

pak f je primitivně rekurzívní. Podmínky (6) a (7) jsou tedy korektní varianty primitivní rekurze. Také omezení v definici operace substituce požadující, aby

všechny vnitřní funkce měly stejný počet k proměnných, je nepodstatné. Je-li například f odvozena z g a h (dvou proměnných) předpisem

$$f(x, y, z) = h(g(x, y), z), \tag{8}$$

pak platí $f = h \circ [g \circ [\mathrm{i}^3_1, \mathrm{i}^3_2], \mathrm{i}^3_3]$, a jsou-li g a h primitivně rekurzívní nebo rekurzívní, pak i f je primitivně rekurzívní resp. rekurzívní.

Postupu, kterým byla v důkazu lemmatu 2.2.8 odvozena funkce h' z funkce h, říkejme *přidání jalové proměnné* a postupu, kterým byla funkce f získána z funkce f' říkejme *dosazení konstanty*. Další podobně jednoduchou operací je *ztotožnění proměnných*: víme-li například, že funkce $h(x, y) = x \cdot y$ je primitivně rekurzívní, pak i funkce $f(x) = x^2$ je primitivně rekurzívní, protože $f = h \circ [\mathrm{i}^1_1, \mathrm{i}^1_1]$. Množina všech primitivně rekurzívních funkcí je tedy uzavřená na operace přidání jalové proměnné, dosazení konstanty a ztotožnění proměnných, na varianty primitivní rekurze tvaru (6) a (7) a na různé varianty substituce podobné tvaru (8). Totéž je pravda i o množině všech rekurzívních funkcí a o množině všech částečně rekurzívních funkcí. Tyto fakty budeme v dalším užívat bez upozorňování.

Příklad 2.2.9 Nechť $y \dot{-} x$ je definováno jako $y - x$ pro $y \geq x$ a jako 0 pro $y < x$. Této funkci říkejme *podmíněné odčítání*. Funkce $y \mapsto y \dot{-} 1$ je primitivně rekurzívní:

$$0 \dot{-} 1 = 0, \qquad (y + 1) \dot{-} 1 = y,$$

a z funkce $y \mapsto y \dot{-} 1$ lze odvodit funkci $[x, y] \mapsto y \dot{-} x$:

$$y \dot{-} 0 = 0, \qquad y \dot{-} (x + 1) = (y \dot{-} x) \dot{-} 1.$$

Podmíněné odčítání je tedy primitivně rekurzívní funkcí.

Příklad 2.2.10 Víme-li již, že mocnina a podmíněné odčítání jsou primitivně rekurzívní funkce, můžeme tvrdit, že také funkce $g(x, y) = (x + 1) \dot{-} 2^y$ je primitivně rekurzívní. Funkce g splňuje podmínku $g(x, y) = 0 \Leftrightarrow x < 2^y$. Z příkladu 2.2.3 plyne, že funkce ℓ, tj. celočíselný logaritmus, je rekurzívní funkcí.

K příkladu 2.2.10 je nutno poznamenat, že dá-li se nějaká funkce odvodit s použitím minimalizace, není to ještě důkaz, že užití operace minimalizace bylo k jejímu odvození nutné. O funkci ℓ později zjistíme, že ji lze odvodit bez užití minimalizace, a že je tedy dokonce primitivně rekurzívní. Uvést příklad funkce, která je obecně rekurzívní, ale není primitivně rekurzívní, není zcela snadné. Je ale snadné uvést příklad funkce, která je částečně rekurzívní a není obecně rekurzívní; například funkce $x \mapsto \mu y(\mathrm{i}^2_1(x, y) = 0)$ je netotální částečně rekurzívní funkcí.

Definice 2.2.11 *Nechť $A \subseteq \mathrm{N}^k$. (a) Množina A je* rekurzívně spočetná*, jestliže existuje částečně rekurzívní funkce ψ taková, že $A = \mathrm{Dom}(\psi)$.*
(b) Charakteristická funkce *množiny A je funkce c_A, která je definovaná předpisem $c_A(\underline{x}) = 1$ pro $[x_1, \ldots, x_k] \in A$ a $c_A(\underline{x}) = 0$ jinak.*

(c) Množina A je (obecně) rekurzívní, *jestliže c_A je rekurzívní funkce.*
(d) Množina A je primitivně rekurzívní, *jestliže c_A je primitivně rekurzívní funkce.*
(e) Množinu všech rekurzívně spočetných, rekurzívních a primitivně rekurzívních množin značíme RS, OR resp. PR.

Snadno lze ověřit, že definujeme-li funkci g předpisem $g(\underline{x}, y) = 1 \dot{-} c_A(\underline{x})$ a odvodíme-li z funkce g funkci ψ minimalizací: $\psi(\underline{x}) \simeq \mu y(g(\underline{x}, y) = 0)$, platí $\mathrm{Dom}(\psi) = A$. Navíc je-li $c_A \in \mathsf{FOR}$, pak $\psi \in \mathsf{FPartR}$. Tím je zdůvodněno, že každá rekurzívní množina je rekurzívně spočetná. Platí tedy inkluze $\mathsf{PR} \subseteq \mathsf{OR} \subseteq \mathsf{RS}$.

Domluvme se, že je-li $A \subseteq \mathrm{N}^k$, symbolem $\overline{A}$ značíme komplement množiny A, tj. množinu $\mathrm{N}^k - A$.

Lemma 2.2.12 *(a) Sjednocení, průnik a komplement rekurzívních množin je opět rekurzívní množina.*
(b) Sjednocení, průnik a komplement primitivně rekurzívních množin je opět primitivně rekurzívní množina.

Důkaz Pro každou k-tici $[x_1, \ldots, x_k]$ platí

$$\begin{aligned} c_{A\cap B}(\underline{x}) &= c_A(\underline{x}) \cdot c_B(\underline{x}), \\ c_{\overline{A}}(\underline{x}) &= 1 \dot{-} c_A(\underline{x}), \\ c_{A\cup B}(\underline{x}) &= 1 \dot{-} (1 \dot{-} (c_A(\underline{x}) + c_B(\underline{x}))). \end{aligned}$$

Tyto funkce jsou rekurzívní, jsou-li c_A a c_B rekurzívní, a jsou primitivně rekurzívní, jsou-li c_A a c_B primitivně rekurzívní. QED

Snadno lze ověřit, že každá jednoprvková podmnožina množiny N^k je primitivně rekurzívní. Z toho a z lemmatu 2.2.12 plyne, že všechny konečné množiny a také jejich komplementy jsou primitivně rekurzívní.

Místo $[x_1, \ldots, x_k] \in A$ budeme často psát $A(x_1, \ldots, x_k)$ nebo $A(\underline{x})$. Je-li $k = 2$, místo $[x, y] \in A$ nebo $A(x, y)$ se také píše $x\ A\ y$ (tuto konvenci jsme už použili v kapitole 1).

Je-li $A \subseteq \mathrm{N}^{k+1}$, pak zápis $\mu y A(\underline{x}, y)$ značí funkci, jejíž hodnota v $[x_1, \ldots, x_k]$ je $\min\{\, y \,;\, A(\underline{x}, y) \,\}$ v případech, kdy $\exists y A(\underline{x}, y)$, a jejíž hodnota není definovaná v ostatních případech. Je lehké ověřit, že je-li množina A rekurzívní, pak funkce $[x_1, \ldots, x_k] \mapsto \mu y A(\underline{x}, y)$ je částečně rekurzívní.

Místo o množinách k-tic nebo o množinách čísel budeme často mluvit o *podmínkách* a o *vlastnostech*. Řekneme-li například, že „podmínka $x < y$ je primitivně rekurzívní“, znamená to, že množina $\{[x, y]; x < y\}$ je primitivně rekurzívní. (Snadno lze dokázat, že opravdu ano, podmínka $x < y$, a také podmínky $x \leq y$ a $x = y$ jsou primitivně rekurzívní.) Lemma 2.2.12 lze také formulovat takto: jak rekurzívní, tak primitivně rekurzívní podmínky jsou uzavřeny na disjunkci, konjunkci a negaci. Řeč podmínek a vlastností je výhodná v tom, že snadno umožňuje vzít do hry také kvantifikaci.

Nejprve uvažujme jen jistý druh kvantifikace, totiž omezenou kvantifikaci. Zápis $\forall v{<}x\, A(v,\underline{y})$, kde A je $(k+1)$-ární podmínka, znamená $\forall v(v < x \Rightarrow A(v,\underline{y}))$. Zápis $\exists v{<}x\, A(v,\underline{y})$ znamená $\exists v(v < x \;\&\; A(v,\underline{y}))$. Analogický význam mají podmínky $\forall v{\leq}x\, A(v,\underline{y})$ a $\exists v{\leq}x\, A(v,\underline{y})$. Je-li B kterákoliv z $(k+1)$-árních podmínek $\forall v{<}x\, A(v,\underline{y})$, $\exists v{<}x\, A(v,\underline{y})$, $\forall v{\leq}x\, A(v,\underline{y})$ a $\exists v{\leq}x\, A(v,\underline{y})$, říkáme, že podmínka B je z podmínky A odvozena *omezenou kvantifikací*.

Lemma 2.2.13 *Je-li podmínka B odvozena z podmínky A omezenou kvantifikací a je-li A rekurzívní, pak B je rekurzívní. Je-li A primitivně rekurzívní, pak B je primitivně rekurzívní.*

Důkaz Nechť například B je podmínka $\exists v{<}x\, A(v,\underline{y})$, tj. platí

$$B = \{\, [x,\underline{y}]\,;\, \exists v{<}x\,([v,\underline{y}] \in A)\,\}.$$

Označme sg (jako signum) funkci definovanou předpisem $\mathrm{sg}(x) = 1 \dot{-} (1 \dot{-} x)$. Platí $\mathrm{sg}(0) = 0$ a $\mathrm{sg}(x) = 1$ pro $x \neq 0$. Charakteristickou funkci množiny B lze odvodit primitivní rekurzí z funkce sg a z charakteristické funkce množiny A:

$$c_B(0,\underline{y}) = 0, \qquad c_B(x+1,\underline{y}) = \mathrm{sg}(c_B(x,\underline{y}) + c_A(x,\underline{y})).$$

Je-li A rekurzívní, pak i B je rekurzívní, a je-li A primitivně rekurzívní, pak i B je primitivně rekurzívní. Zbývající případy ponecháváme za cvičení. QED

Příklad 2.2.14 Obě funkce $[v,x,y] \mapsto v \cdot x$ a $[v,x,y] \mapsto y$ jsou primitivně rekurzívní. Jejich substitucí do charakteristické funkce relace $\{\, [u,t]\,;\, u = t\,\}$, tj. do charakteristické funkce rovnosti, dostaneme charakteristickou funkci relace $\{\, [v,x,y]\,;\, v \cdot x = y\,\}$. Podle lemmatu 2.2.13 také relace $\{\, [z,x,y]\,;\, \exists v{\leq}z\,(v \cdot x = y)\,\}$ je primitivně rekurzívní. Protože proměnné z a y můžeme ztotožnit, je primitivně rekurzívní i relace $\{[x,y];\, \exists v{\leq}y\,(v{\cdot}x = y)\}$. Kdybychom to měli zdůvodnit stručně, řekneme, že podmínka $x \mid y$ („x dělí y“) je primitivně rekurzívní, protože rovnost je primitivně rekurzívní relace, násobení je primitivně rekurzívní funkce a omezená kvantifikace je primitivně rekurzívní operace.

Příklad 2.2.15 Nechť $\mathrm{Prime}(x)$ je zkratka pro „x je prvočíslo“, tj. Prime je množina všech prvočísel. Platí

$$\mathrm{Prime}(x) \;\Leftrightarrow\; 1 < x \;\&\; \forall v{<}x\,(v \mid x \;\Rightarrow\; v = 1).$$

Protože $<$, $\mid$ a $=$ jsou primitivně rekurzívní relace, omezená kvantifikace a konjunkce jsou primitivně rekurzívní operace a implikaci lze přepsat pomocí negace a disjunkce, které jsou primitivně rekurzívními operacemi, množina všech prvočísel je primitivně rekurzívní.

Na tomto místě se hodí poznamenat, že (konstantní) jména objektů, například Prime, z, Dom nebo At, většinou zapisujeme užitím běžného písma (tj. nikoliv například kurzívy). Chceme-li ale zdůraznit, že jde o jméno úlohy, užíváme tzv.

kapitálky, neboli malá velká písmena, například SAT nebo PRVOČÍSELNOST. Prime a PRVOČÍSELNOST jsou dvě různá označení pro tutéž množinu, totiž pro množinu všech prvočísel. Fakt, že tato množina je (primitivně) rekurzívní, znamená, že úloha PRVOČÍSELNOST je rozhodnutelná, prohlásíme-li formalismus částečně rekurzívních funkcí za základní výpočtový model, tj. definujeme-li pojem algoritmu pomocí částečně rekurzívních funkcí.

Lemma 2.2.16 *Nechť $A \subseteq \mathrm{N}^k$, nechť g_1 a g_2 jsou funkce k proměnných a nechť f je definována předpisem*

$$f(\underline{x}) = \begin{cases} g_1(\underline{x}) & \text{když } A(\underline{x}) \\ g_2(\underline{x}) & \text{jinak.} \end{cases}$$

Jsou-li g_1, g_2 a A rekurzívní, pak i f je rekurzívní. Jsou-li primitivně rekurzívní, pak i f je primitivně rekurzívní.

Důkaz Platí $f(\underline{x}) = g_1(\underline{x}) \cdot c_A(\underline{x}) + g_2(\underline{x}) \cdot (1 \dot{-} c_A(\underline{x}))$. QED

Jsou-li f, g_1, g_2 a A jako v lemmatu 2.2.16, říkáme, že funkce f je (z funkcí g_1 a g_2) odvozena *větvením* (podle podmínky A).

Lemma 2.2.17 *Nechť g je funkce $k+1$ proměnných a nechť f je definována předpisem*

$$f(z, \underline{x}) = \begin{cases} \mu y(g(\underline{x}, y) = 0) & \text{když } \exists y{<}z\,(g(\underline{x}, y) = 0) \\ z & \text{jinak.} \end{cases}$$

Je-li g rekurzívní, pak i f je rekurzívní. Je-li g primitivně rekurzívní, pak i f je primitivně rekurzívní.

Důkaz Platí

$$f(0, \underline{x}) = 0,$$
$$f(z+1, \underline{x}) = \begin{cases} f(z, \underline{x}) & \text{když } \exists y{\leq}z\,(g(\underline{x}, y) = 0) \\ z+1 & \text{jinak.} \end{cases}$$

Funkce f je tedy odvozena primitivní rekurzí z funkce h, kde

$$h(v, z, \underline{x}) = \begin{cases} v & \text{když } \exists y{\leq}z\,(g(\underline{x}, y) = 0) \\ z+1 & \text{jinak.} \end{cases}$$

Vzhledem k lemmatům 2.2.13 a 2.2.16 je funkce h rekurzívní, je-li $g \in \mathit{FOR}$, a je primitivně rekurzívní, je-li $g \in \mathit{FPR}$. QED

Jsou-li f a g jako v tvrzení lemmatu 2.2.17, říkáme, že f je z g odvozena *omezenou minimalizací* a píšeme $f(z, \underline{x}) = \mu y < z(g(\underline{x}, y) = 0)$. Omezená minimalizace je primitivně rekurzívní operací. Ve zřejmém smyslu budeme psát také $\mu y \leq z(g(\underline{x}, y) = 0)$. Protože $\mu y \leq z(g(\underline{x}, y) = 0) = \mu y < (z+1)(g(\underline{x}, y) = 0)$, je i tato varianta omezené minimalizace primitivně rekurzívní operací.

Příklad 2.2.18 Platí $\ell(x) = \mu y < x((x+1) \dot{-} 2^y = 0)$. Celočíselný logaritmus je tedy primitivně rekurzívní funkcí.

Příklad 2.2.19 Nechť y je libovolné přirozené číslo. Číslo $y!$ je dělitelné všemi čísly od dvojky do y. Číslo $y!+1$ tedy není dělitelné žádným z čísel 2 až y. Rozložíme-li číslo $y!+1$ na prvočísla, dostaneme součin prvočísel, z nichž každé je větší než y a jejichž počet je alespoň 1. Tím jsme si připomněli (klasický Eukleidův) důkaz, že pro každé y existuje prvočíslo v takové, že $y < v \leq y!+1$, a že tedy množina všech prvočísel je nekonečná. Na základě vědomosti, že za každým prvočíslem y existují další prvočísla v taková, že $v \leq y!+1$, lze odvodit *rostoucí posloupnost* p *všech prvočísel*:

$$\mathrm{p}(0) = 2, \qquad \mathrm{p}(x+1) = \mu v \leq (\mathrm{p}(x)!+1)(\mathrm{Prime}(v) \ \& \ \mathrm{p}(x) < v).$$

Hodnoty funkce p v bodech 0, 1, 2, 3, 4, ... jsou 2, 3, 5, 7, 11 atd. Podmínka $\mathrm{Prime}(v)$ & $y < v$ je primitivně rekurzívní, a lze ji tedy převést na podmínku tvaru $g(y,v) = 0$. Funkce p je tedy odvozena primitivní rekurzí z funkce, která je odvozena dosazením primitivně rekurzívní funkce $y \mapsto y!+1$ do funkce, která je z g odvozena omezenou minimalizací. Rostoucí posloupnost všech prvočísel je tedy primitivně rekurzívní funkcí. V dalším výkladu pišme p_x místo $\mathrm{p}(x)$, tj. argument funkce p pišme jako dolní index.

Kdybychom chtěli na základě dosavadních znalostí zdůvodnit, že Fibonacciho funkce zmíněná na začátku tohoto oddílu je primitivně rekurzívní, narazili bychom na tuto potíž: je-li $x > 1$, podmínky (2) převádějí otázku po hodnotě v bodě x na *dvě* otázky, totiž na otázky po hodnotách v bodech $x-1$ a $x-2$. Přitom je myslitelná ještě složitější situace, kdy hodnota (nějaké jiné) funkce f v bodě x je nějakým předpisem převáděna na blíže neurčený (tj. měnící se s x) počet dalších otázek po hodnotách v bodech menších než x. Představme si například, že chceme zdůvodnit, že *ke každé rekurzívní funkci g jedné proměnné s nekonečným oborem hodnot existuje prostá rekurzívní funkce f s týmž oborem hodnot.* V tom případě je přirozené odvodit funkci f z funkce g předpisem

$$f(x) = g(\mu y(g(y) \notin \{f(0), \ldots, f(x-1)\})); \tag{9}$$

lze ověřit, že takto definovaná funkce f je opravdu prostá a má stejný obor hodnot jako funkce g. Předpis (9) umožňuje určit hodnotu $f(x)$, známe-li *všechny* předchozí hodnoty $f(0), \ldots, f(x-1)$. Program, který počítá funkci f s užitím podprogramu pro výpočet funkce g, potřebuje datovou strukturu, která při zpracování vstupu x obsahuje x číselných hodnot $f(0)$ až $f(x-1)$. Velikost této datové struktury nelze určit v době psaní programu; jedná se tedy o *dynamickou datovou strukturu.* Nyní se budeme zabývat *kódováním konečných posloupností* (přirozených čísel přirozeným číslem), které nám mimo jiné pomůže zdůvodnit, že funkce f odvozená z funkce g na základě podmínky (9) je rekurzívní, je-li g rekurzívní. Chceme-li se na formalismus rekurzívních funkcí dívat jako na svého druhu programovací jazyk, kódování konečných posloupností v tomto jazyce reprezentuje dynamické datové struktury.

Z více druhů kódování konečných posloupností vyskytujících se v literatuře si volíme následující. Kód posloupnosti $x_0, \ldots, x_{n-1}$ značíme $\langle x_0, \ldots, x_{n-1} \rangle$ a definujeme jako číslo $w = 2^{x_0+1} \cdot 3^{x_1+1} \cdot \ldots \cdot \mathrm{p}_{n-1}^{x_{n-1}+1}$. Platí tedy například

$$\langle 2, 1, 3 \rangle = 2^3 \cdot 3^2 \cdot 5^4 = 45000.$$

Fakt, že w je kódem posloupnosti, značíme $\mathrm{Seq}(w)$. Platí $\mathrm{Seq}(45000)$ a dále například $\mathrm{Seq}(6)$, $\mathrm{Seq}(1)$, $\neg\mathrm{Seq}(10)$ a $\neg\mathrm{Seq}(0)$. Obecně platí

$$\begin{aligned}\mathrm{Seq}(w) \;\Leftrightarrow\; w \neq 0 \;\&\; \forall x{\leq}w \forall y{\leq}w\, (\mathrm{Prime}(x) \\ \&\; \mathrm{Prime}(y) \;\&\; y \mid w \;\&\; x \leq y \;\Rightarrow\; x \mid w),\end{aligned}$$

vlastnost „býti kódem posloupnosti“ je tedy primitivně rekurzívní. Místo „w je kódem posloupnosti“ říkáme také „w je posloupnost“.

Počet členů posloupnosti w neboli *délku posloupnosti* w značíme $\mathrm{Lh}(w)$. Protože chceme tvrdit, že funkce Lh je primitivně rekurzívní, a protože primitivně rekurzívní funkce musí být totální, musí funkce Lh přisuzovat nějakou (jinak nedůležitou) hodnotu i těm w, pro která platí $\neg\mathrm{Seq}(w)$. Předpis

$$\mathrm{Lh}(w) = \mu y < w(\neg(\mathrm{p}_y \mid w))$$

evidentně definuje primitivně rekurzívní funkci a lze ověřit, že tato funkce má správnou hodnotu ve všech bodech w splňujících $\mathrm{Seq}(w)$. Například čísla 0, 1 a 9 mají shodně délku 0, čísla 6 a 42 mají délku 2.

Člen s indexem x posloupnosti w značíme $(w)_x$. Lze psát

$$(w)_x = \mu y < w(\neg(\mathrm{p}_x^{y+1} \mid w)) \dot{-} 1.$$

Opět platí, že funkce $[w, x] \mapsto (w)_x$ je primitivně rekurzívní a že přisuzuje správnou hodnotu všem dvojicím $[w, x]$ splňujícím podmínky $\mathrm{Seq}(w)$ a $x < \mathrm{Lh}(w)$. Funkci $[w, x] \mapsto (w)_x$ můžeme říkat *dekódovací funkce*. V dalších úvahách nesmíme zapomenout, že členy posloupností indexujeme od nuly a že posloupnost w má členy s indexy 0 až $\mathrm{Lh}(w) \dot{-} 1$.

Platí-li $w_1 = \langle x_0, \ldots, x_{n-1} \rangle$ a $w_2 = \langle y_0, \ldots, y_{m-1} \rangle$, pak zápis $w_1 * w_2$ značí číslo $\langle x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1} \rangle$, tj. kód posloupnosti vzniklé *konkatenací* (spojením) posloupností $x_0, \ldots, x_{n-1}$ a $y_0, \ldots, y_{m-1}$. Platí

$$w_1 * w_2 = w_1 \cdot \prod_{v < \mathrm{Lh}(w_2)} \mathrm{p}_{\mathrm{Lh}(w_1)+v}^{(w_2)_v+1}.$$

Protože funkci $[x, \underline{y}] \mapsto \prod_{v<x} g(v, \underline{y})$ lze z libovolné funkce g snadno odvodit primitivní rekurzí, je funkce $[w_1, w_2] \mapsto w_1 * w_2$ odvozena ze samých primitivně rekurzívních funkcí, a je tedy primitivně rekurzívní.

Nechť h je totální funkce $k+1$ proměnných. Definujme funkci $\tilde{h}$ předpisem

$$\tilde{h}(x, \underline{y}) = \langle h(0, \underline{y}), \ldots, h(x-1, \underline{y}) \rangle.$$

Číslo $\tilde{h}(x, \underline{y})$ je údaj o hodnotách funkce h ve všech bodech $[v, \underline{y}]$ pro $v < x$, a můžeme na ně nahlížet jako na onu výše zmíněnou dynamickou datovou strukturu.

Lemma 2.2.20 *Nechť h je totální funkce $k+1$ proměnných. Pak existuje jediná funkce f, která je funkcí $k+1$ proměnných a která pro každé x a $y_1, \ldots, y_k$ splňuje podmínku*

$$f(x, \underline{y}) = h(\tilde{f}(x, \underline{y}), \underline{y}). \tag{10}$$

Navíc je-li h rekurzívní, pak i f je rekurzívní, a je-li primitivně rekurzívní, pak i f je primitivně rekurzívní.

Důkaz Snadno lze dokázat indukcí podle z, že pro danou k-tici $y_1, \ldots, y_k$ a pro každé z existuje právě jedna funkce ψ splňující $\mathrm{Dom}(\psi) = \{0, \ldots, z-1\}$ a splňující dále $\psi(x, \underline{y}) = h(\tilde{\psi}(x, \underline{y}), \underline{y})$ pro všechna $x < z$. Z toho plyne existence právě jedné funkce f splňující podmínku (10); funkce f (jako množina $(k+2)$-tic) je sjednocením všech takových funkcí ψ. Funkci $\tilde{f}$ lze odvodit z funkce h a z primitivně rekurzívní funkce $[w, v] \mapsto w * \langle v \rangle$ obyčejnou primitivní rekurzí:

$$\tilde{f}(0, \underline{y}) = \langle\rangle = 1, \qquad \tilde{f}(x+1, \underline{y}) = \tilde{f}(x, \underline{y}) * \langle h(\tilde{f}(x, \underline{y}), \underline{y})\rangle.$$

Funkci f lze dále odvodit z funkce $\tilde{f}$ a z primitivně rekurzívní funkce $[w, v] \mapsto (w)_v$:

$$f(x, \underline{y}) = (\tilde{f}(x+1, \underline{y}))_x.$$

Funkce f je tedy opravdu rekurzívní nebo primitivně rekurzívní, je-li h rekurzívní resp. primitivně rekurzívní. QED

Variantě primitivní rekurze popsané v lemmatu 2.2.20 se v anglické literatuře říká *course of values recursion*. Protože podmínka (10) se podobá variantě rekurze užívané v teorii množin, říkejme jí *ordinální rekurze*.

Příklad 2.2.21 Definujme funkci h předpisem

$$h(w) = \begin{cases} (w)_{\mathrm{Lh}(w) \dot{-} 1} + (w)_{\mathrm{Lh}(w) \dot{-} 2} & \text{když } \mathrm{Lh}(w) \geq 2 \\ 1 & \text{jinak.} \end{cases}$$

Funkce h tedy považuje svůj vstup w za posloupnost a pracuje tak, že sečte dva poslední členy posloupnosti w, pokud w má alespoň dva členy, a vydá výsledek 1, je-li w kratší. Pro funkci f odvozenou z funkce h pomocí ordinální rekurze platí

$$\begin{aligned} f(0) &= h(\tilde{f}(0)) = h(\langle\rangle) = 1, \\ f(1) &= h(\tilde{f}(1)) = h(\langle f(0)\rangle) = 1, \\ f(x+1) &= h(\tilde{f}(x+2)) = h(\langle f(0), \ldots, f(x+1)\rangle) = f(x+1) + f(x). \end{aligned}$$

Tím je zdůvodněno, že Fibonacciho funkce je primitivně rekurzívní.

Máme-li kódování konečných posloupností, můžeme zavést také kódování syntaktických objektů pomocí přirozených čísel a o libovolné množině syntaktických objektů pak uvažovat, zda množina všech číselných kódů oněch objektů je například primitivně rekurzívní. Ukažme si to podrobněji na množině všech výrokových

formulí. V oddílu 2.1 jsme se domluvili, že indexy u výrokových atomů se zapisují binárně a že každá výroková formule je slovem v abecedě $\Sigma = \{\texttt{→}, \texttt{¬}, \texttt{\&}, \texttt{∨}, \texttt{(}, \texttt{)}, \texttt{0}, \texttt{1}, \texttt{a}\}$. Máme kódovou tabulku, která znakům přiřazuje číselné kódy. Řekněme, že prvkům abecedy Σ jsou číselné kódy přiřazeny takto:

→	¬	&	∨	(	)	0	1	a
0	1	2	3	12	13	32	33	70.

Každé slovo v abecedě Σ tedy můžeme pokládat za konečnou posloupnost sestavenou z čísel 0, 1, 2, 3, 12, 13, 32, 33 a 70. A díky kódování konečných posloupností pak každé takové slovo můžeme pokládat za jediné přirozené číslo. Můžeme si myslet, že slova v abecedě Σ *jsou* přirozená čísla, tj. že nerozlišujeme mezi slovem a jeho číselným kódem. Nechť zápis $\mathrm{Atom}(w)$ znamená, že w je výrokový atom, tj. že w je číselný kód zápisu výrokového atomu. Platí

$$\begin{aligned}\mathrm{Atom}(w) \;\Leftrightarrow\; \mathrm{Seq}(w) \;\&\; \mathrm{Lh}(w) \geq 2 \;\&\; (\mathrm{Lh}(w) \neq 2 \;\Rightarrow\; (w)_1 \neq 32) \;\&\\ \&\; (w)_0 = 70 \;\&\; \forall x{<}\mathrm{Lh}(w)\,(x \neq 0 \;\Rightarrow\; 32 \leq (w)_x \leq 33).\end{aligned}$$

Posloupnost w je výrokovým atomem, jestliže má délku alespoň 2, začíná znakem a a pokračuje binárním zápisem přirozeného čísla, tj. posloupností nul a jedniček, která může začínat nulou pouze v případě, kdy nula je jejím jediným členem. Je zřejmé, že podmínka Atom je primitivně rekurzívní.

Nechť dále $\mathrm{VForm}(w)$ je zkratka pro „w je výroková formule“. Platí

$$\begin{aligned}\mathrm{VForm}(w) \;\Leftrightarrow\; \mathrm{Atom}(w) \;\vee\\ \vee\; \exists w_1{<}w\,\exists w_2{<}w\,(\mathrm{VForm}(w_1) \;\&\; \mathrm{VForm}(w_2) \;\&\\ \&\; w = \langle 12\rangle * w_1 * \langle 0\rangle * w_2 * \langle 13\rangle)\\ \vee\; (\ldots \text{ podobně pro spojky } \texttt{¬}, \texttt{\&} \text{ a } \texttt{∨} \ldots).\end{aligned} \tag{11}$$

Slovo w je tedy výrokovou formulí, je-li je výrokovým atomem, nebo je-li je utvořeno ze dvou jednodušších formulí pomocí závorek a některé binární logické spojky, nebo je-li je utvořeno z jedné jednodušší formule pomocí negace. Jinak řečeno, charakteristická funkce množiny všech výrokových formulí má v bodě w hodnotu 1, právě když tato funkce má hodnotu 1 v jistých bodech, které jsou menší než w, jejichž počet je nejvýše dva a které vůči w splňují další podmínku. Ekvivalence (11) je tedy odvozením charakteristické funkce množiny všech výrokových formulí pomocí ordinální rekurze. Množina všech (číselných kódů všech) výrokových formulí je primitivně rekurzívní.

Podobně lze zdůvodnit, že také funkce $[A, v] \mapsto v(A)$, přiřazující dané výrokové formuli A její pravdivostní hodnotu při daném pravdivostním ohodnocení v, je primitivně rekurzívní. Lze také říci, že úloha Pravdivostní hodnota výrokové formule je primitivně rekurzívní.

Připomeňme si, že v minulém oddílu jsme přijali úmluvu, že pravdivostní ohodnocení přiřazující atomům $a_{i_1}, \ldots, a_{i_r}$ hodnoty $k_1, \ldots, k_r$ zapisujeme jako posloupnost

```
Z:    mov     #0,@1(SP)
      ret
S:    add     #1,@1(SP)
      ret
I52:  mov     @2(SP),@5(SP)                ; a, x1, x2, x3, x4, x2
      mov     @(SP)+,@3(SP)                ; x1, x2, x3, a, x2
      add     #3,SP                        ; a, x2
      ret
F:    mov     @(SP),-@(SP)                 ; a, a, x
      mov     #0,@1(SP)                    ; a, 0, x
      loop                                 ; a, y, x
        mov     @1(SP),-@(SP)              ; y, a, y, x
        mov     @3(SP),-@(SP)              ; x, y, a, y, x
        call    G                          ; g(x,y), a, y, x
        if      @(SP)+ eq #0  then exit
        add     #1,@1(SP)                  ; a, y+1, x
      endloop
      mov     @1(SP),@2(SP)                ; a, y, y
      mov     @(SP)+,@(SP)                 ; a, y
      ret
```

Obrázek 2.2.1: Počítání rekurzívních funkcí na počítači RASP

zápisů čísel $i_1, k_1, \ldots, i_r, k_r$ oddělených středníky a že atomy, kterým není hodnota explicitně přiřazena, mají pravdivostní hodnotu 0. Za těchto okolností lze snadno zdůvodnit (indukcí podle složitosti výrokové formule A), že je-li formule A splnitelná, pak existuje ohodnocení v, které ji splňuje a pro jehož délku (tj. pro počet znaků $|v|$ jeho zápisu) navíc platí $|v| \leq |A| + 2$. K zapisování pravdivostních ohodnocení potřebujeme znaky `0`, `1` a `;`, jimž jsou v kódové tabulce přiřazeny kódy 32, 33 a 17. Posloupnost, která má délku $\mathrm{Lh}(A) + 2$ a jejíž všechny členy jsou nejvýše 33, má při našem kódování posloupností číselný kód nejvýše $\mathrm{p}_{\mathrm{Lh}(A)+1}^{34(\mathrm{Lh}(A)+2)}$. Formule (číslo) A je tedy splnitelnou výrokovou formulí, platí-li

$$\mathrm{VForm}(A) \ \&\ \exists v{\leq}\mathrm{p}_{\mathrm{Lh}(A)+1}^{34(\mathrm{Lh}(A)+2)}\,(v(A) = 1).$$

Protože funkce $w \mapsto \mathrm{p}_{\mathrm{Lh}(w)+1}^{34(\mathrm{Lh}(w)+2)}$ je primitivně rekurzívní, množina všech splnitelných výrokových formulí, čili množina SAT, je primitivně rekurzívní.

Analogickými úvahami lze zdůvodnit, že také množiny TAUT a QBF jsou primitivně rekurzívní.

Věta 2.2.22 *Ke každé částečně rekurzívní funkci existuje program v jazyce RASP, který ji počítá.*

Důkaz Ke každé částečně rekurzívní funkci φ, která je funkcí k proměnných, existuje *pod*program, který ji počítá v tom smyslu, že je-li zavolán s parametry $x_1, \ldots, x_k$ v zásobníku, dopočítá se, právě když $!\varphi(\underline{x})$, a pokud to nastane, odstraní ze zásob-

```
F:    mov     @2(SP),-@(SP)              ; y, a, x, y
      if      @2(SP) eq #0  then         ; y, a, 0, y
        call    G                        ; f(0,y), a, 0, y
      else
        sub     #1,@2(SP)                ; y, a, x-1, y
        mov     @2(SP),-@(SP)            ; x-1, y, a, x-1, y
        call    F                        ; f(x-1,y), a, x-1, y
        mov     @2(SP),-@(SP)            ; x-1, f(x-1,y), a, ...
        mov     @1(SP),-@(SP)            ; f(x-1,y), x-1, ...
        mov     @5(SP),@2(SP)            ; f(x-1,y), x-1, y, ...
        call    H                        ; f(x,y), a, x-1, y
      endif
      mov     @(SP)+,@2(SP)              ; a, ?, f(x,y)
      mov     @(SP)+,@(SP)               ; a, f(x,y)
      ret
```

Obrázek 2.2.2: Počítání funkce odvozené primitivní rekurzí

níku položky $x_1, \ldots, x_k$ a místo nich tam uloží jednu položku $\varphi(\underline{x})$. Toto tvrzení se snadno dokáže indukcí podle počtu kroků, kterými je funkce φ odvozena ze základních funkcí. Podprogramy, které v tomto smyslu počítají některé ze základních funkcí, jsou na obrázku 2.2.1 nahoře. Podprogram `I52` počítá funkci i_2^5.

V komentáři za středníkem je u každé instrukce uvedeno, co je v zásobníku *po* provedení oné instrukce, písmeno `a` označuje návratovou adresu. S parametry v zásobníku se zachází stejně jako v podprogramech z obrázků 2.1.3 a 2.1.6. Je zřejmé, jak by vypadal podprogram pro výpočet kterékoliv jiné funkce i_j^k.

Na obrázku 2.2.1 dole je uveden podprogram `F` pro výpočet funkce φ jedné proměnné, která je odvozena z funkce ψ dvou proměnných operací minimalizace, a to za předpokladu, že podprogram `G` počítá funkci ψ. A na obrázku 2.2.2 je podprogram opět pojmenovaný `F`, který počítá funkci φ dvou proměnných odvozenou z funkcí ψ a χ operací primitivní rekurze, a to za předpokladu, že podprogramy `G` a `H` počítají funkce ψ a χ. Ponecháváme na čtenáři, aby uvážil, zda by podprogram z obrázku 2.2.2 nešlo napsat jednodušeji (s využitím cyklu). Také úvahy, jak je třeba naše podprogramy modifikovat pro funkce většího počtu proměnných, a úvahy týkající se operace substituce ponecháváme za cvičení.

Máme-li podprogram `F` počítající danou funkci φ, snadno napíšeme kompletní program `P`, který počítá tutéž funkci φ: před a za volání podprogramu `F` je třeba vložit vstupní a výstupní konverze, které přečtou vstup ze vstupní pásky, a potom naopak zapíší výsledek na výstupní pásku. QED

Čtyři z pěti podprogramů z obrázků 2.2.1 a 2.2.2 jsou na obrázku 2.2.3 zapsány v témže smyšleném vyšším programovacím jazyce, který je použit také v zápisech programů na obrázcích 2.1.9 a 5.1.3.

```
function     Z(x)              function   I(x_1, x_2, x_3, x_4, x_5)
    return   0                     return   x_2
endfunction                    endfunction
;                              ;
function     S(x)              function   F(x, y)
    return   x + 1                 if       x eq #0  then return G(y)
endfunction                        return   H(F(x − 1, y), x − 1, y)
                               endfunction
```

Obrázek 2.2.3: Zápis programů ve vyšším programovacím jazyce

Věta 2.2.23 *Každá funkce, kterou počítá libovolný program v jazyce RASP, je částečně rekurzívní.*

Náznak důkazu Nechť P je daný program, který počítá funkci ψ, která je funkcí k proměnných. V oddílu 2.1 jsme definovali konfiguraci jako jisté slovo v abecedě $\{\texttt{-}, \texttt{,}, \texttt{0}, \texttt{1}\}$, které lze interpretovat jako informaci o okamžitém stavu počítače RASP. Dále jsme definovali výpočet programu P ze vstupu w jako jistou posloupnost konfigurací. Domluvíme-li se, že konfigurace oddělujeme od sebe znakem středník, pak každý výpočet je slovem v abecedě $\{\texttt{-}, \texttt{,}, \texttt{0}, \texttt{1}, \texttt{;}\}$. Díky kódování konečných posloupností je každý výpočet zároveň přirozeným číslem. Nechť $R(\underline{x}, w)$ označuje podmínku „w je výpočet programu P ze vstupu $[x_1, \ldots, x_k]$“ a nechť f je funkce, která z výpočtu w určí jeho výsledek, tj. to číslo, jehož zápis je po skončení výpočtu w na výstupní pásce. Lze zdůvodnit (v případě funkce f podobně, jako jsme to udělali s množinou všech výrokových formulí; v případě relace R jednodušeji, neboť relace R není definována pomocí rekurze), že funkce f i relace R jsou primitivně rekurzívní. Máme-li čísla $x_1, \ldots, x_k$, trpělivým probíráním všech přirozených čísel lze najít číslo w, které je kódem výpočtu programu P ze vstupu $[x_1, \ldots, x_k]$, pokud ovšem takový výpočet existuje. To znamená, že funkce $[x_1, \ldots, x_k] \mapsto \mu w R(\underline{x}, w)$ se dopočítá, právě když $!\psi(\underline{x})$, a pokud to nastane, jejím výsledkem je výpočet programu P ze vstupu $[x_1, \ldots, x_k]$. Pro funkci ψ pak platí $\psi(\underline{x}) \simeq f(\mu w R(\underline{x}, w))$; funkce ψ je odvoditelná užitím minimalizace a pak substituce z funkcí c_R a f, které jsou primitivně rekurzívní, a je tedy částečně rekurzívní. QED

Částečně rekurzívní funkce jsou tedy přesně ty funkce, které jsou počitatelné na počítači RASP. Oba naše výpočtové modely jsou tedy v tomto smyslu ekvivalentní. V literatuře se vyskytují ještě další výpočtové modely (Turingovy stroje, vývojové diagramy, ...); o všech dosavadních výpočtových modelech ale bylo dokázáno, že jsou navzájem ekvivalentní. Nikomu se nepodařilo navrhnout žádný obecnější (silnější) model a nikomu se také nepodařilo podat neformální algoritmus, který by se nedal přepsat do formalismu (kteréhokoliv) výpočtového modelu. Tvrzení, že nic takového se nepodaří ani v budoucnu, neboť všechny rozumné výpočtové modely správně vystihují pojem *algoritmu*, který je pojmem absolutním a na zvoleném formalismu nezávislým, je známé jako *Churchova teze*. Zájemce o podrobnější úvahy

o Churchově tezi, o jejích interpretacích a o jejích filozofických a přírodovědných souvislostech odkazujeme na oddíl I.8 knihy [61].

Z vět 2.2.22 a 2.2.23 plyne, že množina $A \subseteq \mathrm{N}^k$ je rekurzívní, právě když existuje program pro počítač RASP, který ji rozhoduje, a je rekurzívně spočetná, právě když existuje program pro počítač RASP, který ji přijímá.

Věta 2.2.24 (o normální formě) *Existuje primitivně rekurzívní funkce* U *a pro každé* $k \geq 1$ *existuje* $(k+2)$*-ární primitivně rekurzívní relace* T_k *taková, že pro každou částečně rekurzívní funkci* ψ*, která je funkcí* k *proměnných, existuje číslo* e *takové, že*

$$\forall x_1 \,..\, \forall x_k(\psi(\underline{x}) \simeq \mathrm{U}(\mu w \mathrm{T}_k(e, \underline{x}, w))).$$

Náznak důkazu V důkazu věty 2.2.23 se pracovalo s tvrzením, že relace

$$\{\, [\underline{x}, w] \,;\, w \text{ je výpočet programu } \texttt{P} \text{ ze vstupu } [x_1, \ldots, x_k] \,\}$$

je primitivně rekurzívní. Toto tvrzení znamená, že na základě znalosti programu `P` můžeme napsat několik podprogramů, mezi nimi například takový, který rozhoduje, zda konfigurace D je konfigurace odvozená z konfigurace C, a z těchto podprogramů pak sestavit program `R`, který rozhoduje, zda w je výpočet ze vstupu $[x_1, \ldots, x_k]$. Nyní, tj. pro důkaz věty o normální formě, je důležité toto pozorování: není nutné, aby program `P` byl znám předem, čili v době psaní programu `R`; stačí, bude-li znám až za běhu, tj. bude-li sdělen spolu s parametry $[x_1, \ldots, x_k]$ a w. Přesněji řečeno, kromě kódování konfigurací a výpočtů lze zavést také kódování programů tak, aby vlastnost „e je kód programu“ byla primitivně rekurzívní. Za relaci T_k pak lze vzít podmínku „e je kód programu a w je výpočet téhož programu ze vstupu $[x_1, \ldots, x_k]$“ a zdůvodnit, že tato relace je primitivně rekurzívní. Za funkci U lze vzít tutéž funkci, která byla v důkazu věty 2.2.23 označena f. QED

Poznamenejme ještě pro úplnost, že není-li číslo e kódem programu, pak pro žádné w neplatí $\mathrm{T}_k(e, \underline{x}, w)$, a funkce $[x_1, \ldots, x_k] \mapsto \mathrm{U}(\mu w \mathrm{T}_k(e, \underline{x}, w))$ má prázdný definiční obor.

Libovolnou funkci ψ, která je částečně rekurzívní funkcí k proměnných, lze tedy získat dosazením vhodné konstanty e do jisté částečně rekurzívní funkce $k+1$ proměnných, totiž do funkce $[e, \underline{x}] \mapsto \mathrm{U}(\mu w \mathrm{T}_k(e, \underline{x}, w))$. Funkci $k+1$ proměnných, ze které lze získat všechny funkce z jisté množiny $\mathcal{F}$ (které všechny mají týž počet k proměnných) dosazením konstanty za první proměnnou, se říká *univerzální funkce* pro množinu $\mathcal{F}$. Věta 2.2.24 tedy tvrdí, že pro každé k má množina všech částečně rekurzívních funkcí k proměnných univerzální funkci, která přitom sama je částečně rekurzívní. Z věty 2.2.24 navíc plyne, že mezi více odvozeními dané částečně rekurzívní funkce lze nalézt takové, v němž je operace minimalizace užita právě jednou.

V knize [61] lze nalézt podrobnější důkaz věty o normální formě, který se neodvolává na kódování programů, nýbrž vystačí s úvahami o částečně rekurzívních funkcích. I tam definovanou relaci $\mathrm{T}_k(e, \underline{x}, w)$ lze ale číst „w je výpočet programu e

ze vstupu $[x_1, .., x_k]$“. Přitom za „program“ počítající funkci ψ se považuje (číselný kód) odvození funkce ψ a „výpočet“ funkce ψ ze vstupu $[x_1, .., x_k]$ je zhruba to, co by zůstalo na papíře, kdybychom na základě odvození funkce ψ počítali hodnotu $\psi(\underline{x})$ funkce ψ v bodě $[x_1, .., x_k]$ s tužkou v ruce.

Existuje tedy více způsobů, jak definovat relace T_k a funkci U, a tedy také více způsobů, jak dokázat větu 2.2.24. Nadále budeme využívat pouze vlastnosti relací T_k a funkce U dané *zněním* věty 2.2.24, nebudeme se spoléhat na vlastnosti, jejichž platnost lze vyvodit z jejího *důkazu* (z důkazu věty 2.2.24 lze například usoudit, že pro každou k-tici $[x_1, .., x_k]$ a číslo e existuje nejvýše jedno w splňující $\mathrm{T}_k(e, \underline{x}, w)$). Větu 2.2.24 a větu 2.2.40 uvedenou dále lze pokládat za jakési základní kameny teorie rekurzívních funkcí. Relaci $\mathrm{T}_k(e, \underline{x}, w)$ se říká *Turingův predikát* (pro částečně rekurzívní funkce k proměnných). Místo $\mathrm{T}_1(e, x, w)$ píšeme jen $\mathrm{T}(e, x, w)$.

Pro každé e a každé $k \geq 1$ definujme částečně rekurzívní funkci $\varphi_e^{(k)}$ předpisem

$$\varphi_e^{(k)}(x_1, .., x_k) \simeq \mathrm{U}(\mu w \mathrm{T}_k(e, \underline{x}, w)).$$

Věta 2.2.24 tvrdí, že v posloupnosti $\varphi_0^{(k)}$, $\varphi_1^{(k)}$, ... se vyskytuje každá částečně rekurzívní funkce k proměnných a navíc že funkce $[e, \underline{x}] \mapsto \varphi_e^{(k)}(\underline{x})$ je částečně rekurzívní funkcí $k+1$ proměnných. Posloupnosti $\varphi_0^{(k)}$, $\varphi_1^{(k)}$, ... říkejme *enumerace částečně rekurzívních funkcí* k proměnných. Místo $\varphi_e^{(1)}$ pišme jen φ_e. Někteří autoři píší $\{e\}^k$ a $\{e\}$ místo $\varphi_e^{(k)}$ resp. φ_e. Dále definujme množiny $\mathrm{W}_e^{(k)}$:

$$\mathrm{W}_e^{(k)} = \mathrm{Dom}(\varphi_e^{(k)}).$$

Platí

$$!\varphi_e^{(k)}(\underline{x}) \Leftrightarrow !\mu w \mathrm{T}_k(e, \underline{x}, w) \Leftrightarrow \exists w \mathrm{T}_k(e, \underline{x}, w),$$

a tedy také

$$\mathrm{W}_e^{(k)} = \{\, [x_1, .., x_k] \,;\, \exists w \mathrm{T}_k(e, \underline{x}, w) \,\}.$$

Posloupnosti $\mathrm{W}_0^{(k)}$, $\mathrm{W}_1^{(k)}$, ... říkejme *enumerace rekurzívně spočetných* k-árních *relací*. Je zřejmé, že v této posloupnosti se vyskytuje každá k-ární rekurzívně spočetná relace a že $(k+1)$-ární relace $\{\, [e, \underline{x}]; [x_1, .., x_k] \in \mathrm{W}_e^{(k)} \,\}$ je také rekurzívně spočetná. Opět pišme jen W_e místo $\mathrm{W}_e^{(1)}$. Číslu e v zápisu $\varphi_e^{(k)}$ a $\mathrm{W}_e^{(k)}$ se říká *index funkce* $\varphi_e^{(k)}$ resp. *index množiny* $\mathrm{W}_e^{(k)}$. Místo index se také říká *Kleeneho číslo* funkce $\varphi_e^{(k)}$ nebo množiny $\mathrm{W}_e^{(k)}$.

Věta 2.2.25 (o projekci) *Množina $A \subseteq \mathrm{N}^k$ je rekurzívně spočetná, právě když existuje rekurzívní relace $R \subseteq \mathrm{N}^{k+1}$ taková, že $A = \{\, [x_1, .., x_k] \,;\, \exists y R(\underline{x}, y) \,\}$.*

Důkaz Je-li A rekurzívně spočetná, pak A má nějaký index, tj. platí $A = \mathrm{W}_e^{(k)}$ pro jisté e. Víme, že $\mathrm{W}_e^{(k)} = \{\, [x_1, .., x_k] \,;\, \exists w \mathrm{T}_k(e, \underline{x}, w) \,\}$. Můžeme tedy položit $R = \{\, [x_1, .., x_k, y] \,;\, \mathrm{T}_k(e, \underline{x}, y) \,\}$. Takto definovaná relace R je dokonce primitivně rekurzívní. Na druhou stranu, platí-li $A = \{\, [x_1, .., x_k] \,;\, \exists y R(\underline{x}, y) \,\}$, kde R je rekurzívní relace, pak pro částečně rekurzívní funkci ψ definovanou předpisem $\psi(\underline{x}) \simeq \mu y R(\underline{x}, y)$ platí $\mathrm{Dom}(\psi) = A$, a tedy A je rekurzívně spočetná množina. QED

Operaci, kterou byla množina A ve větě 2.2.25 odvozena z relace R, se říká *projekce* (množiny R). Projekce jako operace na relacích je totéž, co existenční kvantifikátor jako operace na podmínkách. Věta 2.2.25 tvrdí, že rekurzívně spočetné podmínky (relace) jsou právě ty, které lze získat z rekurzívních pomocí projekce (jedné existenční kvantifikace).

Definujme *množiny* K *a* K_0:

$$\mathrm{K} = \{\, x \,;\, x \in \mathrm{W}_x \,\}, \qquad \mathrm{K}_0 = \{\, \langle x, v\rangle \,;\, v \in \mathrm{W}_x \,\}.$$

Připomeňme, že lomené závorky značí kód (v tomto případě dvouprvkové) posloupnosti. Množina K_0 je tedy (stejně jako množina K) množinou čísel, nikoliv množinou dvojic.

Věta 2.2.26 *Množiny* K *a* K_0 *jsou rekurzívně spočetné nerekurzívní množiny.*

Důkaz Protože $\mathrm{W}_x = \{\, v \,;\, \exists w \mathrm{T}(x, v, w) \,\}$, platí rovnosti $\mathrm{K} = \{\, x \,;\, \exists w \mathrm{T}(x, x, w) \,\}$ a $\mathrm{K}_0 = \{\, \langle x, v\rangle \,;\, \exists w \mathrm{T}(x, v, w) \,\}$. Z věty 2.2.25 plyne, že obě množiny jsou rekurzívně spočetné. Kdyby K byla rekurzívní, dle 2.2.12(a) by byl rekurzívní i její komplement $\overline{\mathrm{K}}$. Zdůvodníme sporem, že množina $\overline{\mathrm{K}}$ není ani rekurzívně spočetná. Nechť tedy $\overline{\mathrm{K}}$ je rekurzívně spočetná. Pak $\overline{\mathrm{K}} = \mathrm{W}_e$ pro jisté e. Uvažujme, zda e je nebo není ve W_e. Když $e \in \mathrm{W}_e$, pak $e \in \mathrm{K}$, což je ve sporu s rovností $\overline{\mathrm{K}} = \mathrm{W}_e$. Když $e \notin \mathrm{W}_e$, pak $e \notin \mathrm{K}$, což je také spor s rovností $\overline{\mathrm{K}} = \mathrm{W}_e$. Zbývá zdůvodnit, že K_0 není rekurzívní. Platí

$$x \in \mathrm{K} \;\Leftrightarrow\; \langle x, x\rangle \in \mathrm{K}_0.$$

Funkci $x \mapsto \langle x, x\rangle$ na chvíli označme g. Z podmínky $x \in \mathrm{K} \;\Leftrightarrow\; g(x) \in \mathrm{K}_0$ plyne ekvivalence $c_{\mathrm{K}}(x) = 1 \;\Leftrightarrow\; c_{\mathrm{K}_0}(g(x)) = 1$. Platí tedy $c_{\mathrm{K}} = c_{\mathrm{K}_0} \circ g$. Funkce g je rekurzívní. Kdyby c_{K_0} byla rekurzívní, i c_{K} by byla rekurzívní. QED

Protože index e funkce φ_e nebo množiny W_e lze chápat jako kód programu, který počítá funkci φ_e resp. přijímá množinu W_e, je fakt, že množina K_0 není rekurzívní, vlastně reformulací tvrzení, že Problém zastavení je algoritmicky nerozhodnutelný, a fakt, že množina K_0 je rekurzívně spočetná, je reformulací tvrzení, že existuje algoritmus, který Problém zastavení přijímá. Větu 2.2.26 lze tedy chápat jako rekurzívně teoretickou variantu věty 2.1.3. Dále tvrzení z 2.2.12(a), že rekurzívní množiny jsou uzavřeny na komplement, se předtím již objevilo v 2.1.2(a), a inkluze $\mathsf{OR} \subseteq \mathsf{RS}$ je v 2.1.2(b).

Vidíme tedy, že neplatí rovnost $\mathsf{OR} = \mathsf{RS}$. Některé rekurzívně spočetné množiny nejsou rekurzívní, a některé dokonce mají komplement, který není ani rekurzívně spočetný. Rekurzívně spočetné množiny nejsou uzavřeny na komplement a rekurzívní množiny nejsou uzavřeny na projekci.

Věta 2.2.27 (Postova) *Nechť* $A \subseteq \mathrm{N}^k$ *je rekurzívně spočetná množina taková, že i její komplement* $\overline{A}$ *je rekurzívně spočetný. Pak* A *(a ovšem i* $\overline{A}$*) je rekurzívní.*

Důkaz Máme dva různé algoritmy, z nichž jeden přijímá množinu A a druhý přijímá množinu $\overline{A}$. Potřebujeme jeden algoritmus, který množinu A rozhoduje. Je-li dána k-tice $[x_1,..,x_k]$, můžeme oba algoritmy nechat pracovat současně na tomtéž vstupu $[x_1,..,x_k]$. To, který z nich se dopočítá, pak určuje, zda $[x_1,..,x_k]$ je nebo není v A. Na této úvaze lze založit přesný důkaz.

Nechť tedy $A \in \mathsf{RS}$ a $\overline{A} \in \mathsf{RS}$. Dle věty 2.2.25 existují $(k+1)$-ární obecně rekurzívní relace P a Q takové, že $A = \{[x_1,..,x_k]; \exists y P(\underline{x},y)\}$ a $\overline{A} = \{[x_1,..,x_k]; \exists y Q(\underline{x},y)\}$. Protože $A \cup \overline{A} = \mathrm{N}$, platí $\forall \underline{x} \exists y (P(\underline{x},y) \vee Q(\underline{x},y))$. Podmínka $P \vee Q$ je rekurzívní dle tvrzení 2.2.12(a). Předpis

$$f(\underline{x}) = \mu y (P(\underline{x},y) \vee Q(\underline{x},y))$$

tedy definuje rekurzívní funkci. Platí-li $P(\underline{x}, f(\underline{x}))$, pak $[x_1,..,x_k] \in A$. Neplatí-li $P(\underline{x}, f(\underline{x}))$, musí platit $Q(\underline{x}, f(\underline{x}))$, a v tom případě $[x_1,..,x_k] \in \overline{A}$. Funkce g definovaná předpisem

$$g(\underline{x}) = \begin{cases} 1 & \text{když } P(\underline{x}, f(\underline{x})) \\ 0 & \text{jinak} \end{cases}$$

je tedy charakteristickou funkcí množiny A a je to rekurzívní funkce díky lemmatu 2.2.16. QED

Bylo tedy poněkud zavádějící, když jsme v komentáři za důkazem věty 2.2.26 řekli, že některé rekurzívně spočetné množiny, které nejsou rekurzívní, dokonce mají komplement, který není ani rekurzívně spočetný. Rekurzívně spočetná množina, která není rekurzívní, má *vždycky* tu vlastnost, že její komplement není rekurzívně spočetný. V následujících kapitolách uvidíme, že Postova věta má zajímavé důsledky v logice.

Věta 2.2.28 *Nechť $k \geq 1$ a nechť $Q \subseteq \mathrm{N}^{k+1}$ je rekurzívně spočetná. Pak existuje částečně rekurzívní funkce ψ, která je funkcí k proměnných a která pro každou k-tici $x_1,..,x_k$ splňuje podmínky*

- $!\psi(\underline{x}) \Leftrightarrow \exists y Q(\underline{x},y)$,
- $!\psi(\underline{x}) \Rightarrow Q(\underline{x}, \psi(\underline{x}))$.

Důkaz Dle věty 2.2.25 k relaci Q existuje rekurzívní relace $R \subseteq \mathrm{N}^{k+2}$ taková, že $\forall \underline{x} \forall y (Q(\underline{x},y) \Leftrightarrow \exists v R(\underline{x},y,v))$. Odvoďme funkci ψ předpisem

$$\psi(\underline{x}) \simeq (\mu w(\mathrm{Seq}(w) \ \&\ \mathrm{Lh}(w) = 2 \ \&\ R(\underline{x}, (w)_0, (w)_1)))_0.$$

Takto definovaná funkce je částečně rekurzívní a snadno lze ověřit, že má požadované vlastnosti. QED

K předchozímu důkazu poznamenejme, že je-li $Q \subseteq \mathrm{N}^{k+1}$ rekurzívně spočetná, předpis $\psi(\underline{x}) \simeq \mu y Q(\underline{x},y)$ nedefinuje částečně rekurzívní funkci (viz cvičení 24). V našem důkazu bylo podstatné hledat *najednou* dvojici $[y,v]$ takovou, že $R(\underline{x},y,v)$, tj. hledat současně funkční hodnotu y a „svědka“ v pro fakt, že $Q(\underline{x},y)$. Je-li taková dvojice reprezentovaná číslem w nalezena, $y = (w)_0$ je hledaná funkční hodnota a svědek $(w)_1$ je už nedůležitý.

Věta 2.2.29 *Nechť $A \subseteq \mathrm{N}$. Pak následující podmínky jsou ekvivalentní:*
(i) A je rekurzívně spočetná.
(ii) $A = \emptyset$ nebo A je obor hodnot jisté rekurzívní funkce.
(iii) A je konečná nebo A je obor hodnot jisté prosté rekurzívní funkce.

Důkaz (i) $\Rightarrow$ (ii) Nechť A je rekurzívně spočetná a neprázdná. Nechť $a \in A$ je její pevně zvolený prvek. Zvolme rekurzívní relaci R takovou, že $R \subseteq \mathrm{N}^2$ a $A = \{\, x \,;\, \exists y R(x,y) \,\}$. Definujme funkci f předpisem

$$f(z) = \begin{cases} (z)_0 & \text{když } R((z)_0,(z)_1) \\ a & \text{jinak.} \end{cases}$$

Kdykoliv platí $R((z)_0,(z)_1)$, pak $\exists y R((z)_0,y)$ a $(z)_0 \in A$. Tedy $\mathrm{Rng}(f) \subseteq A$. Když naopak $x \in A$, pak existuje y takové, že $R(x,y)$. Pro $z = \langle x,y\rangle$ platí $f(z) = x$. Tedy $A \subseteq \mathrm{Rng}(f)$.

(ii) $\Rightarrow$ (iii) Nechť A je nekonečná a nechť $A = \mathrm{Rng}(f)$, kde $f \in \mathit{FOR}$. V souvislosti s úvahami o zobecněné (ordinální) rekurzi jsme zdůvodnili, že funkce g definovaná z funkce f předpisem

$$g(x) = f(\mu y(f(y) \notin \{g(0),\ldots,g(x-1)\}))$$

je obecně rekurzívní. Lze zdůvodnit, že g je prostá a platí $\mathrm{Rng}(g) = \mathrm{Rng}(f)$.

(iii) $\Rightarrow$ (i) Nechť $A = \mathrm{Rng}(g)$, kde $g \in \mathit{FOR}$. Pak $A = \{\, y \,;\, \exists x(g(x) = y) \,\}$. Protože podmínka $g(x) = y$ je rekurzívní, je množina A rekurzívně spočetná dle věty 2.2.25. QED

K této větě poznamenejme, že nelze požadovat, aby prostá rekurzívní funkce g taková, že $\mathrm{Rng}(g) = A$, byla dokonce rostoucí. Některé rekurzívně spočetné množiny (cvičení 8 tvrdí, že všechny nerekurzívní) nejsou oborem hodnot žádné rostoucí rekurzívní funkce.

Řekneme, že množina $A \subseteq \mathrm{N}$ je *m-převeditelná* na množinu $B \subseteq \mathrm{N}$, a píšeme $A \leq_{\mathrm{m}} B$, existuje-li rekurzívní funkce g taková, že

$$\forall x(x \in A \Leftrightarrow g(x) \in B).$$

Jinak řečeno, $A \leq_{\mathrm{m}} B$ platí právě tehdy, existuje-li $g \in \mathit{FOR}$ taková, že $c_A = c_B \circ g$. Písmeno „m“ pochází od anglického „many-one“. V literatuře se totiž studuje také 1-převeditelnost: množina A je *1-převeditelná* na množinu B, jestliže existuje prostá rekurzívní funkce g splňující podmínku $\forall x(x \in A \Leftrightarrow g(x) \in B)$. Prostá se anglicky řekne „one-one“; písmeno „m“ v naší definici tedy naznačuje, že g nemusí být prostá. Platí-li $c_A = c_B \circ g$, říkáme také, že A je m-převeditelná na B *via* g.

Příklad 2.2.30 V důkazu věty 2.2.26 jsme zdůvodnili, že platí $\mathrm{K} \leq_{\mathrm{m}} \mathrm{K}_0$.

Lemma 2.2.31 *(a) Relace $\leq_{\mathrm{m}}$ je tranzitivní a reflexivní relace na množině $\mathcal{P}(\mathrm{N})$ všech podmnožin množiny* N.

(b) Když $A \leq_{\mathrm{m}} B$ *a* $B \in \mathsf{OR}$*, pak* $A \in \mathsf{OR}$*.*
(c) Když $A \leq_{\mathrm{m}} B$ *a* $B \in \mathsf{RS}$*, pak* $A \in \mathsf{RS}$*.*
(d) Když $A \leq_{\mathrm{m}} B$*, pak* $\overline{A} \leq_{\mathrm{m}} \overline{B}$*.*
(e) Když $A \in \mathsf{OR}$ *a* B *není* $\emptyset$ *ani* N*, pak* $A \leq_{\mathrm{m}} B$*.*
(f) Když $(A - B) \cup (B - A)$ *je konečná a* B *není* $\emptyset$ *ani* N*, pak* $A \leq_{\mathrm{m}} B$*.*

Důkaz Když $A \leq_{\mathrm{m}} B$ via g_1 a $B \leq_{\mathrm{m}} C$ via g_2, pak $A \leq_{\mathrm{m}} C$ via $g_2 \circ g_1$. Dále $A \leq_{\mathrm{m}} A$ via $x \mapsto x$.

Nechť $A \leq_{\mathrm{m}} B$ via g a $B \in \mathsf{RS}$. Dle věty o projekci k B existuje relace R taková, že $B = \{\, x \,;\, \exists y R(x, y) \,\}$. Platí $A = \{\, x \,;\, \exists y R(g(x), y) \,\}$. Protože podmínka $R(g(x), y)$ je rekurzívní, množina A je rekurzívně spočetná dle věty o projekci užité opačným směrem. Důkaz tvrzení (b) a (d) ponecháváme za cvičení.

V (e) zvolme čísla c a d taková, že $c \in B$ a $d \notin B$. Definujeme-li $g(x) = c$ pro $x \in A$ a $g(x) = d$ jinak, je funkce g rekurzívní dle lemmatu 2.2.16 a platí $A \leq_{\mathrm{m}} B$ via g.

V (f) opět zvolme $c \in B$ a $d \notin B$. Dále označme $E = A - B$ a $F = B - A$. Množiny E a F jsou konečné, tedy rekurzívní. Definujme $g(x) = c$ pro $x \in E$, dále $g(x) = d$ pro $x \in F$ a konečně $g(x) = x$ jinak. Funkce g je rekurzívní, protože ji lze odvodit (dvojím) užitím lemmatu 2.2.16, a platí $A \leq_{\mathrm{m}} B$ via g. QED

Příklad 2.2.32 Protože $\overline{\mathrm{K}} \notin \mathsf{RS}$ a $\mathrm{K} \in \mathsf{RS}$, z (c) plyne $\overline{\mathrm{K}} \not\leq_{\mathrm{m}} \mathrm{K}$. Z toho a z (d) plyne $\mathrm{K} \not\leq_{\mathrm{m}} \overline{\mathrm{K}}$. Množiny K a $\overline{\mathrm{K}}$ jsou tedy vůči relaci $\leq_{\mathrm{m}}$ nesrovnatelné.

Na m-převeditelnosti je důležité, že pro určité množiny A a B lze někdy dokázat, že platí $A \leq_{\mathrm{m}} B$, i když o žádné z množin A a B nevíme, je-li rekurzívní nebo rekurzívně spočetná. Zjistí-li se později například, že A *není* rekurzívní, podle tvrzení 2.2.31(a) to znamená, že ani B *není* rekurzívní. Analogicky lze užít tvrzení 2.2.31(b) k důkazu, že nějaká množina není rekurzívně spočetná. Příklady na tyto situace ještě uvidíme. Intuitivní význam podmínky $A \leq_{\mathrm{m}} B$ je „úloha A je z algoritmického hlediska jednodušší nebo stejně obtížná jako úloha B“. Relaci $\leq_{\mathrm{m}}$ můžeme tedy chápat jako uspořádání množin přirozených čísel podle algoritmické složitosti.

Řekneme, že množina B je *kompletní*, jestliže je rekurzívně spočetná a jestliže navíc platí $A \leq_{\mathrm{m}} B$ pro každou rekurzívně spočetnou množinu A.

Příklad 2.2.33 Podmínka $\forall x(x \in \mathrm{W}_a \Leftrightarrow \langle a, x \rangle \in \mathrm{K}_0)$ platí pro každou rekurzívně spočetnou množinu W_a. Protože funkce $x \mapsto \langle a, x \rangle$ je rekurzívní, znamená to $\forall a(\mathrm{W}_a \leq_{\mathrm{m}} \mathrm{K}_0)$. Množina K_0 je tedy kompletní.

Je-li množina B kompletní, pak není rekurzívní, a navíc máme plnou informaci o tom, jaké m-převeditelnosti platí mezi ní a ostatními rekurzívně spočetnými množinami: na množinu B jsou m-převeditelné všechny rekurzívně spočetné množiny, naopak B je m-převeditelná právě na ty rekurzívně spočetné množiny, které jsou kompletní.

Nechť $n \geq 1$. Řekneme, že množina $A \subseteq \mathrm{N}^k$ je *Σ_n-množina*, jestliže existuje rekurzívní relace $R \subseteq \mathrm{N}^{k+n}$ taková, že

$$A = \{\, [x_1, \ldots, x_k] \,;\, \exists v_1 \forall v_2 \exists \ldots v_n R(\underline{x}, \underline{v}) \,\}.$$

Podmínka A je tedy Σ_n-podmínkou, jestliže ji lze získat z rekurzívní podmínky pomocí n střídajících se kvantifikátorů, z nichž první (zleva) je existenční. Přitom poslední (neuvedený) kvantifikátor je existenční nebo univerzální podle toho, zda n je liché nebo sudé. Řekneme, že množina $A \subseteq \mathrm{N}^k$ je *Π_n-množina*, jestliže existuje rekurzívní relace $R \subseteq \mathrm{N}^{k+n}$ taková, že

$$A = \{\, [x_1, \ldots, x_k] \,;\, \forall v_1 \exists v_2 \ldots v_n R(\underline{x}, \underline{v}) \,\}.$$

Podmínka A je tedy Π_n-podmínkou, jestliže ji lze získat z rekurzívní podmínky pomocí n střídajících se kvantifikátorů, z nichž tentokrát první je univerzální a poslední je existenční nebo univerzální podle toho, zda n je sudé nebo liché. Označení Σ_n a Π_n budeme užívat i samostatně: Σ_n je množina všech Σ_n-relací, Π_n je množina všech Π_n-relací.

Příklad 2.2.34 Platí $\overline{\mathrm{K}} = \{\, x \,;\, \forall y \neg \mathrm{T}(x, x, y) \,\}$. Množina $\overline{\mathrm{K}}$ je tedy Π_1-množinou.

Lemma 2.2.35 *(a)* $\mathsf{RS} = \Sigma_1$, $\mathsf{OR} = \Sigma_1 \cap \Pi_1$.
(b) $A \in \Sigma_n \Leftrightarrow \overline{A} \in \Pi_n$, *a dále* $A \in \Pi_n \Leftrightarrow \overline{A} \in \Sigma_n$.
(c) Sjednocení a průnik k-árních Σ_n relací nebo k-árních Π_n-relací je opět Σ_n-relace nebo Π_n-relace. Jinými slovy, Σ_n-podmínky i Π_n-podmínky jsou uzavřeny na konjunkci a disjunkci.
(d) Σ_n-podmínky i Π_n-podmínky jsou uzavřeny na omezenou kvantifikaci.
(e) Σ_n-podmínky jsou uzavřeny na existenční kvantifikaci, Π_n-podmínky jsou uzavřeny na univerzální kvantifikaci.
(f) $\Sigma_n \cup \Pi_n \subseteq \Sigma_{n+1} \cap \Pi_{n+1}$.
(g) Když $A \leq_{\mathrm{m}} B$ *a* $B \in \Sigma_n$, *pak* $A \in \Sigma_n$. *Když* $A \leq_{\mathrm{m}} B$ *a* $B \in \Pi_n$, *pak* $A \in \Pi_n$.

Důkaz Tvrzení $\mathsf{RS} = \Sigma_1$ je věta o projekci. A i $\overline{A}$ je rekurzívně spočetná, právě když A je současně Σ_1 i Π_1. Tvrzení $\mathsf{OR} = \Sigma_1 \cap \Pi_1$ je tedy vlastně Postova věta.

Má-li podmínka $A(\underline{x})$ tvar $\forall v_1 \exists \ldots v_n R(\underline{x}, \underline{v})$, pak podmínka $\neg A(\underline{x})$ je ekvivalentní s $\exists v_1 \forall \ldots v_n \neg R(\underline{x}, \underline{v})$. Stejně lze zdůvodnit i zbývající tři implikace v (b).

Tvrzení (c), (d) a (e) dokážeme najednou indukcí podle n. Nechť tedy $n \geq 1$ je dáno. Předpokládejme, že je-li $n \geq 2$, pak Σ_{n-1}-podmínky jsou uzavřeny na konjunkci, disjunkci, omezenou kvantifikaci a existenční kvantifikaci, kdežto Π_{n-1}-podmínky jsou uzavřeny na konjunkci, disjunkci, omezenou kvantifikaci a univerzální kvantifikaci. Uvažujme o n. Nechť A je $(k+1)$-ární Σ_n-podmínka tvaru $\exists v P(\underline{x}, y, v)$, kde P je rekurzívní v případě, kdy $n = 1$, a P je Π_{n-1} jinak. Podmínka $\exists y \exists v P(\underline{x}, y, v)$, která vznikne z podmínky A existenční kvantifikací, je ekvivalentní s podmínkou $\exists w \exists y \leq w \exists v \leq w\, P(\underline{x}, y, v)$. Je-li $n = 1$, pak podmínka $\exists y \leq w \exists v \leq w\, P(\underline{x}, y, v)$ je rekurzívní dle 2.2.13. Je-li $n > 1$, tato podmínka je Π_{n-1}

dle indukčního předpokladu pro tvrzení (d). Úvaha pro druhou část tvrzení (e), uzavřenost Π_n-podmínek na univerzální kvantifikaci, je analogická, podmínka P je v tom případě rekurzívní nebo Σ_{n-1} a existenční kvantifikátory je třeba nahradit univerzálními. Nechť nyní $\exists v P(\underline{x}, v)$ a $\exists v Q(\underline{x}, v)$ jsou dvě Σ_n-podmínky, přičemž opět P a Q jsou rekurzívní, je-li $n = 1$, jinak jsou Π_{n-1}. Jejich konjunkce je ekvivalentní s $\exists v_1 \exists v_2 (P(\underline{x}, v_1)\ \&\ P(\underline{x}, v_2))$. Přitom podmínka $P(\underline{x}, v_1)\ \&\ P(\underline{x}, v_2)$ je rekurzívní dle 2.2.12 resp. je Π_{n-1} dle indukčního předpokladu pro tvrzení (c), podmínka $\exists v_1 \exists v_2 (..)$ je Σ_n dle již dokázaného tvrzení (e). Zbývající úvahy v (c) jsou podobné či zřejmé. Nechť konečně $\exists v P(\underline{x}, y, v)$ je Σ_n-podmínka, uvažujme podmínky $\exists y{<}z \exists v P(\underline{x}, y, v)$ a $\forall y{<}z \exists v P(\underline{x}, y, v)$. První z nich je ekvivalentní s $\exists v \exists y{<}z\, P(\underline{x}, y, v)$, druhá je ekvivalentní s $\exists w \forall y{<}z \exists v{<}w\, P(\underline{x}, y, v)$. Opět platí, že obě tyto podmínky jsou Σ_n vzhledem k tvrzení 2.2.13 či díky indukčnímu předpokladu pro tvrzení (d). Úvahy pro kvantifikátory $\exists y{\leq}z$ a $\forall y{\leq}z$ a pro Π_n-podmínky jsou opět analogické.

Když A je Σ_n-podmínka tvaru $\exists v_1 \forall .. v_n R(\underline{x}, \underline{v})$ a v rekurzívní podmínce R se nic nepraví o y, pak A je ekvivalentní s podmínkou $\forall y \exists v_1 \forall .. v_n R(\underline{x}, \underline{v})$, která je Π_{n+1}, s podmínkou $\exists v_1 \forall .. v_n \exists y R(\underline{x}, \underline{v})$, která je Σ_{n+1} pro n sudé, a také s podmínkou $\exists v_1 \forall .. v_n \forall y R(\underline{x}, \underline{v})$, která je Σ_{n+1} pro n liché. Zbývající úvahy včetně důkazu tvrzení (g) ponecháváme za cvičení. QED

Příklad 2.2.36 Pokusme se pro množinu $\mathrm{Unb} = \{\, x\,;\, \mathrm{W}_x \text{ je nekonečná} \,\}$ stanovit její aritmetickou klasifikaci, tj. najít pokud možno minimální n takové, že $\mathrm{Unb} \in \Sigma_n$ nebo $\mathrm{Unb} \in \Pi_n$. Platí

$$\mathrm{W}_x \text{ je nekonečná} \Leftrightarrow \forall v_1 \exists v_2 (v_1 < v_2\ \&\ v_2 \in \mathrm{W}_x).$$

Podmínka $v_1 < v_2$ je primitivně rekurzívní, tedy rekurzívně spočetná. Podmínka v závorce je rekurzívně spočetná díky 2.2.35(c). Podmínka $\exists v_2 (..)$ je Σ_1 vzhledem k tvrzení 2.2.35 (a) a (e). Platí tedy $\mathrm{Unb} \in \Pi_2$.

Příklad 2.2.37 Dále položme $\mathrm{Rec} = \{\, x\,;\, \mathrm{W}_x \text{ je rekurzívní} \,\}$ a pokusme se i pro tuto množinu stanovit její aritmetickou klasifikaci. Platí

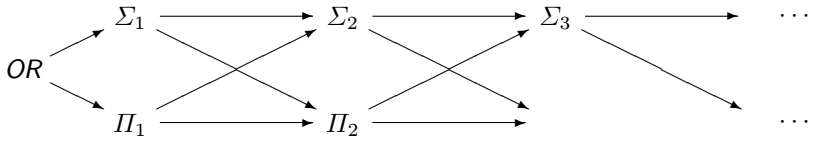
$$\begin{aligned} \mathrm{W}_x \text{ je rekurzívní} &\Leftrightarrow \exists y (\mathrm{W}_y = \overline{\mathrm{W}_x}) \\ &\Leftrightarrow \exists y \forall v ((v \in \mathrm{W}_y\ \&\ v \notin \mathrm{W}_x)\ \vee\ (v \notin \mathrm{W}_y\ \&\ v \in \mathrm{W}_x)). \end{aligned}$$

Podmínka $v \in \mathrm{W}_y$ je Σ_1, podmínka $v \notin \mathrm{W}_x$ je Π_1. Jejich konjunkce je vzhledem k 2.2.35 (f) a (c) současně Σ_2 i Π_2. Totéž platí o podmínce $v \notin \mathrm{W}_y\ \&\ v \in \mathrm{W}_x$. Disjunkce těchto dvou podmínek je tedy také současně Σ_2 i Π_2. Výhodnější je prohlásit, že je Π_2. V tom případě, díky 2.2.35(e), i $\forall v (..)$ je Π_2, a tudíž množina Rec je Σ_3.

Inkluze mezi množinami OR, Σ_n a Π_n pro $n \geq 1$ jsou na obrázku 2.2.4 znázorněny šipkami. Tento diagram je jedním z nejdůležitějších v celé logice. Například v příručce [4] jej lze nalézt nejméně na třech různých místech.

Lemma 2.2.38 *Když $\Sigma_n \subseteq \Pi_n$ nebo $\Pi_n \subseteq \Sigma_n$, pak pro každé $m \geq n$ platí $\Sigma_m = \Pi_m = \Sigma_n$.*

Důkaz Předpokládejme $\Sigma_n \subseteq \Pi_n$. Nechť $A \in \Pi_n$. Pak $\overline{A} \in \Sigma_n$ dle (b) lemmatu 2.2.35. Z předpokladu $\Sigma_n \subseteq \Pi_n$ plyne $\overline{A} \in \Pi_n$. Opětovné užití tvrzení 2.2.35(b) dává $A \in \Sigma_n$. Tedy $\Sigma_n = \Pi_n$. Nechť A je libovolná Σ_{n+1}-podmínka tvaru $\exists v P(\underline{x}, v)$, kde $P \in \Pi_n$. Z inkluze $\Pi_n \subseteq \Sigma_n$ a z 2.2.35(e) plyne $A \in \Sigma_n$. Toto platí pro každou $A \in \Sigma_{n+1}$, tedy $\Sigma_{n+1} \subseteq \Sigma_n = \Pi_n$. A tak dále. QED



Obrázek 2.2.4: Aritmetická hierarchie

Pokud tedy kterákoliv z inkluzí znázorněných na obrázku 2.2.4 je ve skutečnosti rovností, tj. platí-li pro kterékoliv n některá z podmínek $\Sigma_n = \Sigma_{n+1}$, $\Pi_n = \Pi_{n+1}$, $\Sigma_n = \Pi_{n+1}$ nebo $\Pi_n = \Sigma_{n+1}$, pak Σ_{n+1} i Π_{n+1} je sjednocením všech množin Σ_m a Π_m. Takové situaci se říká *kolaps aritmetické hierarchie*. Dále budeme směřovat k důkazu, že nic takového nenastává, aritmetická hierarchie nekolabuje.

Množina B je *Σ_n-kompletní*, platí-li $B \in \Sigma_n$ a navíc $A \leq_{\mathrm{m}} B$ pro každou množinu $A \in \Sigma_n$. Analogicky definujeme, že množina B je *Π_n-kompletní*, platí-li $B \in \Pi_n$ a navíc $A \leq_{\mathrm{m}} B$ pro každou $A \in \Pi_n$. Relace $Q \subseteq \mathrm{N}^2$ je *Σ_n-univerzální*, jestliže $Q \in \Sigma_n$ a jestliže pro každou Σ_n-množinu $A \subseteq \mathrm{N}$ existuje číslo a takové, že $A = \{\, v \,;\, Q(a, v) \,\}$. Analogicky definujeme, že relace Q je *Π_n-univerzální*, jestliže $Q \in \Pi_n$ a pro každou $A \in \Pi_n$ existuje a takové, že $A = \{\, v \,;\, Q(a, v) \,\}$. Definujme následující posloupnost relací a dvě posloupnosti množin:

$$\begin{aligned}
\mathrm{Q}_1 &= \{\, [x, v] \,;\, v \in \mathrm{W}_x \,\},\\
\mathrm{Q}_{n+1} &= \{\, [x, v] \,;\, \exists y \neg \mathrm{Q}_n(x, \langle v, y \rangle) \,\},\\
\mathrm{H}_n &= \{\, \langle x, v \rangle \,;\, \mathrm{Q}_n(x, v) \,\},\\
\mathrm{D}_n &= \{\, x \,;\, \mathrm{Q}_n(x, x) \,\}.
\end{aligned}$$

Evidentně platí $\mathrm{H}_1 = \mathrm{K}_0$ a $\mathrm{D}_1 = \mathrm{K}$. Dále lze snadno ukázat (indukcí), že $\mathrm{Q}_n \in \Sigma_n$. Platí tedy i $\mathrm{H}_n \in \Sigma_n$ a $\mathrm{D}_n \in \Sigma_n$.

Věta 2.2.39 *(a) Každá Q_n je Σ_n-univerzální, každá $\overline{\mathrm{Q}_n}$ je Π_n-univerzální.*
(b) H_n je Σ_n-kompletní, $\overline{\mathrm{H}_n}$ je Π_n-kompletní.
(c) $\mathrm{D}_n \in \Sigma_n - \Pi_n$ a $\overline{\mathrm{D}_n} \in \Pi_n - \Sigma_n$.

Důkaz Platí $\{\, v \,;\, \mathrm{Q}_1(a, v) \,\} = \mathrm{W}_a$. Každá rekurzívně spočetná množina je tedy jednou z množin $\{\, v \,;\, \mathrm{Q}_1(a, v) \,\}$ pro $a \in \mathrm{N}$. Relace Q_1 je tudíž Σ_1-univerzální. Dále postupujme indukcí. Nechť Q_n je Σ_n-univerzální a nechť $A = \{\, v \,;\, \exists y P(v, y) \,\}$,

kde $P \in \Pi_n$, je daná Σ_{n+1}-množina. Množina $C = \{ \langle v, y\rangle \,;\, \neg P(v,y) \}$ je Σ_n. Vzhledem k Σ_n-univerzálnosti relace Q_n tedy existuje a takové, že

$$\forall v \forall y(\langle v, y\rangle \in C \;\Leftrightarrow\; \mathrm{Q}_n(a, \langle v, y\rangle)).$$

Platí tedy

$$\forall v \forall y(\neg P(v,y) \;\Leftrightarrow\; \mathrm{Q}_n(a, \langle v, y\rangle)),$$
$$\forall v(\exists y P(v,y) \;\Leftrightarrow\; \exists y \neg \mathrm{Q}_n(a, \langle v, y\rangle)).$$

Tedy $A = \{ v \,;\, \mathrm{Q}_{n+1}(a, v) \}$. Relace Q_{n+1} je Σ_{n+1}-univerzální.

Nechť je dána libovolná Σ_n množina A. Víme $A = \{ v \,;\, \mathrm{Q}_n(a,v) \}$ pro jisté a. Platí $A \leq_{\mathrm{m}} \mathrm{H}_n$ via $v \mapsto \langle a, v\rangle$. Množina H_n je tedy Σ_n-kompletní.

Předpokládejme $\mathrm{D}_n \in \Pi_n$. Pak $\overline{\mathrm{D}_n} \in \Sigma_n$. Existuje tedy a takové, že

$$\forall v(v \notin \mathrm{D}_n \;\Leftrightarrow\; \mathrm{Q}_n(a,v)).$$

Zvolme $v = a$. Ekvivalence $a \notin \mathrm{D}_n \;\Leftrightarrow\; \mathrm{Q}_n(a,a)$ znamená spor.

Důkazy druhých částí všech tří tvrzení (a), (b) a (c) jsou analogické a ponecháváme je za cvičení. QED

Z tvrzení (c) věty plyne, že neplatí žádná z inkluzí $\Sigma_n \subseteq \Pi_n$ či $\Pi_n \subseteq \Sigma_n$. Aritmetická hierarchie tedy nekolabuje, všechny inkluze v obrázku 2.2.4 jsou ostré. V každé množině Σ_n i Π_n existují nejsložitější množiny, totiž Σ_n-kompletní resp. Π_n-kompletní množiny.

Obraťme nyní pozornost zpět k částečně rekurzívním funkcím a k rekurzívně spočetným množinám. Poslední problematika tohoto oddílu je *věta o parametrech*. Nechť ψ je částečná funkce $n+m$ proměnných. Zápis $\lambda v_1, \ldots, v_m \psi(\underline{x}, \underline{v})$ označuje funkci $[v_1, \ldots, v_m] \mapsto \psi(\underline{x}, \underline{v})$, tj. funkci, která je z funkce ψ odvozena dosazením konstant za prvních n proměnných. Je-li ψ částečně rekurzívní, pak ovšem i každá z funkcí $\lambda v_1, \ldots, v_m \psi(\underline{v}, \underline{x})$ je částečně rekurzívní. Následující věta tvrdí, že (některý) index funkce $\lambda v_1, \ldots v_m \psi(\underline{x}, \underline{v})$ lze stanovit algoritmem na základě vstupů $e, x_1, \ldots, x_n$, kde e je libovolný index původní funkce ψ.

Věta 2.2.40 (o parametrech) *Pro každou dvojici nenulových čísel n a m existuje rekurzívní funkce s_n^m, která je funkcí $n+1$ proměnných, taková, že pro každé e a $x_1, \ldots, x_n$ platí*

$$\varphi^{(m)}_{\mathrm{s}_n^m(e, \underline{x})} = \lambda v_1, \ldots, v_m(\varphi_e^{(n+m)}(\underline{x}, \underline{v})).$$

Náznak důkazu Víme, že index e funkce $\varphi_e^{(n+m)}$ můžeme považovat za kód programu P, který počítá funkci $\varphi_e^{(n+m)}$. Program P, kdykoliv je spuštěn, požaduje (čte ze vstupní pásky) $n+m$ vstupů $x_1, \ldots, x_n$ a $v_1, \ldots, v_m$. Jsou-li vstupy $x_1, \ldots, x_n$ konstantní, tj. známe-li je předem v době programování, můžeme program P upravit na program P', který čísla $x_1, \ldots, x_n$ „zná“ a požaduje pouze vstupy $v_1, \ldots, v_m$. Tato úprava například v jazyce Pascal znamená některé příkazy `read` nebo `readln` nahradit deklaracemi konstant; v jazyce RASP znamená některé instrukce `read` nahradit

instrukcemi `mov`. Program P' je ovšem jiný pro každou volbu konstant $x_1, \ldots, x_n$. Úprava, kterou vznikne program P' z programu P a čísel $x_1, \ldots, x_n$, je zcela mechanická a může ji provádět nějaký program S. Funkce, kterou počítá program S, je hledanou funkcí s_n^m. QED

Věta o parametrech tedy tvrdí, že existuje program, který do daného programu zapracuje dané konstanty, takže výsledný program pak požaduje menší množství vstupů. Podrobný důkaz věty 2.2.40 lze nalézt v knize [61]. Někteří autoři větu o parametrech nazývají „věta s-n-m“.

Věta 2.2.41 *(a) Nechť ψ je částečně rekurzívní funkce $n+m$ proměnných. Pak existuje obecně rekurzívní funkce g, která je funkcí n proměnných a která pro každá $x_1, \ldots, x_k$ splňuje*

$$\varphi^{(m)}_{g(\underline{x})} = \lambda v_1, \ldots, v_m \psi(\underline{x}, \underline{v}).$$

(b) Nechť Q je rekurzívně spočetná $(n+m)$-ární relace. Pak existuje rekurzívní funkce g, která je funkcí n proměnných a která pro každá $x_1, \ldots, x_n$ splňuje

$$\mathrm{W}^{(m)}_{g(\underline{x})} = \{\, [v_1, \ldots, v_m] \,;\, Q(\underline{x}, \underline{v}) \,\}.$$

Důkaz Tvrzení (a) plyne bezprostředně z věty 2.2.40, stačí zvolit nějaký index e funkce ψ a za funkci g vzít funkci $[x_1, \ldots, x_n] \mapsto \mathrm{s}_n^m(e, \underline{x})$. V (b) stačí k dané relaci Q zvolit funkci ψ takovou, že $\mathrm{Dom}(\psi) = Q$, a užít tvrzení (a). QED

Příklad 2.2.42 Nechť $A \subseteq \mathrm{N}$ je libovolná Π_2-množina. Víme, že k A existuje rekurzívní relace $R \subseteq \mathrm{N}^3$ taková, že $A = \{\, x \,;\, \forall v \exists y R(x, v, y) \,\}$. Definujme funkci ψ dvou proměnných předpisem $\psi(x, v) \simeq \mu y R(x, v, y)$. Platí-li $x \in A$, pak $\forall v ! \psi(x, v)$ a funkce $\lambda v \psi(x, v)$ je totální. Platí-li $x \notin A$, pak naopak funkce $\lambda v \psi(x, v)$ není totální. Nyní užijme větu 2.2.41(a) a vezměme funkci g takovou, že $g(x)$ je index funkce $\lambda v \psi(x, v)$. Platí

$$x \in A \Leftrightarrow \varphi_{g(x)} \text{ je totální.}$$

Označme Tot množinu $\{\, x \,;\, \varphi_x \text{ je totální} \,\}$. Právě jsme zjistili, že $A \leq_{\mathrm{m}} \mathrm{Tot}$ platí pro každou množinu $A \in \Pi_2$. Protože lze snadno ověřit, že $\mathrm{Tot} \in \Pi_2$, dokázali jsme tím, že Tot je Π_2-kompletní. To dále znamená $\mathrm{Tot} \notin \Sigma_2$, $\mathrm{Tot} \notin \Pi_1$ a $\mathrm{Tot} \notin \Sigma_1$. Vidíme tedy, že chceme-li podmínku „φ_x je totální“ vyjádřit pomocí rekurzívní podmínky a kvantifikátorů, nestačí jeden kvantifikátor; dva kvantifikátory stačí, ale první musí být univerzální a druhý musí být existenční.

Příklad 2.2.43 Nechť $B = \{\, x \,;\, \mathrm{W}_x \neq \emptyset \,\} = \{\, x \,;\, \exists y (y \in \mathrm{W}_x) \,\}$. Podmínka $y \in \mathrm{W}_x$ je rekurzívně spočetná, díky tvrzení (e) lemmatu 2.2.35 tedy platí $B \in \mathit{RS}$. Nechť A je libovolná rekurzívně spočetná množina. Definujme relaci Q jako množinu $\{[x, v]; x \in A\}$. Relace Q je rekurzívně spočetná. Když $x \in A$, pak $\{v; Q(x, v)\} = \mathrm{N}$, jinak $\{\, v \,;\, Q(x, v) \,\} = \emptyset$. Užijme na relaci Q tvrzení 2.2.41(b): existuje $g \in \mathit{FOR}$ taková, že $x \in A \Leftrightarrow \mathrm{W}_{g(x)} \neq \emptyset$. Platí $A \leq_{\mathrm{m}} B$ via g. Protože množina A byla libovolná, dokázali jsme, že B je kompletní množina. Platí tedy $B \notin \mathit{OR}$ a $\overline{B} \notin \mathit{RS}$.

Příklad 2.2.44 Nechť B je pevně zvolená rekurzívně spočetná množina. Ověříme, že existuje rekurzívní funkce g taková, že pro každé x platí $\mathrm{W}_{g(x)} = B \cup \mathrm{W}_x$. K tomu stačí užít tvrzení 2.2.41(b) na relaci $Q = \{\, [x,v]\,;\, v \in B \,\vee\, v \in \mathrm{W}_x \,\}$; platí $Q \in \mathsf{RS}$ a $\{\, v\,;\, Q(x,v)\,\} = B \cup \mathrm{W}_x$.

V příkladu 2.2.43 jsme dokázali, že ke každé množině $A \in \mathsf{RS}$ existuje rekurzívní funkce g taková, že $\mathrm{W}_{g(x)} = \mathrm{N}$ pro $x \in A$ a $\mathrm{W}_{g(x)} = \emptyset$ pro $x \notin A$. Z toho plyne $x \in A \;\Leftrightarrow\; g(x) \in \mathrm{W}_{g(x)}$, a tedy $x \in A \;\Leftrightarrow\; g(x) \in \mathrm{K}$. Tím je dokázáno, že množina K, čili množina D_1, je Σ_1-kompletní. Složitější, ale podobnou úvahou by bylo možno ověřit, že množina D_n je Σ_n-kompletní pro každé n.

Předpokládejme, že B je nějaká rekurzívně spočetná nerekurzívní množina. Z věty 2.2.27 plyne, že $\overline{B} \notin \mathsf{RS}$. Množina $\overline{B}$ se tedy liší od všech množin W_x. Platí tedy

$$\forall x \exists y((y \notin B \;\&\; y \notin \mathrm{W}_x) \;\vee\; (y \in B \;\&\; y \in \mathrm{W}_x)).$$

To lze přepsat na

$$\forall x \exists y(y \in B \;\Leftrightarrow\; y \in \mathrm{W}_x).$$

Někdy se může stát, že (některé) číslo y splňující podmínku $y \in B \;\Leftrightarrow\; y \in \mathrm{W}_x$, čili dosvědčující, že $\overline{B} \neq \mathrm{W}_x$, lze z čísla x určit algoritmem. V tom případě řekneme, že množina B je efektivně nerekurzívní.

Definice 2.2.45 *Množina B je* efektivně nerekurzívní, *jestliže $B \in \mathsf{RS}$ a jestliže navíc existuje rekurzívní funkce f taková, že $\forall x(f(x) \in B \;\Leftrightarrow\; f(x) \in \mathrm{W}_x)$.*

Efektivně nerekurzívní množina samozřejmě není rekurzívní. Platí ale víc.

Věta 2.2.46 *Množina $B \subseteq \mathrm{N}$ je efektivně nerekurzívní, právě když je kompletní.*

Důkaz Nechť B je efektivně nerekurzívní a nechť rekurzívní funkce f splňuje podmínku $\forall x(f(x) \in B \;\Leftrightarrow\; f(x) \in \mathrm{W}_x)$. Nechť libovolná rekurzívně spočetná množina A je dána. Zvolme k A rekurzívní funkci g takovou, že $\mathrm{W}_{g(x)} = \mathrm{N}$ pro $x \in A$ a $\mathrm{W}_{g(x)} = \emptyset$ pro $x \notin A$. Existenci takové funkce jsme dokázali v příkladu 2.2.43. Platí

$$x \in A \;\Leftrightarrow\; \mathrm{W}_{g(x)} = \mathrm{N} \;\Rightarrow\; f(g(x)) \in \mathrm{W}_{g(x)} \;\Leftrightarrow\; f(g(x)) \in B,$$
$$x \notin A \;\Leftrightarrow\; \mathrm{W}_{g(x)} = \emptyset \;\Rightarrow\; f(g(x)) \notin \mathrm{W}_{g(x)} \;\Leftrightarrow\; f(g(x)) \notin B.$$

Takže $A \leq_{\mathrm{m}} B$ via $f \circ g$.

Nechť naopak B je kompletní. Tedy $A \leq_{\mathrm{m}} B$ pro každou $A \in \mathsf{RS}$. Zvolme $A = \mathrm{K}$: existuje rekurzívní funkce f taková, že $\forall x(x \in \mathrm{K} \;\Leftrightarrow\; f(x) \in B)$. Zvolme funkci $g \in \mathsf{FOR}$, která splňuje podmínku $\forall x(\mathrm{W}_{g(x)} = \{\, v\,;\, f(v) \in \mathrm{W}_x\,\})$. Existenci takové funkce g zaručuje tvrzení 2.2.41(b) (cvičení). Platí

$$f(g(x)) \in B \;\Leftrightarrow\; g(x) \in \mathrm{K} \;\Leftrightarrow\; g(x) \in \mathrm{W}_{g(x)} \;\Leftrightarrow\; f(g(x)) \in \mathrm{W}_x.$$

Funkce $f \circ g$ tedy dosvědčuje, že B je efektivně nerekurzívní. QED

Věta 2.2.47 *Existují rekurzívně spočetné množiny A a B takové, že $A \cap B = \emptyset$, a navíc každá rekurzívně spočetná množina C splňující podmínky $A \subseteq C$ a $C \cap B = \emptyset$ nebo podmínky $B \subseteq C$ a $A \cap C = \emptyset$ je efektivně nerekurzívní, tedy kompletní.*

Důkaz Definujme množiny A a B takto:

$$A = \{\, z \,;\, \exists w(\mathrm{T}((z)_0, z, w) \;\&\; \forall v{<}w\, \neg\mathrm{T}((z)_1, z, v)) \,\},$$
$$B = \{\, z \,;\, \exists w(\mathrm{T}((z)_1, z, w) \;\&\; \forall v{\leq}w\, \neg\mathrm{T}((z)_0, z, v)) \,\}.$$

Množina A je tedy množinou takových z, že začneme-li od nuly a probíráme-li větší a větší svědky w, někdy se zjistí $z \in \mathrm{W}_{(z)_0}$, a to ne později, než by se zjistilo $z \in \mathrm{W}_{(z)_1}$. Množina B je naopak množinou takových z, že $z \in \mathrm{W}_{(z)_1}$ se zjistí dříve než $z \in \mathrm{W}_{(z)_0}$.

Nechť množina C je taková, že $A \subseteq C$ a $C \cap B = \emptyset$. Zvolme pevně nějaký index c množiny C. Tedy $\mathrm{W}_c = C$. Zvolme k množině B funkci g splňující podmínku $\forall x(\mathrm{W}_{g(x)} = B \cup \mathrm{W}_x)$. Existenci takové funkce g jsme dokázali v příkladu 2.2.44. Ověřme, že funkce f definovaná předpisem $f(x) = \langle g(x), c\rangle$ dosvědčuje, že C je efektivně nerekurzívní. Nechť $f(x) \in C$. Protože $C \cap B = \emptyset$, máme $f(x) \notin B$. Dokažme sporem, že $f(x) \in \mathrm{W}_x$. Když ne, pak $f(x) \notin B \cup \mathrm{W}_x$, čili $f(x) \notin \mathrm{W}_{g(x)}$. Platí $(f(x))_0 = g(x)$, $(f(x))_1 = c$, událost $f(x) \in \mathrm{W}_{(f(x))_1}$ má nějakého svědka w, a každý takový svědek w je menší než jakýkoliv svědek pro $f(x) \in \mathrm{W}_{(f(x))_0}$, protože $f(x) \in \mathrm{W}_{(f(x))_0}$ neplatí. Tedy $f(x) \in B$, spor. Nechť naopak $f(x) \in \mathrm{W}_x$. Pak $f(x) \in \mathrm{W}_x \cup B$, tedy $f(x) \in \mathrm{W}_{g(x)} = \mathrm{W}_{(f(x))_0}$. Dokažme sporem, že $f(x) \in C$. Kdyby ne, pak událost $f(x) \in \mathrm{W}_{(f(x))_0}$ má svědka, událost $f(x) \in \mathrm{W}_{(f(x))_1}$ jej nemá, tedy $f(x) \in A$, a to je spor s $A \subseteq C$.

Druhý případ, kdy $B \subseteq C$ a $A \cap B = \emptyset$, je analogický. QED

Nápad vyskytující se v předchozím důkazu, totiž uvažovat, která ze dvou slučitelných událostí má menšího svědka, pochází od Rossera a ještě se s ním setkáme v kapitole 4.

Na závěr poznamenejme, že věty 2.2.46 a 2.2.47 jsme formulovali tak, abychom se obešli bez řady důležitých pojmů. Množiny A a B z důkazu věty 2.2.47 jsou *efektivně neoddělitelné*. Jsou-li A a B libovolné efektivně neoddělitelné množiny, pak každá nadmnožina jedné z nich, která je disjunktní s druhou, je *kreativní*, a dále kreativní množiny jsou přesně ty, které jsou kompletní. Zájemce o tuto nesmírně zajímavou problematiku odkazujeme na knihy [71] a [61]. V kapitole 4 vystačíme s materiálem z tohoto oddílu.

Existují rekurzívně spočetné množiny, které nejsou rekurzívní ani kompletní? Existují rozumně definované pojmy převeditelnosti odlišné od pojmu m-převeditelnosti? Asi by měly existovat, například proto, že některé množiny nejsou m-převeditelné na svůj komplement, ale z intuitivního hlediska je rozhodování o náležení do libovolné množiny A stejně obtížné jako rozhodování o náležení do jejího komplementu $\overline{A}$. O těchto otázkách si také lze přečíst v [71] a [61].

Cvičení

1. Dokažte podrobně, že funkce $[x, y] \mapsto x \cdot y$ je primitivně rekurzívní.

2. Odvoďte násobení tří činitelů, tj. funkci $[x, y, z] \mapsto x \cdot y \cdot z$, několikerým užitím operace substituce (bez užití operace primitivní rekurze) z funkce $[x, y] \mapsto x \cdot y$.

3. Nechť $A \subseteq \mathrm{N}^{k+1}$ je rekurzívní množina a nechť $\psi(\underline{x})$ je $\min\{\, y \,;\, A(\underline{x}, y) \,\}$, když $\exists y A(\underline{x}, y)$, a $\psi(\underline{x})$ je nedefinováno v ostatních případech. Zdůvodněte, že funkce ψ je částečně rekurzívní.

4. Dokažte, že každá jednoprvková podmnožina množiny N^k je primitivně rekurzívní. Dokažte, že podmínky $x < y$, $x \leq y$ a $x = y$ jsou primitivně rekurzívní.

5. Nechť ψ je částečná funkce k proměnných. Definujme graf funkce ψ jako množinu $\mathrm{Graf}(\psi) = \{\, [\underline{x}, z] \,;\, \psi(\underline{x}) = z \,\}$. Množina $\mathrm{Graf}(\psi)$ je tedy totéž co funkce ψ chápaná způsobem obvyklým v teorii množin, tj. chápaná jako množina $(k+1)$-tic. Dokažte, že graf primitivně rekurzívní funkce je primitivně rekurzívní množina. Dále dokažte, že totální funkce je rekurzívní, právě když její graf je rekurzívní množina.

6. Zdůvodněte užitím lemmatu 2.2.13, že vlastnosti „x je sudé“ a „x je mocnina dvojky“ a podmínka „x a y jsou nesoudělná“ jsou primitivně rekurzívní.

7. Dokažte, že je-li f libovolná obecně rekurzívní funkce k proměnných, pak její obor hodnot $\mathrm{Rng}(f)$ je rekurzívně spočetná množina.

8. Je-li f rostoucí rekurzívní nebo primitivně rekurzívní funkce jedné proměnné, pak $\mathrm{Rng}(f)$ je rekurzívní resp. primitivně rekurzívní množina. Dokažte.

   Návod. Nejprve dokažte indukcí podle x, že pro každé x platí $x \leq f(x)$. Pak užijte lemma 2.2.13 a cvičení 5.

9. Musí být funkce f primitivně rekurzívní, jestliže má primitivně rekurzívní graf, je totální a platí $\mathrm{Rng}(f) \subseteq \{0, 1\}$?

   Návod. Odvoďte funkci f větvením, tj. užijte lemma 2.2.16.

10. Nechť pro funkce f a g jedné proměnné platí $\forall x(f(x) \leq g(x))$, nechť f má primitivně rekurzívní graf a nechť g je primitivně rekurzívní. Pak i f je primitivně rekurzívní. Dokažte.

    Návod. Užijte lemma 2.2.17.

11. Dokažte, že částečná funkce má rekurzívní graf, právě když ji lze odvodit jedním užitím operace minimalizace z jisté obecně rekurzívní funkce.

12. Nechť pro funkce ψ a f jedné proměnné platí $\forall x(!\psi(x) \Rightarrow \psi(x) \leq f(x))$, nechť f je rekurzívní a nechť ψ má rekurzívní graf. Musí funkce ψ mít rekurzívní definiční obor?

13. Každá nekonečná rekurzívní množina je oborem hodnot jisté rostoucí obecně rekurzívní funkce. Dokažte.

    Návod. Přizpůsobte důkaz o tom, že rostoucí posloupnost všech prvočísel je primitivně rekurzívní.

14. Je-li g totální funkce jedné proměnné s nekonečným oborem hodnot a platí-li pro každé x, že $f(x) = g(\mu y(g(y) \notin \{f(0), .., f(x-1)\}))$, pak funkce f je totální, prostá a má stejný obor hodnot jako funkce g. Dokažte.

    Návod. Dokažte indukcí podle y, že platí-li $|\{g(0), .., g(y-1)\}| = x$, pak $\{g(0), .., g(y-1)\} = \{f(0), .., f(x-1)\}$.

15. Dokažte podrobně pomocí lemmatu 2.2.20, že jsou-li funkce f a g jako v předchozím cvičení a je-li g rekurzívní, pak i f je rekurzívní. Na jakou funkci h se přitom aplikuje lemma 2.2.20?

16. Změnila by se třída všech funkcí odvoditelných ze základních funkcí pomocí primitivní rekurze, substituce a minimalizace, kdybychom přijali omezení, že primitivní rekurzi a minimalizaci je povoleno použít jen na totální funkce?

    Návod. Použijte větu o normální formě.

17. Rozhodněte, zda graf a definiční obor funkcí α a β definovaných předpisem

$$\alpha(x) \simeq \mu y \mathrm{T}(x, x, y), \qquad \beta(x) \simeq \mathrm{z}(\mu y \mathrm{T}(x, x, y)),$$

    kde z je konstantní funkce s hodnotou nula, jsou obecně rekurzívní.

18. Uvažujte třídu všech funkcí, které mají odvození, v němž jsou všechny tři operace použity vždy jen na totální funkce. Obsahuje tato třída i nějaké netotální funkce? Obsahuje tato třída všechny obecně rekurzívní funkce? Obsahuje tato třída všechny částečně rekurzívní funkce?

    Návod. Zdůvodněte, že má-li netotální funkce ψ odvození, v němž jsou všechny operace použity pouze na totální funkce, pak ψ splňuje podmínku z cvičení 11, a má tedy rekurzívní graf. V předchozím cvičení se ale vyskytla částečně rekurzívní funkce, která nemá rekurzívní graf.

19. Dokažte, že funkce ψ definovaná předpisem $\psi(x) \simeq 1 \dot{-} \varphi_x(x)$ je částečně rekurzívní funkce, která nemá žádné rekurzívní prodloužení, tj. která (jako množina dvojic) není podmnožinou žádné rekurzívní funkce jedné proměnné.

    Návod. Nechť f je rekurzívní prodloužení funkce ψ a nechť e je některý index funkce f. Uvažujte o hodnotách $f(e)$ a $\psi(e)$.

20. Řekneme, že množiny A a B jsou *rekurzívně oddělitelné*, jestliže existuje rekurzívní množina D taková, že $A \subseteq D$ a $D \cap B = \emptyset$. V opačném případě jsou *rekurzívně neoddělitelné*. Dokažte, že existují disjunktní rekurzívně spočetné množiny, které jsou rekurzívně neoddělitelné.

    Návod. Položte $A = \{\, x \,;\, \psi(x) \simeq 0 \,\}$ a $B = \{\, x \,;\, \psi(x) \simeq 1 \,\}$, kde ψ je funkce z předchozího cvičení.

21. Když A a B jsou rekurzívně spočetné množiny takové, že $A \cap B = \emptyset$ a $A \cup B$ je rekurzívní, pak A i B je rekurzívní.

22. Nechť A a B jsou rekurzívně spočetné množiny takové, že $A \cup B = \mathrm{N}$. Dokažte, že existuje rekurzívní množina D taková, že $A - B \subseteq D$ a $B - A \subseteq \overline{D}$.

    Zobecněte důkaz Postovy věty.

23. Dokažte tvrzení, které je v knize [61] nazváno věta o redukci: ke každým dvěma rekurzívně spočetným množinám A a B existují disjunktní rekurzívně spočetné množiny A' a B' takové, že $A - B \subseteq A'$, $B - A \subseteq B'$ a $A' \cup B' = A \cup B$.

    Návod. Buď zobecněte Postovu větu ještě dále, a místo funkcí f a g uvažovaných v jejím důkazu užijte funkce γ a ψ definované předpisy

    $$\gamma(x) \simeq \mu y(P(x,y) \ \vee \ Q(x,y)),$$
    $$\psi(x) \simeq \mathrm{c}_P(x,\gamma(x)) \dot{-} \mathrm{c}_Q(x,\gamma(x)),$$

    nebo užijte větu 2.2.28 na relaci $\{\, [x,1] \,;\, x \in A \,\} \cup \{\, [x,0] \,;\, x \in B \,\}$.

24. Rozhodněte, zda platí: je-li $A \subseteq \mathrm{N}^2$ rekurzívně spočetná relace taková, že $\forall x \exists y A(x,y)$, pak existuje rekurzívní funkce g taková, že pro každé x platí $g(x) = \min\{\, y \,;\, A(x,y) \,\}$.

    Návod. Uvažujte relaci $A = \{\, [x,y] \,;\, x \in \mathrm{K} \ \vee \ y \geq 1 \,\}$.

25. Vyvoďte z cvičení 22, že každé dvě disjunktní Π_1-množiny jsou rekurzívně oddělitelné.

26. Navrhněte aritmetickou klasifikaci pro množiny

    (a) $\{\, x \,;\, \mathrm{W}_x$ je konečná $\,\}$,

    (b) $\{\, x \,;\, \overline{\mathrm{W}_x}$ je konečná $\,\}$,

    (c) $\{\, x \,;\, \overline{\mathrm{W}_x}$ je kompletní $\,\}$.

27. Dokažte, že množina Unb je Π_2-kompletní.

2.3 Pár slov o výpočtové složitosti

Vezmeme-li do ruky libovolnou učebnici logiky (včetně této) a budeme-li listovat v jejích úvodních kapitolách, pravděpodobně najdeme část věnovanou výrokovým tautologiím, a tato část bude obsahovat příklady či cvičení na užití tabulkové metody. Prohlédneme-li si tyto příklady a cvičení, asi zjistíme, že všechny formule, které se v nich vyskytují, obsahují nejvýše tři výrokové atomy. Je nám přitom jasné, proč tomu tak je: tabulka pravdivostních ohodnocení pro formuli s n výrokovými atomy má 2^n řádků, což je pro $n \geq 4$ nepříjemně vysoký počet.

V oddílu 2.1 jsme na tabulkové metodě založili programy pro počítač RASP, které rozhodují úlohy SAT a TAUT. Při tom jsme konstatovali, že lze ušetřit paměťový prostor, protože tabulku pravdivostních ohodnocení není nutné držet v paměti počítače celou najednou, prostor nutný k uložení jednoho pravdivostního ohodnocení může být použit opakovaně. Nenalezli jsme ale způsob, jak ušetřit čas nutný k výpočtu. Formule délky n může obsahovat řádově n různých výrokových atomů, a čas, který náš algoritmus potřebuje na její zpracování, nelze omezit lépe než funkcí $n \mapsto 2^n$.

Představme si, že na určitém (skutečném) počítači provozujeme určitý program P a že po nějaké době získáme nový počítač, který je několikanásobně rychlejší. Pracuje-li program P v čase $2^{\mathcal{O}(n)}$, několikanásobné zrychlení výpočtu nepřináší vlastně žádnou výhodu, neboť neznamená nic víc, než že na novém počítači můžeme za stejný časový úsek zpracovat vstup, který je *o několik* znaků delší. Tím chceme znovu připomenout to, co jsme konstatovali za formulací věty 2.1.1 a co bylo již předtím naznačeno v komentáři k tabulkové metodě: program pracující v exponenciálním čase se těžko dá považovat za efektivní, a úlohy, které lze rozhodovat pouze programem s tak vysokými časovými nároky, se z praktického hlediska příliš neliší od algoritmicky nerozhodnutelných úloh.

Které z algoritmicky rozhodnutelných úloh tedy můžeme považovat za efektivně rozhodnutelné, tj. za rozhodnutelné i z praktického hlediska?

Definujme $\mathsf{TIME}(f)$ jako množinu všech úloh, které jsou na počítači RASP rozhodnutelné programem, který pracuje v čase $\mathcal{O}(f)$, a definujme dále $\mathsf{FTIME}(f)$ jako množinu všech funkcí, které jsou na počítači RASP počitatelné programem, který rovněž pracuje v čase $\mathcal{O}(f)$. Množinám jako $\mathsf{TIME}(f)$ a $\mathsf{FTIME}(f)$ se ve výpočtové složitosti říká *třída (rozhodovacích) úloh* resp. *třída funkcí*. Mohli bychom efektivně počitatelné funkce ztotožnit s funkcemi z vhodně zvolené třídy $\mathsf{FTIME}(f)$, například s funkcemi z třídy $\mathsf{FTIME}(n)$? Proti této volbě mluví několik argumentů. Jeden z nich je ten, že třída $\mathsf{FTIME}(n)$ je neabsolutní v tom smyslu, že je závislá na volbě výpočtového modelu a na detailech definice časových nároků. Například funkce NÁSOBENÍ je sice na počítači RASP a při naší definici časových nároků počitatelná v čase $\mathcal{O}(n)$, je ale otevřeným problémem, zda je v čase $\mathcal{O}(n)$ počitatelná i na Turingově stroji.

Běžný přístup je přijmout za efektivní každý program pracující v čase $\mathcal{O}(n^k)$ pro některé k. Je zřejmé, že pracuje-li program P v čase $\mathcal{O}(n^k)$, pak existují konstanty $c_1, c_2 \in \mathrm{N}$ takové, že program P pracuje v čase $c_1 n^k + c_2$. Na druhé straně, pracuje-li program P v čase $\sum_{i=0}^{k} c_i n^{k-i}$, tj. jsou-li jeho časové nároky omezeny polynomem v n, pak P pracuje v čase $\mathcal{O}(n^k)$. Z tohoto důvodu se o programech, které pracují v čase $\mathcal{O}(n^k)$ pro některé $k \in \mathrm{N}$, říká, že pracují v *polynomiálním čase*. Za funkce či rozhodovací úlohy, které jsou počitatelné či rozhodnutelné z praktického hlediska, prohlašme funkce resp. úlohy, které jsou počitatelné (rozhodnutelné) programem, který pracuje v polynomiálním čase:

$$\mathsf{FP} = \bigcup_{c \in \mathrm{N}} \mathsf{FTIME}(n^c), \qquad \mathsf{P} = \bigcup_{c \in \mathrm{N}} \mathsf{TIME}(n^c).$$

Třída FP je třída všech funkcí *počitatelných v polynomiálním čase* (*polynomiálně počitatelných funkcí*) a třída P je třída všech úloh *rozhodnutelných v polynomiálním čase* (*polynomiálně rozhodnutelných úloh*). K definici tříd FP a P poznamenejme, že se situací, kdy „ta pravá“ třída je definována jako nekonečné sjednocení, jsme se vlastně už setkali. Když jsme v oddílu 2.1 o nějaké úloze řekli, že je rozhodnutelná v čase $2^{\mathcal{O}(n)}$, znamenalo to, že je prvkem sjednocení $\bigcup_{c\in\mathbb{N}} \mathsf{TIME}(2^{cn})$.

Třída P je pokládána za nejpřirozenějšího kandidáta při hledání definice, která by vystihla intuitivní pojem efektivně rozhodnutelné úlohy. Třída P není závislá na tom, který z běžných výpočtových modelů si vybereme. P. Odifreddi v [61] dokonce tvrdí, že platí kvantitativní verze Churchovy teze: pojem polynomiálně rozhodnutelné úlohy je absolutním pojmem, nelze navrhnout rozumný výpočtový model tak, aby třída všech polynomiálně rozhodnutelných úloh pomocí něj definovaná se lišila od třídy všech polynomiálně rozhodnutelných úloh definované pomocí kteréhokoliv z užívaných výpočtových modelů (či pomocí počítače RASP). Z tohoto důvodu můžeme mluvit nejen o programech pro počítač RASP pracujících v polynomiálním čase, ale i o *algoritmech* pracujících v polynomiálním čase čili o *polynomiálních algoritmech*. Také ostatní třídy, o kterých se zmíníme v tomto oddílu, jsou nezávislé na volbě výpočtového modelu.

Dosud víme, že například úloha Pravdivostní hodnota výrokové formule je v třídě P. O úlohách Sat, Taut a QBF není známo, jsou-li v P. O úlohách, jako je Problém zastavení, je jasné, že v P nejsou.

Kromě tříd, jako je P nebo $\mathsf{TIME}(n)$, kterým se říká *časové třídy*, vezměme v úvahu také *prostorové třídy*. Definujme $\mathsf{FSPACE}(f)$ a $\mathsf{SPACE}(f)$ jako množinu všech funkcí či rozhodovacích úloh, které jsou (na počítači RASP) počitatelné resp. rozhodnutelné programem, který pracuje v prostoru $\mathcal{O}(f)$. Dále položme

$$\mathsf{FLOG} = \mathsf{FSPACE}(\ell), \qquad \mathsf{LOG} = \mathsf{SPACE}(\ell), \qquad \mathsf{PSPACE} = \bigcup_{c\in\mathbb{N}} \mathsf{SPACE}(n^c).$$

Třída FLOG či LOG je třída všech funkcí počitatelných (resp. úloh rozhodnutelných) v *logaritmickém prostoru*. Tato terminologie je oprávněna faktem, že ℓ a také každá funkce tvaru $n \mapsto \lceil \log_{c_1}(n) \rceil$, kde $c_1 > 1$, je v $\mathcal{O}(f)$ pro libovolnou funkci f tvaru $n \mapsto \lceil \log_{c_2}(n) \rceil$, kde opět $c_2 > 1$. Můžeme tedy mluvit o logaritmu, aniž bychom specifikovali jeho bázi. Třída PSPACE je třída všech úloh rozhodnutelných v *polynomiálním prostoru*.

V oddílu 2.1 jsme zjistili, že úlohy Sat, Taut a QBF jsou v PSPACE. Úloha rozhodnout, zda dané slovo je booleovským výrazem, je příkladem úlohy ve třídě LOG. Také úloha rozhodnout, zda dané slovo je (syntakticky správnou) výrokovou formulí, je úlohou ve třídě LOG, neboť program z oddílu 2.1, který rozhoduje o syntaktické správnosti booleovských výrazů a pracuje v logaritmickém prostoru, by se dal upravit na program, který by místo toho rozhodoval o výrokových formulích. Lze dokázat (cvičení), že úlohy Hodnota booleovského výrazu a Pravdivostní hodnota výrokové formule jsou také ve třídě LOG. Součet a součin přirozených čísel jsou příklady funkcí ve třídě FLOG.

Rozšiřme nyní naši zásobu zajímavých úloh. Připomeňme, že literál je výrokový atom nebo negovaný výrokový atom a že klauzule je disjunkce literálů. Definujme, že literál je *negativní* nebo *pozitivní* podle toho, je-li negovaným atomem nebo atomem bez negace. *Hornovská klauzule* je klauzule obsahující nejvýše jeden pozitivní literál. *Hornovská formule* je výroková formule, která je konjunkcí hornovských klauzulí. Hornovská formule je tedy zvláštním případem formule v konjunktivním normálním tvaru. Nyní jsme připraveni definovat několik úloh vztahujících se k výrokové logice.

HornSat

Dáno: Hornovská výroková formule A.

Úkol: Zjistit, zda A je splnitelná.

2Sat

Dáno: Výroková formule A v konjunktivním normálním tvaru, v níž každá klauzule obsahuje nejvýše dva literály.

Úkol: Zjistit, zda A je splnitelná.

3Sat

Dáno: Výroková formule A v konjunktivním normálním tvaru, v níž každá klauzule obsahuje nejvýše tři literály.

Úkol: Zjistit, zda A je splnitelná.

Analogicky bychom mohli definovat také úlohy 4Sat, 5Sat atd. Nebudeme je ale potřebovat. Kromě uvedených tří úloh se zmíníme také o úlohách CNFSat a DNFSat (zjistit, zda daná formule v konjunktivním resp. disjunktivním normálním tvaru je splnitelná).

Je zřejmé, že pomocí tabulkové metody lze rozhodovat kteroukoliv z právě uvedených tří úloh. Nyní ale zdůvodníme, že pro úlohu HornSat lze navrhnout mnohem účinnější algoritmus, než je tabulková metoda. Výsledkem bude tvrzení, že úloha HornSat je v P. Úvahy, zda něco podobného platí i pro zbývající dvě úlohy či pro úlohu Sat, odložme na později.

Uvědomme si, že je-li C hornovská klauzule tvaru $\neg q_1 \vee \ldots \vee \neg q_k \vee p$, tj. obsahuje-li klauzule C nějaký pozitivní literál, pak C je výrokově ekvivalentní s formulí $q_1 \& \ldots \& q_k \rightarrow p$. Domluvme se proto, že hornovským klauzulím obsahujícím pozitivní literál budeme chvíli říkat „implikace“, kdežto ostatním (sestávajícím pouze z negativních literálů) budeme říkat „disjunkce“. Například hornovská formule

$$\neg p \,\&\, (\neg r \vee \neg s \vee p) \,\&\, (\neg q \vee s) \,\&\, (\neg r \vee q) \,\&\, r$$

je konjunkcí pěti klauzulí, z nichž první je disjunkce, ostatní jsou implikace. Nyní můžeme popsat algoritmus, o kterém pak dokážeme, že je polynomiálním algoritmem pro úlohu HornSat:

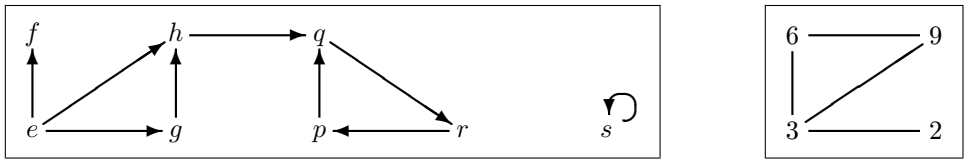
1. Přijmi vstup A a zkontroluj, že A je opravdu hornovskou formulí. Utvoř seznam $r_1, \ldots, r_n$ všech atomů vyskytujících se v A. Vyhraď paměťový

prostor pro pravdivostní ohodnocení v atomů $r_1, \ldots, r_n$. Iniciálně zvol v tak, že všem atomům $r_1, \ldots, r_n$ jsou přiřazeny nuly.

2. Zjisti, zda mezi klauzulemi, ze kterých je sestavena formule A, je nějaká implikace, kterou ohodnocení v nesplňuje. Pokud ne, pokračuj bodem 4.
3. Zvol implikaci $\neg q_1 \vee \ldots \vee \neg q_k \vee p$, kterou ohodnocení v nesplňuje. Polož $v(p) = 1$ a pokračuj bodem 2.
4. Když v splňuje všechny disjunkce, řekni ANO. Jinak řekni NE.

Ohodnocení v zpočátku obsahuje pouze nuly. Některé nuly mohou být v průběhu výpočtu změněny na jedničky; opačná změna ale možná není. Tento algoritmus nejprve pomíjí všechny disjunkce a zabývá se pouze implikacemi. Každá implikace může být příčinou, že některá nula ohodnocení v je změněna na jedničku. Tuto „potíž“ ale každá implikace C tvaru $\neg q_1 \vee \ldots \vee \neg q_k \vee p$ může způsobit nejvýše jednou: poté, co jsme položili $v(p) = 1$, další přidání jedniček už nic nezmění na tom, že $v(C) = 1$. Bod 3 je tedy prováděn nejvýše tolikrát, kolik je ve formuli A implikací. Tím je zdůvodněno, že algoritmus při zpracování libovolného vstupu A dospěje k bodu 4, vydá nějakou odpověď a zastaví se. Zbývá zdůvodnit, že všechny jeho odpovědi jsou správné. Důkaz se opírá o následující pomocné tvrzení. *Nechť v' je libovolné pravdivostní ohodnocení, pro které platí $v'(A) = 1$. Vždy, když je prováděn bod 2, pro každý z atomů $r_1, \ldots, r_n$ splňující podmínku $v(r_i) = 1$ platí i $v'(r_i) = 1$.* Jinými slovy, každá hodnota 1 ohodnocení v je nutná v tom smyslu, že hodnotu 1 má v tomtéž bodě každé ohodnocení, které splňuje formuli A. Toto tvrzení lze snadno dokázat indukcí podle počtu průchodů bodem 3. Když algoritmus dospěje k bodu 4, má v ruce ohodnocení v, které splňuje všechny implikace. Zjistí-li nyní, že v splňuje všechny disjunkce, a řekne-li následkem toho ANO, je to správná odpověď, ohodnocení v splňuje všechny klauzule formule A (implikace i disjunkce), a A je tedy splnitelnou formulí. Když naopak A je splnitelná, existuje ohodnocení v' takové, že $v'(A) = 1$. Ohodnocení v' splňuje všechny disjunkce a pomocné tvrzení říká, že v vznikne z v' změnou některých jedniček na nuly. Taková změna nemůže nic pokazit na tom, že všechny disjunkce mají hodnotu 1. Algoritmus tedy při provedení bodu 4 řekne ANO.

Zbývá uvážit, jak by vypadal přepis P našeho algoritmu do jazyka RASP a jaké by byly jeho časové nároky. Řekněme, že program P požaduje, aby vstupní formule A byla na vstupní pásku zapsána běžným způsobem, ale bez zbytečných závorek určujících pořadí operací stejného druhu (několika konjunkcí nebo několika disjunkcí). Dále řekněme, že formuli A a ohodnocení v budou v paměti počítače reprezentovat dva na sebe navazující záznamy, tj. datová struktura, kterou jsme na str. 74 označili dvěma hvězdičkami. Má-li program P zjistit, zda některá implikace formule A je ohodnocením v nesplněna, znamená to kvůli každému literálu projít ohodnocení v a vyhledat příslušnou pravdivostní hodnotu. Nechť formule A má délku n. Protože literálů je řádově nejvýše n a délka pravdivostního ohodnocení je také řádově n, na provedení bodu 3 program P potřebuje čas $\mathcal{O}(n^2)$. Protože bod 3 se provádí ne více než n-krát, program pracuje v čase $\mathcal{O}(n^3)$.



Obrázek 2.3.1: Příklad orientovaného a neorientovaného grafu

Ačkoliv tvrdíme, že algoritmicky zajímavé úlohy se často objevují v logice, je pravda, že se často objevují také v teorii grafů. *Orientovaný graf* je dvojice $\langle G, R\rangle$, kde G je neprázdná množina a R je binární relace na G. Prvkům množiny G říkáme *vrcholy* nebo *uzly* grafu $\langle G, R\rangle$, prvky množiny R jsou *hrany*. Na obrázku 2.3.1 vlevo je znázorněn orientovaný graf s osmi vrcholy, hrany jsou vyznačeny šipkami. Hranám tvaru $[a, a]$ (z nějakého vrcholu do téhož vrcholu) se říká *smyčky*. *Neorientovaný graf* nebo jen *graf* jsme v oddílu 1.2 na str. 24 definovali jako dvojici $\langle G, R\rangle$, kde R je antireflexivní a symetrická relace na neprázdné množině G. Příklad neorientovaného grafu je znázorněn na obr. 2.3.1 vpravo. Hrany neorientovaného grafu je užitečné si představovat či znázorňovat jako úsečky (obecně neorientované spojnice), smyčky se v neorientovaném grafu nepřipouštějí. Posloupnost $a_0, \ldots, a_n$ vrcholů (orientovaného nebo neorientovaného) grafu $\langle G, R\rangle$ je *sled* z vrcholu c do vrcholu d, platí-li $\forall i{<}n\,(a_i\ R\ a_{i+1})$, a přitom $a_0 = c$ a $a_n = d$. Číslo $n \geq 0$ je délka sledu $a_0, \ldots, a_n$. Sled $a_0, \ldots, a_n$ je *cesta*, platí-li $a_i \neq a_j$ pro každé dva indexy $i \neq j$. Cesta je tedy takový sled, v němž se neopakují vrcholy. Chceme-li zdůraznit, že jde o sled nebo cestu v orientovaném či neorientovaném grafu, mluvíme o *orientovaném* či *neorientovaném sledu* a o *orientované* či *neorientované cestě*. Vrchol d je v grafu $\langle G, R\rangle$ dosažitelný z vrcholu c, jestliže v grafu $\langle G, R\rangle$ existuje sled z c do d. Protože připouštíme i sledy a cesty délky nula, je každý vrchol c dosažitelný sám ze sebe, a to bez ohledu na to, je-li $[c, c]$ hranou. Snadno lze zdůvodnit, že je-li vrchol d dosažitelný z vrcholu c, pak z c do d vede dokonce cesta. *Cyklus* je orientovaný sled $a_0, \ldots, a_n$ takový, že $a_0, \ldots, a_{n-1}$ je cesta a přitom $n \geq 1$ a $a_0 = a_n$. Orientovaný graf $\langle G, R\rangle$ je *acyklický*, jestliže v něm neexistuje cyklus. Graf $\langle G, R\rangle$ je *orientovaný strom*, jestliže v něm existuje vrchol c (zvaný *kořen*) takový, že do každého vrcholu $d \in G$ vede z vrcholu c právě jedna cesta. Vrcholu orientovaného stromu, ze kterého nevedou hrany, říkáme *list*. Lze zdůvodnit, že každý orientovaný strom je acyklickým grafem. O orientovaných stromech jsme již mluvili v oddílech 1.3 a 1.4 v souvislosti s definicí důkazu.

Řekneme, že podmnožina X množiny G je *nezávislou množinou* neorientovaného grafu $\langle G, R\rangle$, jestliže platí $X^2 \cap R = \emptyset$, tj. jestliže žádné dva prvky množiny X nejsou spojeny hranou.

Dosažitelnost (v orientovaném grafu)

Dáno: Konečný orientovaný graf $\langle G, R\rangle$ a jeho dva vrcholy c a d.

Úkol: Zjistit, zda vrchol d je v grafu $\langle G, R\rangle$ dosažitelný z vrcholu c.

Nezávislá množina

Dáno: Konečný neorientovaný graf $\langle G, R\rangle$ a přirozené číslo k.

Úkol: Zjistit, zda v grafu $\langle G, R\rangle$ existuje nezávislá množina s alespoň k prvky.

Pro účely strojového zpracování se domluvme, že graf na vstupní pásku počítače zapisujeme jako posloupnost vrcholů oddělených čárkami následovanou posloupností hran rovněž oddělených čárkami. Hranu zapisujeme jako dvojici vrcholů oddělených čárkou a uzavřenou mezi hranaté závorky, pro zapisování vrcholů jsme předem zvolili konečnou abecedu neobsahující znaky `[`, `]` a `,` (hranaté závorky a čárku). Zapisujeme-li neorientovaný graf, stačí, zapíšeme-li na seznam hran pouze jednu z hran $[a, b]$ a $[b, a]$, druhá se rozumí automaticky. Například domluvíme-li se, že pro zapisování vrcholů jsme zvolili dvouprvkovou abecedu $\{\mathtt{0}, \mathtt{1}\}$, graf z obr. 2.3.1 vpravo může být reprezentován zápisem

`10,11,110,1001,[11,110],[11,1001],[1001,110],[10,11]`.

Když orientovaný graf $\langle G, R\rangle$ má n vrcholů a vrchol d je dosažitelný z vrcholu c, pak existuje cesta z c do d, jejíž délka je nejvýše $n - 1$. Na tomto pozorování lze založit jednoduchý postup, jak určit, je-li vrchol d dosažitelný z vrcholu c: utvořit postupně seznam všech cest délky nejvýše $n-1$ začínajících v c, a podívat se potom, jestli některá z nich vede do d. Potíž je v tom, že všech cest délky $n - 1$ může být až $n!$ — příliš mnoho pro polynomiální algoritmus. O algoritmu, který trpělivě probírá všechny prvky nějakého konečného (ale velkého) oboru, se říká, že postupuje *hrubou silou*. Rovněž tabulkovou metodu lze označit za rozhodování úlohy Sat (nebo Taut) hrubou silou. A také pro úlohu Nezávislá množina bychom snadno navrhli algoritmus, který ji rozhoduje hrubou silou, probíráním všech podmnožin nosné množiny daného grafu. Naproti tomu v případě úlohy HornSat máme k dispozici i něco lepšího, než je hrubá síla. Nyní uvidíme, že úloha Dosažitelnost je podobného druhu jako HornSat. Ukážeme si dva různé algoritmy, které ji rozhodují, jeden polynomiální, druhý trochu pomalejší, ale paměťově úspornější. První z nich pracuje při zpracování vstupů G, R, c a d se dvěma množinami A a B vrcholů:

1. Polož $A := \{c\}$ a $B := \emptyset$.
2. Platí-li $d \in A$, řekni ANO a skonči. Platí-li $B = A$, řekni NE a skonči.
3. Zvol $a \in A - B$ a urči seznam všech $b_1, \ldots, b_k \in G$ takových, že $[a, b_i] \in R$. Polož $A := A \cup \{b_1, \ldots, b_k\}$, $B := B \cup \{a\}$. Opakuj od bodu 2.

Ponecháváme na čtenáři, aby domyslel, že toto je opravdu polynomiální algoritmus pro úlohu Dosažitelnost.

Hlavní částí našeho druhého algoritmu pro úlohu Dosažitelnost je podprogram T. Tento podprogram je volán s parametry a, b a k, kde a a b jsou vrcholy daného grafu $\langle G, R\rangle$ a k je přirozené číslo. Jeho úkolem je zjistit, zda v grafu $\langle G, R\rangle$ zapsaném na vstupní pásce vede z a do b nějaká cesta, jejíž délka je nejvýše k. K nalezení odpovědi na tuto otázku podprogram T (někdy) volá (rekurzívně) sám

sebe. Připomeňme, že $\lceil x \rceil$ označuje nejmenší celé číslo m takové, že $x \leq m$. Nechť $r_1, .., r_n$ je seznam všech vrcholů grafu $\langle G, R \rangle$. Podprogram T pracuje takto:

> Když $k \leq 1$, vrať odpověď ano, je-li $a = b$ nebo je-li $[a, b]$ hrana. Jinak vrať odpověď ne.
>
> Když $k \geq 2$, pak pro každé $i \in \{1, .., n\}$ volej $T(a, r_i, \lceil k/2 \rceil)$ a $T(r_i, b, \lceil k/2 \rceil)$. Pokud pro některé i jsou obě odpovědi ano, vrať ano, jinak vrať ne.

Hlavní program P, tj. náš paměťově úsporný program pro úlohu Dosažitelnost, pracuje podle očekávání:

> Urči počet n vrcholů daného grafu. Volej $T(c, d, n-1)$. Řekni ANO nebo NE podle toho, dostaneš-li odpověď ano nebo ne.

Korektnost tohoto programu je založena na faktech, že je-li $k \geq 2$, pak $\lceil k/2 \rceil < k$, a dále že z a do b vede cesta délky nejvýše k právě tehdy, když pro některé číslo $i \in \{1, .., n\}$ z a do r_i vede cesta délky nejvýše $\lceil k/2 \rceil$ a současně z r_i do b vede cesta délky rovněž nejvýše $\lceil k/2 \rceil$.

Z oddílu 2.1 víme, že činnost programu P si lze představit jako průchod orientovaným stromem, v němž vrcholy odpovídají jednotlivým voláním podprogramu T a v němž vrcholy umístěné na téže větvi odpovídají kopiím podprogramu T, které mohou být současně aktivní. Dále víme, že čas, který program P potřebuje, lze odhadnout jako součet časů, které potřebují všechny kopie podprogramu T (a hlavní program P), kdežto použitý prostor lze odhadnout jako maximální součet velikostí lokálních dat kopií podprogramu T podél jedné větve stromu. Jdeme-li stromem od kořene k některému listu, třetí parametr podprogramu T má zpočátku hodnotu $k = n - 1$, v každém následujícím vrcholu má hodnotu $\lceil k/2 \rceil$ místo k, v listu má hodnotu 1. Operaci $k \mapsto \lceil k/2 \rceil$ stačí opakovat nejvýše $\ell(n-1)$-krát, abychom se od $n-1$ dostali k jedničce. Maximální délka větve je tedy $\ell(n-1)$, a maximální počet současně rozpracovaných kopií podprogramu T je $\ell(n-1)+1$, čili $\mathcal{O}(\ell(n))$. Lokální data podprogramu T jsou a, b a r_i a číslo k. S číslem k není problém, jeho zápis má délku $\mathcal{O}(\ell(n))$. Poslední zápletka při stanovení paměťových nároků programu P je toto: budeme-li vrchol grafu reprezentovat přirozeným číslem, které udává pozici jeho nejlevějšího znaku na vstupní pásce, dosáhneme toho, že pro zápis kteréhokoliv z vrcholů a, b a r_i, a tedy i pro všechna lokální data podprogramu T, vystačíme s prostorem $\mathcal{O}(\ell(n))$. Tím je zdůvodněno, že program P pracuje v prostoru $\mathcal{O}(\ell^2(n))$, a že tedy úloha Dosažitelnost je v třídě $\mathsf{SPACE}(\ell^2)$. Orientovaný strom, jehož každý vrchol kromě listů má n následníků a jehož větve mohou mít délku $\mathcal{O}(\ell(n))$, může mít až $n^{\ell(n)}$ vrcholů. Protože funkci $n \mapsto n^{\ell(n)}$ nelze omezit polynomem, nemůžeme tvrdit, že program P pracuje v polynomiálním čase.

Lemma 2.3.1 *(a) Když $g \in \mathsf{FP}$ a $h \in \mathsf{FP}$, pak $h \circ g \in \mathsf{FP}$.*
(b) $\mathsf{FLOG} \subseteq \mathsf{FP}$.
(c) Když $g \in \mathsf{FLOG}$ a $h \in \mathsf{FLOG}$, pak $h \circ g \in \mathsf{FLOG}$.

Důkaz Nechť program P_1 počítá funkci g a na každém vstupu délky n se dopočítá za nejvýše $p_1(n)$ kroků. Nechť program P_2 počítá funkci h a na každém vstupu délky n se dopočítá za nejvýše $p_2(n)$ kroků. Utvořme z programů P_1 a P_2 program P, který pracuje tak, že na každém vstupu x nejprve simuluje činnost programu P_1, čímž získá $g(x)$, a pak simuluje činnost programu P_2 na vstupu $g(x)$. Simulace programu P_1 znamená počítat úplně stejně jako program P_1, ale výsledek nezapsat na výstupní pásku, nýbrž uložit jej domluveným způsobem do paměti počítače. Simulace programu P_2 znamená pracovat úplně stejně jako program P_2, ale místo dat zapsaných na vstupní pásku použít data zapsaná domluveným způsobem do paměti počítače. Má-li vstup x délku n, program P_1 jej zpracuje za nejvýše $p_1(n)$ kroků. Na simulaci této činnosti program P vystačí s $\mathcal{O}(p_1(n))$ kroky. Během $p_1(n)$ kroků program P_1 nestačí zapsat na výstupní pásku více než $p_1(n)$ symbolů. Výsledek $g(x)$ jeho činnosti má tedy délku nejvýše $p_1(n)$, programu P_2 na jeho zpracování stačí čas $p_2(p_1(n))$ a programu P na simulaci činnosti programu P_2 stačí $\mathcal{O}(p_2(p_1(n)))$ kroků. Program P tedy pracuje v čase $\mathcal{O}(p_1(n) + p_2(p_1(n)))$, což znamená, že jsou-li p_1 a p_2 polynomy, pracuje v polynomiálním čase.

Nechť P je program, který pracuje v logaritmickém prostoru a počítá funkci f. Připomeňme, že v oddílu 2.1 jsme definovali konfiguraci počítače RASP jako údaj o okamžitém obsahu všech paměťových buněk, o hodnotě všech tří podmínkových bitů, o obsahu čítače instrukcí a o tom, zda svítí některé signální světlo. Dále připomeňme, že konfigurací a obsahem vstupní pásky je jednoznačně určeno, co počítač v daném okamžiku udělá, tj. do jaké konfigurace přejde provedením jednoho kroku. Nechť posloupnost $C_0, \ldots, C_m$ konfigurací je výpočtem programu P ze vstupu, který má délku n. Protože program P pracuje v prostoru $\mathcal{O}(\ell)$, zápis každé konfigurace C_i má délku $\mathcal{O}(\ell(n))$. Takových zápisů, tj. slov v abecedě Σ délky $\mathcal{O}(\ell(n))$, je dohromady $c^{\mathcal{O}(\ell(n))}$, kde c je konstanta. Je zřejmé, že v posloupnosti $C_0, \ldots, C_m$ nemohou být dvě stejné konfigurace: kdyby pro $i < j$ platilo $C_j = C_i$, platilo by i $C_{j+1} = C_{i+1}$, $C_{j+2} = C_{i+2}$ atd., počítač by donekonečna procházel konfigurace $C_i, \ldots, C_{j-1}$, čili zacyklil by se. Počet m kroků, které program P může vykonat, než se zastaví, je tedy omezen počtem $c^{\mathcal{O}(\ell(n))}$ možných konfigurací. Trochu počítání postačuje k ověření, že funkce v $c^{\mathcal{O}(\ell(n))}$ je omezena polynomem v n; platí totiž, že $c^{\ell(n)}$ je řádově totéž co $n^{\ell(c)}$.

Nechť P_1 a P_2 jsou programy, které počítají funkce g a h a pracují v logaritmickém prostoru. Opět zkonstruujeme program P, který na každém vstupu x simuluje činnost programu P_1 na vstupu x a činnost programu P_2 na vstupu $g(x)$. Nechť $q : \mathrm{N} \to \mathrm{N}$ je funkce v $\mathcal{O}(\ell)$ taková, že program P_2 každý vstup délky n zpracuje s použitím prostoru nejvýše $q(n)$. Z předchozího odstavce víme, že má-li libovolný vstup x délku nejvýše n, pak $g(x)$ má délku nejvýše $p(n)$, kde p je jistý polynom. Funkce $q \circ p$ je v $\mathcal{O}(\ell)$. To znamená, že na simulaci činnosti programu P_2 ze vstupu $g(x)$ program P vystačí s prostorem $\mathcal{O}(\ell(n))$. Potíž je ale v tom, že program P nemůže postupovat stejně jako v (a), simulovat činnost programu P_1, výsledek $g(x)$ si uložit do paměti a pak simulovat činnost programu P_2, neboť uložením dat $g(x)$ do paměti by mohlo dojít k překročení povoleného prostoru.

Program P místo toho postupuje následovně. Rovnou začne simulací činnosti programu P_2. V každém okamžiku, kdy by program P_2 četl obsah některého pole vstupní pásky, program P simuluje činnost programu P_1, aby obsah onoho pole zjistil. Program P tedy činnost programu P_1 simuluje opakovaně, nenechá jej přitom nic nikam zapisovat, pokaždé ale sleduje jeho zamýšlené zápisy do jednoho určitého pole. QED

Z tvrzení (b) předchozího lemmatu bezprostředně vyplývá inkluze $\mathit{LOG} \subseteq \mathit{P}$. Lze dokázat, že platí také $\mathit{P} \subseteq \mathit{PSPACE}$. Ve větě 2.3.3 ale budeme tvrdit víc.

Vezměme nyní znovu v úvahu úlohy Sat a QBF jako typické zástupce úloh, u kterých nevíme, zda jsou rozhodnutelné polynomiálním algoritmem, a všimněme si určitého rozdílu mezi nimi. Když výroková formule A obsahuje ne úplně malý počet výrokových atomů, může být velmi obtížné *nalézt* pravdivostní ohodnocení, které ji splňuje. Je-li ale takové ohodnocení nalezeno a uschováno, snadno lze kdykoliv později *ověřit*, že formule A je opravdu splnitelnou výrokovou formulí — pro určování, zda dané ohodnocení splňuje danou výrokovou formuli, máme polynomiální algoritmus. Na druhé straně, není vidět žádný snadný způsob, který by umožnil ověřit, že dané pravdivostní ohodnocení splňuje danou *kvantifikovanou* výrokovou formuli, pokud jsme to už jednou zjistili. Pokud jsme to už jednou zjistili a pak o tom zapochybujeme, asi nezbývá než to pracně zjistit znovu.

Obecněji řečeno, některé množiny (úlohy) A mají tu vlastnost, že platí-li pro nějaké x, že $x \in A$, můžeme si poznamenat krátká data w, která nám umožňují kdykoliv později rychle přesvědčit sama sebe nebo kohokoliv jiného, že opravdu platí $x \in A$. V případě splnitelných výrokových formulí lze krátká data definovat jako pravdivostní ohodnocení splňující danou formuli, v případě všech neorientovaných grafů obsahujících nezávislou množinu velikosti k lze krátká data definovat jako nezávislou množinu velikosti k, v případě množiny všech složených čísel (tj. přirozených čísel, která nejsou prvočísly) lze krátká data definovat jako číslo, které je dělitelem daného přirozeného čísla. U úlohy QBF není vidět, jak definovat krátká data, a není tudíž jasné, zda úloha QBF patří do téže kategorie jako úlohy Sat, Nezávislá množina či množina všech složených přirozených čísel. U úlohy Taut by nás mohlo napadnout, že krátká data lze definovat jako důkaz dané formule ve vhodně zvoleném kalkulu. Tento nápad ale (asi) nefunguje, neboť v kapitole 1 se nám (pro tam uvažované kalkuly) nepodařilo zjistit, že každá tautologie A má krátký důkaz (vzhledem k délce formule A).

Úlohy jako je Sat a Nezávislá množina jsou úlohy s *efektivní verifikovatelností pozitivních instancí*. Rozdíl mezi takovými úlohami na jedné straně a úlohou QBF (případně Taut) na straně druhé lze vyjádřit pomocí nedeterministických programů a výpočtů.

Nedeterministické programy v jazyce RASP lze definovat více způsoby. Rozhodněme se pro tento: u instrukce `jmp` se připouští více argumentů. To znamená, že kromě zápisu `jmp` ⟨*arg*⟩, který se jako jediný připouštěl v oddílu 2.1, jsou v nedeterministických programech přípustné zápisy tvaru

$$\texttt{jmp}\ \langle \mathit{arg\_1} \rangle \texttt{,} \ldots \texttt{,} \langle \mathit{arg\_n} \rangle .$$

Dojde-li na provedení takovéto instrukce, program pokračuje tak, jako kdyby byla provedena některá z instrukcí `jmp` ⟨*arg_1*⟩ až `jmp` ⟨*arg_n*⟩. Říkáme, že program *nedeterministicky volí* jedno z n možných pokračování. Také se říká, že program provádí *nedeterministický krok*. Program v jazyce RASP je *deterministický*, jestliže všechny v něm se vyskytující instrukce `jmp` mají právě jeden argument. Řekneme, že nedeterministický program se *dopočítá* při zpracování vstupu x, jestliže, začne-li pracovat se vstupem x na vstupní pásce, dospěje k rozsvícení některého signálního světla při každé volbě nedeterministických pokračování. Program se tedy *zacyklí* při zpracování vstupu x, dají-li se nedeterministické kroky volit tak, aby činnost programu probíhala donekonečna. Pro daný program může existovat více výpočtů z téhož vstupu x. Stejně jako vždy jindy, uznáváme pouze úspěšné výpočty, tj. takové, na jejichž konci dojde k zastavení počítače a k rozsvícení některého signálního světla.

Řekneme, že nedeterministický program P *rozhoduje úlohu* A, jestliže platí, že (i) program P se dopočítá na každém vstupu x, (ii) platí-li $x \in A$, pak některý výpočet programu P končí odpovědí ANO, a (iii) platí-li $x \notin A$, pak všechny výpočty programu P končí odpovědí NE.

Řekneme, že nedeterministický program P *pracuje v čase* f, jestliže pro každé n platí, že při zpracování libovolného vstupu délky nejvýše n program P provede při každé volbě nedeterministických pokračování nejvýše $f(n)$ kroků, a pak se zastaví. Každý výpočet ze vstupu délky nejvýše n má tedy nejvýše $f(n) + 1$ konfigurací. Program P *pracuje v prostoru* f, jestliže se dopočítá na každém vstupu x a jestliže navíc při každém výpočtu ze vstupu x délky nejvýše n má obsazená paměť velikost nejvýše $f(n)$.

Rozmysleme si, jak může vypadat nedeterministický program pro úlohu Sat a jaké jsou jeho časové nároky. Program začne svou práci tak, že zkontroluje formát dané formule A a uloží ji do volné paměti za koncem programu. Program dále určí seznam $\mathtt{a}_{i_1}, \ldots, \mathtt{a}_{i_r}$ všech výrokových atomů vyskytujících se ve formuli A a za zápis formule A uloží do paměti počítače datovou strukturu tvaru

...	r	i_1	0	i_2	0	...	i_r	0	...

tj. zápis pravdivostního ohodnocení v, které všem výrokovým atomům formule A přiřazuje nuly. Tato část programu je deterministická a je úplně stejná jako v případě deterministického programu pro úlohu Sat z oddílu 2.1. Má-li vstupní formule A délku nejvýše n, na dosavadní činnost stačí čas $\mathcal{O}(n^2)$. Náš program dále projde zápis ohodnocení v, zvolí si nedeterministicky některé nuly a přepíše je na jedničky. To může udělat například tak, jak je naznačeno na obrázku 2.3.2. Fragment programu na obrázku 2.3.2 předpokládá, že ukazatel `X` byl nasměrován na začátek záznamu v, tj. na buňku obsahující počet r atomů. Tato část programu je nedeterministická, je na ni potřeba čas $\mathcal{O}(n)$ a po jejím provedení má program v paměti uloženu formuli A a nějaké pravdivostní ohodnocení v. Program dále pokračuje (deterministicky) stejně jako program pro rozhodování úlohy Pravdivostní hodnota výrokové formule: určí pravdivostní hodnotu formule A při

```
      mov     @(X),-@(SP)              ; Počet atomů
      loop    gt                       ; Dokud zbývají
        add     #2,X                   ; Následující atom
        jmp     YES,NO                 ; Zvol nedeterministicky
YES:    mov     #1,@(X)                ; jedničku
NO:                                    ; nebo nulu
        sub     #1,@(SP)               ; Další atom?
      endloop                          ; Opakuj, když gt
      add     #1,SP                    ; Srovnej zásobník
```

Obrázek 2.3.2: Nedeterministická volba pravdivostního ohodnocení

ohodnocení v a řekne ANO nebo NE podle toho, je-li formule A ohodnocením v splněna nebo nesplněna. Na to mu opět stačí čas $\mathcal{O}(n^2)$. Je zřejmé, že je-li formule A splnitelná, pak je možné zvolit ohodnocení v, které ji splňuje, a existuje tedy výpočet, po jehož provedení program řekne ANO. Není-li A splnitelná, všechny výpočty končí odpovědí NE. Všechny výpočty mají délku $\mathcal{O}(n^2)$. Úloha SAT je tedy rozhodnutelná nedeterministickým programem, který pracuje v čase $\mathcal{O}(n^2)$.

Mezi dvěma algoritmy, které máme k dispozici pro rozhodování úlohy SAT, deterministickým a nedeterministickým, tedy existuje obrovský rozdíl v časových nárocích. Zdůrazněme ale, že pro nedeterministické algoritmy platí totéž, co jsme dříve řekli o rekurzívně spočetných množinách a přijímatelnosti úloh: jde o teoretický prostředek ke klasifikaci úloh. Nedeterministické algoritmy rozhodně nelze považovat za vynález, který v programátorské praxi může zrychlit výpočty.

Dovolíme-li si nedeterministické kroky, lze nejen zkrátit čas nutný k výpočtu, ale i ušetřit paměťový prostor. Zdá se ale, že rozdíl v prostorových nárocích mezi deterministickými a nedeterministickými programy není tak propastný jako v případě časových nároků. Ukažme si, že úlohu DOSAŽITELNOST, o které víme, že je v $\mathit{SPACE}(\ell^2)$, lze nedeterministickým programem rozhodovat v prostoru ℓ:

Přijmi data G, R, c a d. Urči počet n vrcholů grafu $\langle G, R\rangle$. Polož $x := c$.

Opakuj $(n-1)$-krát toto:

- platí-li $x = d$, řekni ANO a skonči.
- nevycházejí-li z x žádné hrany, řekni NE a skonči.
- zvol nedeterministicky y takové, že $[x, y]$ je hrana, a polož $x := y$.

Řekni ANO, když $x = d$, jinak řekni NE.

Tento program nedeterministicky volí sled délky n začínající ve vrcholu c. ANO řekne tehdy, když na konci sledu nebo někdy dříve dospěje k vrcholu d. NE řekne tehdy, když nenarazí na vrchol d nebo když se mu nepodaří zvolit tak dlouhý sled. Je zřejmé, že z vrcholu c vede sled do vrcholu d právě tehdy, když program *může* říci ANO, tj. když existuje jeho výpočet ze vstupů G, R, c a d, který končí odpovědí ANO. Program tedy rozhoduje úlohu DOSAŽITELNOST. Jediná data programu

jsou proměnné x a y pro vrcholy grafu a interní řídící proměnná cyklu. Má-li celý vstup délku n a reprezentujeme-li opět vrchol grafu pozicí jeho nejlevějšího znaku na vstupní pásce, x i y jsou data velikosti $\mathcal{O}(\ell(n))$. Na zápis řídící proměnné cyklu také stačí $\mathcal{O}(\ell(n))$ bitů.

Nechť $\mathsf{NTIME}(f)$ je třída všech úloh, které jsou rozhodnutelné nedeterministickým programem, který pracuje v čase f, a nechť $\mathsf{NSPACE}(f)$ je třída všech úloh, které jsou rozhodnutelné nedeterministickým program, který pracuje v prostoru f. Dále označme

$$\mathsf{NLOG} = \mathsf{NSPACE}(\ell), \quad \mathsf{NP} = \bigcup_{c\in\mathrm{N}} \mathsf{NTIME}(n^c), \quad \mathsf{NPSPACE} = \bigcup_{c\in\mathrm{N}} \mathsf{NSPACE}(n^c).$$

Třídy NLOG, NP a $\mathsf{NPSPACE}$ jsou třídy všech úloh rozhodnutelných v nedeterministickém logaritmickém prostoru, v nedeterministickém polynomiálním čase resp. v nedeterministickém polynomiálním prostoru. Zatím víme, že Sat $\in \mathsf{NTIME}(n^2)$, tedy Sat $\in \mathsf{NP}$. Dále víme, že Dosažitelnost je úloha v NLOG.

Je zřejmé, že inkluze $\mathsf{TIME}(f) \subseteq \mathsf{NTIME}(f)$ a $\mathsf{SPACE}(f) \subseteq \mathsf{NSPACE}(f)$ platí pro každou funkci f. Platí tedy $\mathsf{LOG} \subseteq \mathsf{NLOG}$, $\mathsf{P} \subseteq \mathsf{NP}$ a $\mathsf{PSPACE} \subseteq \mathsf{NPSPACE}$.

Lemma 2.3.2 *Ke každému (deterministickému nebo nedeterministickému) programu P existuje konstanta c taková, že když program P provede k kroků, pak*

- *v každé paměťové buňce je číslo, jehož binární zápis má nejvýše $k + c$ bitů,*
- *nejvýše $k + c$ paměťových buněk má nenulový obsah,*
- *každá paměťová buňka s nenulovým obsahem má adresu menší než 2^{k+c}.*

Důkaz První tvrzení lze snadno dokázat indukcí podle k. Když po provedení k kroků mají zápisy všech čísel v paměti počítače nejvýše i bitů, pak po provedení instrukce `add` nebo `sub` mají nejvýše $i+1$ bitů. Po provedení jakékoliv jiné instrukce mají stále nejvýše i bitů.

Má-li paměťová buňka s adresou a nenulový obsah, mohl do ní tento obsah být uložen například provedením instrukce `mov ..,@(X)`. V tom případě je číslo a obsahem buňky `X` a podle již dokázaného tvrzení platí $a < 2^{k+c}$. Není-li do paměťové buňky s adresou a její nenulový obsah uložen provedením instrukce se vzdáleným operandem, musel tam být uložen provedením instrukce s běžným operandem nebo tam byl uložen již překladačem. V obou případech je číslo a omezeno délkou programu. QED

Věta 2.3.3 *(a)* $\mathsf{NLOG} \subseteq \mathsf{P}$.
(b) $\mathsf{NPSPACE} \subseteq \mathsf{PSPACE}$.
(c) $\mathsf{NP} \subseteq \mathsf{NPSPACE}$.

Důkaz Úvahy ve všech třech případech jsou z velké části společné. Nechť P je nedeterministický program, který rozhoduje určitou úlohu a pracuje v prostoru q. Předpokládejme, že program nic nezapisuje na výstupní pásku a že výstupy ANO

a NE dává najevo rozsvícením zeleného nebo červeného signálního světla. Každá konfigurace, ve které se program P může při zpracování libovolného vstupu délky nejvýše n ocitnout, je slovem v předem pevně zvolené abecedě Σ, které má délku nejvýše $q(n)$. Přitom abecedu Σ jsme v oddílu 2.1 zvolili tak, že má 4 znaky. Nechť x je vstup programu P délky n. Definujme orientovaný graf $\langle G_x, R_x\rangle$. Množina G_x je množina všech slov v abecedě Σ, která mají délku nejvýše $q(n)$. Ze slova C vede hrana do slova D (tj. dvojice $[C, D]$ je v R_x), jestliže C a D jsou konfigurace takové, že je-li program P v konfiguraci C a na vstupní pásce je slovo x, program P může provedením jednoho kroku přejít do konfigurace D. Protože program P je nedeterministický, ke konfiguraci C může existovat více konfigurací D takových, že $[C, D] \in R_x$. V grafu $\langle G_x, R_x\rangle$ je jedna počáteční konfigurace a větší počet koncových konfigurací. Definujme, že koncová konfigurace je pozitivní nebo negativní podle toho, říká-li v ní program ANO či NE, tj. podle toho, je-li v ní rozsvíceno zelené nebo červené signální světlo. Je jasné, že program P při zpracování vstupu x může říci ANO právě tehdy, když v grafu $\langle G_x, R_x\rangle$ vede cesta z počáteční konfigurace do některé pozitivní koncové konfigurace. Pro určování, zda z počáteční konfigurace vede cesta do *dané* pozitivní koncové konfigurace, máme k dispozici dva algoritmy, z nichž jeden pracuje v polynomiálním čase, druhý v prostoru $\mathcal{O}(\ell^2)$. Určování, zda z počáteční konfigurace vede cesta do *některé* pozitivní koncové konfigurace, neznamená žádné (podstatně) větší nároky na čas ani na prostor. Označme h funkci, která graf $\langle G_x, R_x\rangle$ přepracuje na ANO, pokud v grafu $\langle G_x, R_x\rangle$ vede cesta z počáteční konfigurace do některé pozitivní koncové konfigurace, a na NE v ostatních případech. Zatím víme, že funkce h je současně v FP a v $\mathsf{FSPACE}(\ell^2)$. Označme g funkci, která vstup x programu P přepracuje na graf $\langle G_x, R_x\rangle$, a uvažujme o programu P_1, který počítá funkci g.

Program P_1 nejprve stanoví délku n vstupu x, vypočítá číslo $q(n)$ (o počitatelnosti funkce q se ještě zmíníme) a zapíše na výstupní pásku seznam $C_0, \ldots, C_m$ všech slov v abecedě Σ, která mají délku nejvýše $q(n)$. Pak prochází seznam $C_0, \ldots, C_m$, o každém slově C_i zjistí, je-li konfigurací, a pokud ano, zapíše na výstupní pásku seznam všech dvojic $[C_i, D]$ takových, že $[C_i, D] \in R_x$. Platí-li $[C_i, D] \in R_x$, konfigurace D se s konfigurací C_i shoduje v obsahu všech paměťových buněk až na nejvýše tři a vytvoření konfigurace D z konfigurace C_i má blízko k okopírování konfigurace C_i. Také vytvoření seznamu všech dvojic $[C_i, D]$, kde $[C_i, D] \in R_x$, je do značné míry kopírováním obsahu určitých paměťových buněk do jiného místa paměti. To znamená, že na vytvoření grafu $\langle G_x, R_x\rangle$ program P_1 vystačí s několika ukazateli do výstupní pásky. Všech možných konfigurací délky $q(n)$ je méně než $4^{q(n)+1}$, prvků množiny R_x je méně než $4^{2(q(n)+1)}$, čili $2^{\mathcal{O}(q(n))}$, délka zápisu grafu $\langle G_x, R_x\rangle$ je také $2^{\mathcal{O}(q(n))}$. V každém z několika ukazatelů do výstupní pásky se tedy může ocitnout číslo, jehož zápis má nejvýše $\mathcal{O}(q(n))$ bitů. Program P_1 tedy pracuje v prostoru $\mathcal{O}(q)$.

V případě (a) platí $q \in \mathcal{O}(\ell)$, o funkci q lze předpokládat, že je počitatelná v prostoru $\mathcal{O}(q)$, program P_1 tedy pracuje v prostoru $\mathcal{O}(q)$, čili v prostoru $\mathcal{O}(\ell)$, a platí $g \in \mathsf{FLOG}$. Z 2.3.1(b) plyne $g \in \mathsf{FP}$, z 2.3.1(a) plyne $h \circ g \in \mathsf{FP}$.

V případě (b) lze předpokládat, že q je polynom, což je funkce, kterou lze počítat v polynomiálním prostoru. Program P_1 tedy pracuje v polynomiálním prostoru a platí $g \in \bigcup_{c\in\mathrm{N}} \mathsf{FSPACE}(n^c)$. Tentokrát nemůžeme bezprostředně využít žádné z našich předchozích tvrzení. Důkaz lemmatu 2.3.1(c) lze ale modifikovat na důkaz tohoto tvrzení: když $h \in \mathsf{FSPACE}(\ell^2)$ a $g \in \bigcup_{c\in\mathrm{N}} \mathsf{FSPACE}(n^c)$, pak $h \circ g \in \bigcup_{c\in\mathrm{N}} \mathsf{FSPACE}(n^c)$. Důkaz tohoto tvrzení a podrobnosti vynechané v předchozích úvahách ponecháváme na čtenáři.

V případě (c) máme nedeterministický program P, který pracuje v čase p, kde p je polynom. Při naší definici konfigurace v tomto případě není pravda, že každá konfigurace má délku polynomiální v n. Definujme ale *modifikovanou konfiguraci* jako slovo tvaru

$$d_1 d_2 d_3 d_4 b \texttt{[}a_1\texttt{:}c_1\texttt{]}\,\texttt{[}a_2\texttt{:}c_2\texttt{]}\,..\,\texttt{[}a_k\texttt{:}c_k\texttt{]}, \qquad (*)$$

kde slovo b udává hodnotu čítače instrukcí a každé ze slov c_i udává obsah paměťové buňky, jejíž adresu udává slovo a_i. O ostatních paměťových buňkách (jiných než $a_1, .., a_k$) se rozumí, že obsahují nuly. Modifikovaná konfigurace je tedy slovem v abecedě $\{\texttt{-}, \texttt{0}, \texttt{1}, \texttt{[}, \texttt{]}, \texttt{:}\}$. Je-li C modifikovaná konfigurace tvaru $(*)$, pak lemma 2.3.2 říká, že délka zápisu každého z čísel a_i a c_i i jejich počet k je omezen funkcí v $\mathcal{O}(p(n))$. Celková délka slova C je omezena funkcí q, kde $q \in \mathcal{O}(p^2(n))$, neboli je omezena polynomem. Graf $\langle G_x, R_x\rangle$ nyní obsahuje modifikované konfigurace. Další úvahy jsou úplně stejné jako v případě (b). QED

Tvrzení (b) předchozí věty je zvláštním případem obecnějšího tvrzení známého jako Savitchova věta: když funkce q splňuje jisté nepříliš omezující předpoklady, pak $\mathsf{NSPACE}(q) \subseteq \mathsf{SPACE}(q^2)$.

Z věty 2.3.3 plyne, že platí $\mathsf{PSPACE} = \mathsf{NPSPACE}$ a navíc že pro dosud uvažované třídy úloh platí inkluze

$$\mathsf{LOG} \subseteq \mathsf{NLOG} \subseteq \mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSPACE}.$$

O žádné z těchto čtyř inkluzí se dosud nepodařilo zjistit, zda je ostrá, ačkoliv odborníci odhadují, že ostré jsou všechny čtyři. C. Papadimitriou píše v [62], že tato situace je zdrojem značné frustrace. Je přitom známo, že $\mathsf{NLOG} \neq \mathsf{PSPACE}$, takže můžeme s jistotou říci, že ze čtyř inkluzí je ostrá alespoň některá. Otázka, zda platí $\mathsf{P} = \mathsf{NP}$, je dnes považována za jeden z nejdůležitějších otevřených problémů teoretické informatiky (a logiky, a matematiky vůbec).

Řekneme, že úloha A je na úlohu B *převeditelná logaritmickým převodem*, a píšeme $A \leq_{\mathrm{m}}^{\log} B$, existuje-li funkce $g \in \mathsf{FLOG}$ taková, že $\forall x(x \in A \Leftrightarrow g(x) \in B)$. Relace $\leq_{\mathrm{m}}^{\log}$ je reflexivní, a z lemmatu 2.3.1(c) plyne, že je i tranzitivní. Uvidíme, že relace $\leq_{\mathrm{m}}^{\log}$ má i další společné vlastnosti s relací $\leq_{\mathrm{m}}$ z oddílu 2.2. Nebude-li hrozit nedorozumění, budeme místo o převeditelnosti logaritmickým převodem mluvit prostě jen o převeditelnosti. Ukažme si několik typických příkladů na převeditelnost logaritmickým převodem.

Příklad 2.3.4 Jsou-li všechny výrokové atomy výrokové formule A mezi $p_1, \ldots, p_n$, pak A je splnitelná, právě když kvantifikovaná výroková formule $\exists p_1 \,..\, \exists p_n A$ je

splněna kterýmkoliv pravdivostním ohodnocením. Na ověření, zda A je výrokovou formulí, a na sestavení seznamu všech atomů, které se v ní se vyskytují, stačí logaritmický prostor. To znamená, že definujeme-li $g(A)$ jako $\exists p_1 \,..\, \exists p_n A$ a dodefinujeme-li funkci g vhodně i na argumentech, které nejsou výrokovými formulemi, máme logaritmický převod úlohy SAT na úlohu QBF. Z analogických důvodů platí i TAUT $\leq_{\mathrm{m}}^{\log}$ QBF, místo existenčních se použijí univerzální výrokové kvantifikátory.

Příklad 2.3.5 Když A je kvantifikovaná výroková formule a e je pravdivostní ohodnocení, pak $e \models A \Leftrightarrow e \not\models \neg A$, tedy

$$[A, e] \in \mathrm{QBF} \Leftrightarrow [\neg A, e] \notin \mathrm{QBF}.$$

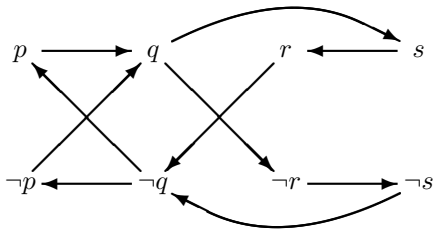
Ověření, zda A je kvantifikovaná formule a e je pravdivostní ohodnocení, a pak připsání negace je proveditelné v logaritmickém prostoru. Platí tedy QBF $\leq_{\mathrm{m}}^{\log} \overline{\mathrm{QBF}}$, úloha QBF je převeditelná na vlastní komplement. Z analogických důvodů platí SAT $\leq_{\mathrm{m}}^{\log} \overline{\mathrm{TAUT}}$ a TAUT $\leq_{\mathrm{m}}^{\log} \overline{\mathrm{SAT}}$. O žádné z úloh SAT a TAUT ale není známo, je-li převeditelná na vlastní komplement.

Příklad 2.3.6 Ukážeme, že platí SAT $\leq_{\mathrm{m}}^{\log}$ 3SAT. Nechť A je daná výroková formule. Přiřaďme každé neatomické podformuli B formule A výrokový atom q_B tak, aby takto přiřazené atomy byly navzájem různé a různé od všech atomů formule A. To lze udělat třeba tak, že stanovíme maximální m takové, že atom p_m se vyskytuje v A, a atom q_B pak definujeme jako p_{m+1+i}, kde i je pozice nejlevějšího znaku nejlevějšího výskytu podformule B na vstupní pásce. Dále pro atomickou podformuli B formule A definujme atom q_B jako B. Tím je atom q_B přiřazen každé podformuli B formule A, atomické i neatomické. Podle toho, je-li neatomická podformule B tvaru $C \& D$, $C \vee D$, $C \to D$ nebo $\neg C$, jí přiřaďme dvě nebo tři klauzule podle této tabulky:

$C \,\&\, D$	$\neg q_C \vee \neg q_D \vee q_B$	$\neg q_B \vee q_C$	$\neg q_B \vee q_D$
$C \vee D$	$\neg q_C \vee q_B$	$\neg q_D \vee q_B$	$\neg q_B \vee q_C \vee q_D$
$C \to D$	$q_C \vee q_B$	$\neg q_D \vee q_B$	$\neg q_B \vee \neg q_C \vee q_D$
$\neg C$	$q_C \vee q_B$	$\neg q_B \vee \neg q_C$.	

Význam klauzulí se trochu ozřejmí, přepíšeme-li si je bez negací, pomocí implikací (například v prvním řádku vlastně jsou implikace $q_C \& q_D \to q_B$, $q_B \to q_C$ a $q_B \to q_D$). Označme $A^\sharp$ konjunkci všech klauzulí takto přidělených neatomickým podformulím formule A. Tvrdíme, že *je-li v pravdivostní ohodnocení takové, že $v(A^\sharp) = 1$, a je-li B podformule formule A, pak $v(B) = v(q_B)$*. Toto pomocné tvrzení lze snadno dokázat indukcí dle složitosti formule B. Dále tvrdíme, že *jsou-li v a v' pravdivostní ohodnocení taková, že pro každou podformuli B formule A platí $v'(q_B) = v(B)$, pak $v'(A^\sharp) = 1$*. I toto pomocné tvrzení lze snadno dokázat; indukcí podle složitosti formule B lze ověřit, že v' splňuje všechny klauzule přiřazené formuli B. Když pro nějaké pravdivostní ohodnocení v platí $v(q_A \,\&\, A^\sharp) = 1$, pak z prvního pomocného tvrzení plyne, že platí i $v(A) = 1$. Když naopak $v(A) = 1$, můžeme

ohodnocení v změnit na ohodnocení v' splňující $v'(q_B) = v(B)$ pro každou podformuli B; díky druhému pomocnému tvrzení pak platí $v'(q_A \,\&\, A^\sharp) = 1$. Formule A je tedy splnitelná právě tehdy, když je formule $q_A \,\&\, A^\sharp$ splnitelná. Formule $q_A \,\&\, A^\sharp$ je v konjunktivním normálním tvaru a lze si rozmyslet, že může být z formule A získána algoritmem pracujícím v logaritmickém prostoru. Funkce $A \mapsto q_A \,\&\, A^\sharp$ je tedy logaritmickým převodem úlohy SAT na úlohu 3SAT.

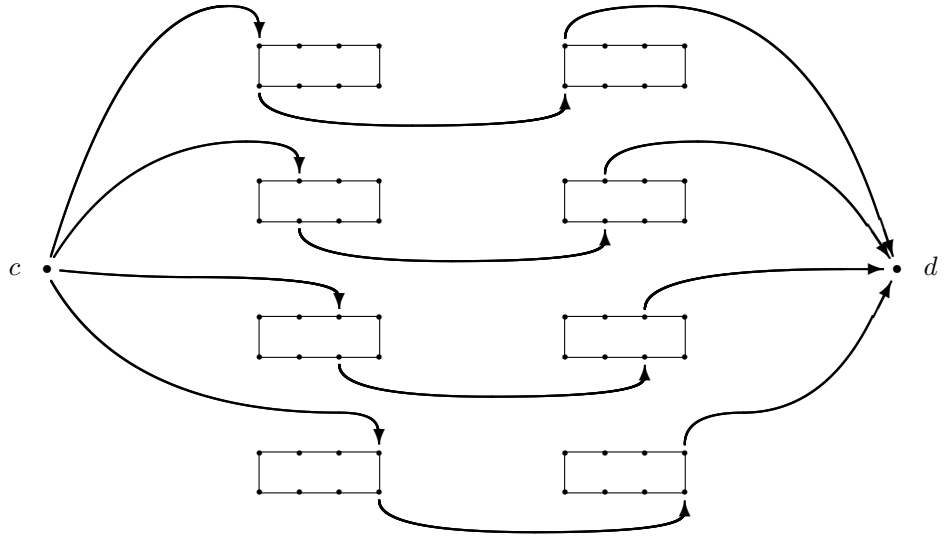


Obrázek 2.3.3: Převod úlohy 2SAT ...

Příklad 2.3.7 Rozmyslíme si, že platí $2\text{SAT} \leq_{\text{m}}^{\log} \overline{\text{DOSAŽITELNOST}}$. Máme sestrojit funkci g počitatelnou v logaritmickém prostoru, která pro každý vstup A splňuje podmínku, že A je výroková formule v konjunktivním normálním tvaru s klauzulemi nejvýše dvouprvkovými, právě když $g(A)$ *není* tvaru $\langle G, R, c, d\rangle$, kde $\langle G, R\rangle$ je orientovaný graf, v němž z c vede cesta do d. Nechť tedy A je daný vstup funkce g. Z obvyklých důvodů můžeme předpokládat, že A je formule v konjunktivním normálním tvaru s klauzulemi nejvýše dvouprvkovými (splnitelná nebo nesplnitelná). Nejprve z formule A sestrojíme pomocný graf $\langle H, Q\rangle$. Potom, vhodným pospojováním několika kopií grafu $\langle H, Q\rangle$ a dvou dodatečných vrcholů c a d, sestrojíme graf $\langle G, R\rangle$, v němž z c vede cesta do d právě tehdy, když formule A není splnitelná. Nechť $p_1, \ldots, p_n$ je seznam všech atomů formule A. V grafu $\langle H, Q\rangle$ bude $2n$ vrcholů, jeden pro každý z literálů $p_1, \ldots, p_n$ a $\neg p_1, \ldots, \neg p_n$. Je-li a literál, nechť $\overline{a}$ označuje literál opačný k a (tj. ten, který vznikne z a odstraněním negace, pokud a je negovaný atom, a přidáním negace, pokud není). Relace Q obsahuje dva prvky pro každou klauzuli $a \vee b$ formule A, totiž $[\overline{a}, b]$ a $[\overline{b}, a]$. Přitom jednočlenná klauzule a se považuje za disjunkci $a \vee a$ a je jí přidělena hrana $[\overline{a}, a]$. Graf $\langle H, Q\rangle$ příslušný například k formuli

$$(\neg p \vee q) \,\&\, (\neg q \vee \neg r) \,\&\, (r \vee \neg s) \,\&\, (s \vee \neg q) \,\&\, (q \vee p)$$

je na obrázku 2.3.3. Všimněme si, že v grafu $\langle H, Q\rangle$ vede cesta z a do b, právě když v něm vede cesta z $\overline{b}$ do $\overline{a}$. Tvrdíme, že *formule A je nesplnitelná, právě když pro některý literál a v grafu $\langle H, Q\rangle$ současně existují cesty z a do $\overline{a}$ i z $\overline{a}$ do a.* Ukažme si stručně, jak se dokáže implikace $\Rightarrow$ tohoto pomocného tvrzení. Nechť neexistuje literál a takový, že současně $\overline{a}$ je dosažitelný z a a a je dosažitelný z $\overline{a}$. Proberme postupně všechny literály formule A (v nějakém zvoleném pořadí). Nechť a je literál, kterému dosud nebyla přiřazena pravdivostní hodnota.



Obrázek 2.3.4: ... na komplement úlohy Dosažitelnost

Je-li a v grafu $\langle H, Q\rangle$ dosažitelný z $\overline{a}$, volme $v(a) = 1$ a $v(\overline{a}) = 0$. Je-li naopak $\overline{a}$ dosažitelný z a, volme $v(a) = 0$ a $v(\overline{a}) = 1$. Neplatí-li ani jedno, přiřaďme literálu a libovolnou pravdivostní hodnotu a literálu $\overline{a}$ ovšem přiřaďme opačnou pravdivostní hodnotu. Dále pro každý literál b, který je v grafu $\langle H, Q\rangle$ dosažitelný z toho literálu z dvojice a a $\overline{a}$, jemuž jsme přiřadili jedničku, položme $v(b) = 1$ a $v(\overline{b}) = 0$. To automaticky znamená, že pro každý literál b, z něhož je dosažitelný ten z dvojice a a $\overline{a}$, kterému jsme přiřadili nulu, platí $v(b) = 0$ a $v(\overline{b}) = 1$. Ponecháváme na čtenáři, aby domyslel, že tímto postupem je korektně definováno pravdivostní ohodnocení a že je to pravdivostní ohodnocení, které splňuje formuli A. Důkaz implikace $\Leftarrow$ pomocného tvrzení také ponecháváme na čtenáři.

Vezměme nyní $2n$ kopií grafu $\langle H, Q\rangle$ a uspořádejme je do n řádků a dvou sloupců tak, jak je naznačeno na obrázku 2.3.4, a přidejme dále dva dodatečné vrcholy c a d. Z vrcholu c vede n hran, přičemž i-tá vede do i-tého řádku, a sice do literálu p_i v levé kopii grafu $\langle H, Q\rangle$. V i-tém řádku je dále hrana směřující z literálu $\neg p_i$ v levé kopii grafu $\langle H, Q\rangle$ do téhož literálu $\neg p_i$ v pravé kopii a pak je tam hrana směřující z literálu p_i v pravé kopii do vrcholu d. Tím je definován graf $\langle G, R\rangle$. Je zřejmé, že vrchol d je v grafu $\langle G, R\rangle$ dosažitelný z vrcholu c právě tehdy, když pro některé i je v grafu $\langle H, Q\rangle$ současně $\neg p_i$ dosažitelný z p_i a p_i dosažitelný z $\neg p_i$, a to je právě tehdy, když formule A není splnitelná. Funkce $A \mapsto g(A)$ tedy má požadované vlastnosti.

Lemma 2.3.8 *Nechť Γ je libovolná z tříd LOG, NLOG, P, NP nebo PSPACE. Když $A \leq_{\mathrm{m}}^{\log} B$ a $B \in \Gamma$, pak i $A \in \Gamma$.*

Důkaz Pro $\Gamma = \mathsf{LOG}$ a $\Gamma = \mathsf{P}$ toto tvrzení plyne bezprostředně z lemmatu 2.3.1. Zbývající úvahy jsou podobné postupům z důkazů lemmatu 2.3.1 a věty 2.3.3. QED

Ve výpočtové složitosti tedy platí analogie bodů (b) a (c) lemmatu 2.2.31. Snadno lze ověřit, že budeme-li ve zbývajících bodech (d)–(f) psát $\leq_{\mathrm{m}}^{\log}$ místo $\leq_{\mathrm{m}}$ (a LOG místo OR v bodě (e)), také dostaneme pravdivá tvrzení.

Z příkladu 2.3.7 (a z výpočtově-složitostní analogie tvrzení (d) lemmatu 2.2.31) víme, že platí $\overline{\text{2SAT}} \leq_{\mathrm{m}}^{\log}$ DOSAŽITELNOST. Platí tedy $\overline{\text{2SAT}} \in \mathsf{NLOG}$. Podobně z příkladu 2.3.4 plyne TAUT $\in \mathsf{PSPACE}$.

Nechť Γ je třída úloh. Řekneme, že úloha B je Γ-*těžká*, platí-li $A \leq_{\mathrm{m}}^{\log} B$ pro každou úlohu $A \in \Gamma$. Úloha B je Γ-*kompletní*, je-li Γ-těžká a platí-li navíc $B \in \Gamma$.

Pojem kompletní úlohy má podobný smysl jako v teorii rekurzívních funkcí. Dokážeme-li, že nějaká úloha B je Γ-kompletní pro nějakou třídu Γ, je tím řečeno poměrně definitivní slovo o její algoritmické složitosti. Zároveň je tím *podmíněně* dokázáno, že úloha B není prvkem žádné menší třídy (z těch, které uvažujeme). Například když B je P-kompletní, znamená to, že $B \notin \mathsf{NLOG}$, ledaže by platilo $\mathsf{NLOG} = \mathsf{P}$. Dále to znamená, že $B \notin \mathsf{LOG}$, ledaže by platilo dokonce $\mathsf{LOG} = \mathsf{P}$. Následující věta tvrdí, že Γ-kompletní úlohy existují pro každou z tříd Γ, které uvažujeme (kromě třídy LOG, pro kterou to smysl nemá).

Věta 2.3.9 *Každá z úloh* DOSAŽITELNOST, HORNSAT, SAT *a* QBF *je na své úrovni kompletní:* DOSAŽITELNOST *je* NLOG*-kompletní,* HORNSAT *je* P*-kompletní,* SAT *je* NP*-kompletní,* QBF *je* PSPACE*-kompletní.*

Tuto důležitou větu ponecháváme bez důkazu, čtenáře odkazujeme na knihy [62], [77], případně [3] či [52]. Poznamenejme však, že důkazy jsou spíše pracné než obtížné a že důkaz NLOG-kompletnosti úlohy DOSAŽITELNOST je z větší části obsažen v důkazu věty 2.3.3(a).

Z věty 2.3.9 plyne například toto: pokud vůbec existuje nějaká úloha v množině $\mathsf{PSPACE} - \mathsf{NP}$, pak QBF je příklad takové úlohy, pokud vůbec existuje nějaká úloha v $\mathsf{NP} - \mathsf{P}$, pak SAT je příklad takové úlohy apod. Nebo jinak, nemá smysl hledat algoritmus pro úlohu HORNSAT, který vystačí s logaritmickým prostorem, ledaže bychom si vytkli úkol dokázat rovnost $\mathsf{P} = \mathsf{LOG}$, nemá smysl hledat polynomiální algoritmus pro úlohu SAT, ledaže bychom chtěli dokázat rovnost $\mathsf{NP} = \mathsf{P}$. Chceme-li o nějaké dané úloze $B \in \mathsf{NP}$ dokázat, že B je NP-kompletní, stačí dokázat SAT $\leq_{\mathrm{m}}^{\log} B$. Z příkladu 2.3.6 plyne, že také stačí dokázat 3SAT $\leq_{\mathrm{m}}^{\log} B$.

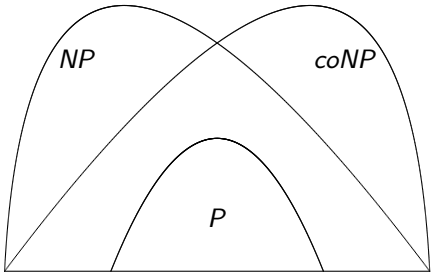
Protože, jak víme z oddílu 2.2, je množina QBF primitivně rekurzívní, z její PSPACE-kompletnosti plyne inkluze $\mathsf{PSPACE} \subseteq \mathsf{PR}$.

Poslední problematika, o které se chceme v tomto oddílu zmínit, je uzavřenost tříd úloh na komplement. Je-li Γ kterákoliv z našich pěti tříd, můžeme uvažovat třídu coΓ všech komplementů úloh z Γ. Je-li ale Γ kterákoliv z tříd LOG, P a PSPACE, nedává to nic nového, neboť deterministické třídy jsou evidentně uzavřeny na komplement. Kupodivu ani coNLOG není nic nového, neboť Immermanova-Szelepcsényiho věta (viz [62] nebo [77]) tvrdí, že i třída NLOG je uzavřena

na komplement, a že tedy platí $coNLOG = NLOG$. Z Immermanovy-Szelepcsényiho věty, z příkladu 2.3.7 a z lemmatu 2.3.8 například plyne, že $2\textsc{Sat} \in NLOG$. Dále lze (s užitím cvičení 15) zdůvodnit, že kromě úlohy Dosažitelnost také úlohy $\overline{\textsc{Dosažitelnost}}$, $2\textsc{Sat}$ a $\overline{2\textsc{Sat}}$ jsou $NLOG$-kompletní.

Ze všech tříd tvaru $co\Gamma$, kde Γ je některá z našich pěti tříd, pouze $coNP$ je (možná) novou třídou, různou od ostatních pěti. Vztah třídy $coNP$ k třídě NP je podobný jako vztah třídy Π_1 k třídě Σ_1: úvahou analogickou jako v první části důkazu lemmatu 2.2.38 lze totiž ověřit, že platí-li mezi třídami NP a $coNP$ některá inkluze, pak platí dokonce rovnost.

Není známo, zda platí $NP = coNP$, ale „oficiální domněnka“ zní, že NP a $coNP$ jsou různé třídy. Z $NP \neq coNP$ ovšem plyne $P \neq NP$. Není také známo, zda ve výpočtové složitosti platí analogie Postovy věty: $NP \cap coNP = P$. Vztahy mezi třídami P, NP a $coNP$ jsou znázorněny na obrázku 2.3.5. Dosavadní (ne)znalosti nás nutí počítat s tím, že jak množina $(NP - coNP) \cup (coNP - NP)$, tak množina $(NP \cap coNP) - P$ může být prázdná, a to nezávisle na sobě. Víme pouze, jak jsme už poznamenali, že $NP - coNP \neq \emptyset$, právě když $coNP - NP \neq \emptyset$.



Obrázek 2.3.5: Vztahy mezi třídami P, NP a $coNP$

Z důvodů stejných jako v teorii rekurzívních funkcí platí, že libovolná úloha je Γ-kompletní, právě když její komplement je $co\Gamma$-kompletní. Tedy $\overline{\textsc{Sat}}$ je $coNP$-kompletní úloha. Uvažme ještě ekvivalence

$$A \in \textsc{Taut} \Leftrightarrow \neg A \notin \textsc{Sat} \quad \text{a} \quad A \notin \textsc{Sat} \Leftrightarrow \neg A \in \textsc{Taut}.$$

První říká $\textsc{Taut} \leq_{\mathrm{m}}^{\log} \overline{\textsc{Sat}}$. Z toho (a z analogie tvrzení 2.3.8 pro třídu $coNP$) plyne $\textsc{Taut} \in coNP$. Druhá říká $\overline{\textsc{Sat}} \leq_{\mathrm{m}}^{\log} \textsc{Taut}$. Úloha Taut je tedy příkladem $coNP$-kompletní úlohy.

Fakt, že Taut je $coNP$-kompletní úloha, poskytuje podmíněnou odpověď na otázku uvedenou na str. 37, která se týká délek důkazů ve výrokových kalkulech.

Věta 2.3.10 *Platí-li $NP \neq coNP$, pak neexistuje výrokový kalkulus C a polynom p tak, že každá tautologie délky nejvýše n má v kalkulu C důkaz délky nejvýše $p(n)$.*

Důkaz Nechť kalkulus C a polynom p jsou takové, že každá tautologie A má v kalkulu C důkaz, jehož délka je nejvýše $p(|A|)$. Pak algoritmus, který každou výrokovou formuli A zpracuje tak, že nejprve nedeterministicky vygeneruje důkaz $\mathcal{P}$ délky

nejvýše $p(|A|)$ a pak ověří, že $\mathcal{P}$ je opravdu důkazem formule A v kalkulu C, je korektním (nedeterministickým) algoritmem, který rozhoduje úlohu TAUT v polynomiálním čase. Platí tedy TAUT $\in$ *NP*. Vzhledem ke *coNP*-kompletnosti úlohy TAUT platí také *coNP* $\subseteq$ *NP*, a tedy *coNP* $=$ *NP*. To je spor s předpokladem *coNP* $\neq$ *NP*. QED

Vidíme tedy, že navrhnout efektivní výrokový kalkulus, ve kterém každá tautologie má důkaz polynomiální délky, znamená dokázat zároveň nepravděpodobný výsledek ve výpočtové složitosti, totiž že *coNP* $=$ *NP*.

Pojem Γ-kompletní úlohy byl nejprve studován pro Γ $=$ *NP*. Průkopnickými pracemi o *NP*-kompletnosti jsou Cookovy a Karpovy články [13] a [46]. Čtenářově pozornosti doporučujeme také knihu [24]. Ta je důležitá tím, že obsahuje seznam několika stovek úloh z různých oblastí matematiky, které jsou *NP*-kompletní. O *P*-kompletních úlohách si lze přečíst v [44].

Cvičení

1. Zdůvodněte, že NÁSOBENÍ lze počítat v logaritmickém prostoru.

   Návod. Obrázek 2.3.6 naznačuje školní algoritmus pro násobení přirozených čísel modifikovaný pro případ, kdy čísla se zapisují binárně. Na tomto algoritmu lze založit program, tabulku umístěnou mezi dvěma vodorovnými čarami ale není nutné uchovávat v paměti počítače celou najednou. Spokojte se s programem, který číslice výsledku zapíše na výstupní pásku v obráceném pořadí, tj. od nejnižšího řádu počínaje. Správného pořadí číslic by se dalo dosáhnout například užitím (modifikací důkazu) lemmatu 2.3.1(c).

2. Zdůvodněte, že úloha DNFSAT je rozhodnutelná algoritmem, který pracuje v polynomiálním čase a logaritmickém prostoru.

3. Každou výrokovou formuli lze převést na ekvivalentní formuli v disjunktivním normálním tvaru, o formuli v disjunktivním normálním tvaru lze díky předchozímu cvičení rychle rozhodnout, je-li splnitelná; to dohromady dává polynomiální algoritmus pro úlohu SAT. Vysvětlete podrobně, proč tato úvaha není správná.

$$
\begin{array}{r}
1\,0\,1\,1\,1\,0 \\
\quad 1\,0\,1\,1 \\
\hline
1\,0\,1\,1\,1\,0 \\
1\,0\,1\,1\,1\,0 \\
0\,0\,0\,0\,0\,0 \\
1\,0\,1\,1\,1\,0 \\
\hline
1\,1\,1\,1\,1\,1\,0\,1\,0
\end{array}
$$

Obrázek 2.3.6: Školní algoritmus pro násobení

4. Zdůvodněte, že jak úloha Hodnota booleovského výrazu, tak úloha Pravdivostní hodnota výrokové formule je rozhodnutelná v logaritmickém prostoru.

   Návod. Navrhněte algoritmus, který postupuje tak, že má-li zjistit pravdivostní hodnotu podformule $B \,\&\, C$, $B \vee C$ či $B \to C$ dané formule A při daném ohodnocení v, zjistí $v(B)$, a hodnotu $v(C)$ zjišťuje pouze tehdy, když je to nutné (např. pokud u formule tvaru $B \,\&\, C$ vyšlo, že $v(B) = 0$, není už nutné zjišťovat $v(C)$, platí totiž $v(B \,\&\, C) = 0$). Algoritmus si nemusí pamatovat dříve určené pravdivostní hodnoty. Když například v nějakém stadiu výpočtu určil $v(C)$ ve formuli $B \,\&\, C$, je jasné, že předtím vyšlo $v(B) = 1$, jinak by nebylo došlo na zjišťování hodnoty $v(C)$.

5. Nechť A je výroková formule v konjunktivním normálním tvaru, nechť p je atom takový, že v žádné klauzuli formule A se nevyskytuje současně p i $\neg p$. Pišme formuli A v tvaru

   $$(B_1 \vee p) \,\&\, \ldots \,\&\, (B_n \vee p) \,\&\, (C_1 \vee \neg p) \,\&\, \ldots \,\&\, (C_m \vee \neg p) \,\&\, D_1 \,\&\, \ldots \,\&\, D_k,$$

   kde klauzule B_i, C_j a D_l neobsahují p. Jinými slovy, rozdělme klauzule formule A na klauzule obsahující p, klauzule obsahující $\neg p$ a klauzule neobsahující p ani $\neg p$. Utvořme z formule A formuli A':

   $$\bigwedge_{i,j} (B_i \vee C_j) \,\&\, \bigwedge_{l} D_l.$$

   Zdůvodněte, že A' je splnitelná, právě když A je splnitelná. Musí být formule A a A' ekvivalentní?

6. Navrhněte na základě předchozího cvičení algoritmus, který rozhoduje úlohu CNFSat. Je váš algoritmus polynomiálním algoritmem?

7. Zdůvodněte, že je-li formule A v cvičení 5 hornovská, pak i A' je hornovská. Dále zdůvodněte, že je-li hornovská formule nesplnitelná, pak obsahuje klauzuli sestávající z jediného pozitivního literálu. Na základě toho navrhněte polynomiální algoritmus pro úlohu HornSat.

8. Zdůvodněte, že na základě cvičení 5 lze navrhnout i polynomiální algoritmus pro úlohu 2Sat.

9. V *rezolučním výrokovém kalkulu* se nepřipouštějí konjunkce, disjunkce ani implikace; jediná operace s formulemi je operace $a \mapsto \overline{a}$, která z negativního literálu odstraní negaci resp. k pozitivnímu literálu připíše negaci. Klauzule se definuje jako množina literálů, formulím v konjunktivním normálním tvaru odpovídají množiny klauzulí, tj. množiny množin literálů. Pravdivostní ohodnocení v splňuje klauzuli, jestliže splňuje některý její prvek; množina klauzulí je splnitelná, jestliže existuje ohodnocení v, které splňuje všechny její prvky.

Prázdná množina klauzulí je splnitelná, prázdná klauzule je jediná klauzule, která není splnitelná. *Pravidlo rezoluce* je pravidlo

$$C \cup \{a\}\ ,\ D \cup \{\overline{a}\}\ \ /\ \ C \cup D,$$

kde C a D jsou klauzule. *Rezoluční odvození* z množiny klauzulí Γ je posloupnost $C_1, \ldots, C_n$ klauzulí taková, že každá C_i je v Γ nebo je z některých klauzulí C_j a C_k, kde $j, k < i$, odvozena pravidlem rezoluce. Zdůvodněte užitím cvičení 5, že neprázdná množina Γ klauzulí je nesplnitelná, právě když existuje rezoluční odvození prázdné klauzule z množiny Γ.

10. Nechť Σ je abeceda a $f : \Sigma^* \to \mathrm{N}$. Definujme SUBGRAF funkce f jako množinu

$$\textsc{Subgraf}(f) = \{\ [w, y]\ ;\ y \leq f(w)\ \}.$$

Dokažte, že $f \in \mathsf{FP}$, právě když platí $\textsc{Subgraf}(f) \in \mathsf{P}$ a současně existuje polynom p takový, že pro každé slovo $w \in \Sigma^*$ platí $|f(w)| \leq p(|w|)$ (kde, jako obvykle, $|w|$ označuje délku slova w).

Návod. Je-li dáno slovo w, lze začít s intervalem $[\![0, p(|w|)]\!]$ a hodnotu $f(w)$ nalézt půlením intervalů.

11. Pokud úloha NEZÁVISLÁ MNOŽINA je v P, pak existuje polynomiální algoritmus, který ke každému grafu $\langle G, R\rangle$ určí maximální velikost množiny, která je v grafu $\langle G, R\rangle$ nezávislá. Dokažte využitím předchozího cvičení.

12. Když $h \in \mathsf{FSPACE}(\ell^2)$ a $g \in \bigcup_{c\in\mathrm{N}} \mathsf{FSPACE}(n^c)$, pak $h \circ g \in \bigcup_{c\in\mathrm{N}} \mathsf{FSPACE}(n^c)$. Dokažte.

13. Dokažte, že funkce $x \mapsto 2^{2^x}$ není v $\bigcup_{c\in\mathrm{N}} \mathsf{FSPACE}(n^c)$. Na základě toho zdůvodněte, že třída $\bigcup_{c\in\mathrm{N}} \mathsf{FSPACE}(n^c)$ není uzavřena na substituci.

Návod. Přizpůsobte úvahu z důkazu lemmatu 2.3.1, která se týkala maximálního počtu různých konfigurací, a tudíž maximálního počtu znaků zapsaných na výstupní pásku.

14. Dokažte podrobně, že úloha NEZÁVISLÁ MNOŽINA je ve třídě NP.

15. Zdůvodněte, že platí $\textsc{Dosažitelnost} \leq^{\log}_{\mathrm{m}} \overline{\textsc{2Sat}}$.

Návod. Nechť je dán orientovaný graf $\langle G, R\rangle$ a jeho dva vrcholy c a d. Přidělme každému vrcholu a atom p_a, přidělme každé hraně $[a, b]$ klauzuli $\overline{a} \vee b$ a ke konstruované formuli ještě přidejme dvě klauzule c a $\overline{d}$.

16. Nalezněte jednoduchý převod úlohy CNFSAT na úlohu 3SAT.

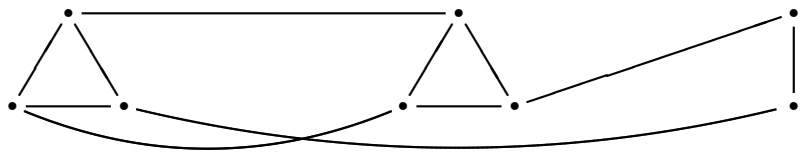
Návod. Když v dané formuli A je klauzule C tvaru $a_1 \vee \ldots \vee a_n$, kde $n > 3$, zvolte nový atom s a klauzuli C nahraďte dvěma klauzulemi $a_1 \vee \ldots \vee a_{n-2} \vee s$ a $a_{n-1} \vee a_n \vee \neg s$.

17. Zdůvodněte, že NEZÁVISLÁ MNOŽINA je *NP*-kompletní úloha.

    Návod. Převádějte úlohu 3SAT. Nechť je dána výroková formule A v konjunktivním normálním tvaru s nejvýše tříprvkovými klauzulemi. Vrcholy konstruovaného neorientovaného grafu $\langle G, R\rangle$ jsou dvojice tvaru $[C, a]$, kde C je klauzule formule A a a je v ní se vyskytující literál. Hrany jsou všechny dvojice tvaru $[[C, a], [C, b]]$ a dále všechny dvojice tvaru $[[C, a], [D, \overline{a}]]$. Například graf příslušný k formuli

    $$(p \vee \neg r \vee s) \,\&\, (\neg p \vee q \vee \neg s) \,\&\, (r \vee \neg q)$$

    je na obrázku 2.3.7. Číslo k (velikost požadované nezávislé množiny) je počet klauzulí formule A.



Obrázek 2.3.7: *NP*-kompletnost úlohy NEZÁVISLÁ MNOŽINA

18. Zdůvodněte, že $\mathsf{NLOG} \subseteq \mathsf{SPACE}(\ell^2)$.

19. Protože úloha HORNSAT je v *P*, je také v $\mathsf{TIME}(n^c)$ pro jisté c. Protože všechny úlohy v *P* jsou na úlohu HORNSAT převeditelné, znamená to, že existuje c takové, že $\mathsf{P} \subseteq \mathsf{TIME}(n^c)$. Proč tato úvaha není správná?

20. Zdůvodněte, že úloha QBF je *PSPACE*-kompletní i za následujících omezujících předpokladů na vstupní formuli $Q_1 p_1 \,..\, Q_n p_n B$:

    - formule B je v konjunktivním normálním tvaru a neobsahuje jiné atomy než $p_1, \ldots, p_n$,
    - n je sudé, $Q_1 = \exists$ a v posloupnosti $Q_1, \ldots, Q_n$ se střídají existenční a univerzální kvantifikátory.

    Návod. V příkladu 2.3.6 jsme k dané výrokové formuli $B(\underline{p})$ sestrojili formuli $E(\underline{p}, \underline{q})$ v konjunktivním normálním tvaru sestavenou z atomů $p_1, \ldots, p_n$ a $q_1, \ldots, q_m$ takovou, že pro každé pravdivostní ohodnocení e platí $e \models B$, právě když $e \models \exists q_1 \,..\, \exists q_m E$. Formuli $Q_1 p_1 \,..\, Q_n p_n A$ lze tedy nahradit formulí $Q_1 p_1 \,..\, Q_n p_n \exists q_1 \,..\, \exists q_m E$. Pak lze přidat jalové kvantifikátory (tj. kvantifikátory $\exists r$ nebo $\forall r$, kde r je atom různý od všech p_i a q_j).

3

Predikátová logika

My opinion is simply that a concept can only be logically fixed through its relation to other concepts. These relations, formulated in precise statements, I call axioms and I add, that the axioms (...) are the definitions of the concepts.
(D. Hilbert, citát uveden v [81])

3.1 Formule a sémantika predikátové logiky

3.1.1 Jazyky, termy a formule

Náš výklad o predikátové logice bude po určitou dobu paralelní s výkladem v kapitole 1 o výrokové logice. I tady budeme nejprve mluvit o tom, co jsou (predikátové) formule, pak o sémantice, která mimo jiné určí, které z formulí jsou logicky platné (tj. pravdivé za každých okolností), a potom stanovíme logický kalkulus tak, abychom pro něj byli schopni dokázat větu o úplnosti, která (mimo jiné) tvrdí, že dokazatelné jsou přesně ty predikátové formule, které jsou logicky platné.

V predikátových formulích (přesněji formulích predikátové logiky prvního řádu) se mohou vyskytovat symboly několikerého druhu:

- *Logické spojky* $\rightarrow$, $\neg$, $\&$, $\vee$.
- *Kvantifikátory*: *univerzální* kvantifikátor $\forall$ a *existenční* kvantifikátor $\exists$.
- *Závorky* ( ).
- *Proměnné* $x, y, u, v, \ldots, x_0, x_1, \ldots$
- *Funkční symboly* pro označení operací s objekty. Každému funkčnímu symbolu F je přiřazeno přirozené číslo $n \geq 0$ zvané *četnost* symbolu F. Například „+“ zpravidla označuje binární funkční symbol, tj. funkční symbol četnosti 2. Funkční symboly četnosti nula se nazývají *konstanty*.
- *Predikátové symboly* (též *relační symboly*) pro označení vztahů mezi objekty. Každému predikátovému symbolu P je přiřazeno přirozené číslo $n \geq 1$ zvané četnost symbolu P. Například „$\in$“ zpravidla označuje binární predikátový symbol, tj. predikátový symbol četnosti 2.

Množinu všech proměnných označme Var a předpokládejme o ní, že je nekonečná spočetná. Logickým spojkám a kvantifikátorům se říká *logické symboly*. Funkční a predikátové symboly se dohromady nazývají *mimologické symboly*. Kdykoliv budeme mluvit o formulích, důkazech nebo axiomatické teorii, budeme předpokládat, že nejprve byla pevně zvolena nebo zadána množina L mimologických symbolů zvaná jazyk (nějaké teorie). *Jazyk* je tedy množina L mimologických symbolů spolu s údajem, který pro každý prvek množiny L určuje, zda je to funkční nebo predikátový symbol a jaká je jeho četnost.

Jeden ze symbolů, totiž rovnítko „=“, si zasluhuje zvláštní zmínku. Nejprve budeme mluvit o predikátové logice bez rovnosti, ve které se rovnítko považuje za mimologický symbol, který se může nebo nemůže vyskytovat ve formulích podle toho, zda byl nebo nebyl přijat do zvoleného jazyka. Později, v predikátové logice s rovností, se rovnítko bude považovat za logický symbol, který se ve formulích může vyskytovat, přestože není jmenován mezi prvky jazyka, a kterému sémantika predikátové logiky s rovností i definice kalkulů pro predikátovou logiku s rovností přisuzují zvláštní význam.

Bude-li se to hodit, budeme užívat i symboly $\top$, $\bot$ a $\equiv$ ve významu z kapitoly 1. Spojce $\equiv$ v tom případě přisuzujeme nižší prioritu než všem ostatním spojkám.

Definice 3.1.1 *Množina všech* termů jazyka L *je nejmenší množina výrazů splňující podmínky*

- *každá proměnná je term (jazyka L),*
- *jsou-li $t_1, \ldots, t_n$ termy a $F \in L$ je funkční symbol četnosti n, pak $F(t_1, \ldots, t_n)$ je term jazyka L.*

Atomická formule jazyka L *je každý výraz tvaru $P(t_1, \ldots, t_n)$, kde $t_1, \ldots, t_n$ jsou termy jazyka L a $P \in L$ je predikátový symbol četnosti n. Množina všech* (predikátových) formulí jazyka L *je nejmenší množina výrazů splňující podmínky*

- *každá atomická formule je formule jazyka L,*
- *jsou-li φ a ψ formule jazyka L a x je proměnná, pak i výrazy $(\varphi \to \psi)$, $(\varphi \& \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$, $\forall x\varphi$ a $\exists x\varphi$ jsou formule jazyka L.*

Místo formule jazyka L se také říká formule *v jazyce* L. V druhé podmínce v definici termu se připouští i případ $n = 0$. To znamená, že každá konstanta $c \in L$ je zároveň termem jazyka L. Formule $\forall x\varphi$ a $\exists x\varphi$ čteme „pro každé x (platí) φ“ resp. „existuje x takové, že (platí) φ“. Často, zejména nepůjde-li nám právě o algoritmy pracující s formulemi a důkazy, připustíme i zápisy, které ne zcela vyhovují definici 3.1.1. Stejně jako ve výrokové logice nebudeme psát úplně vnější dvojici závorek. Naopak, pokud to pomůže čitelnosti, budeme závorkovat i výrazy, u kterých to definice 3.1.1 nepředepisuje, například atomické formule. Binární symboly, a to jak funkční, tak predikátové, se zpravidla píší mezi operandy, například $x + y$ nebo $(x + y)$ místo $+(x, y)$, nebo $x \in y$ místo $\in(x, y)$. U binárních predikátů se často užívá přeškrtnutí místo negace: $t \neq s$ a $t \notin s$ jsou zkrácené zápisy pro $\neg(t = s)$ a $\neg(t \in s)$.

Příklad 3.1.2 *Jazyk teorie množin* $\{\in\}$ obsahuje jediný symbol, který je binárním predikátem. Fakt, že v tomto jazyce nejsou žádné funkční symboly, znamená, že jediné termy v jazyce teorie množin jsou proměnné. Výrazy $x \in x$ nebo $\exists x \forall y(y \in x)$ jsou příklady formulí jazyka teorie množin. Uvažujeme-li teorii množin v predikátové logice s rovností, pak ovšem také $\forall v(v \in x \ \& \ x = y \ \rightarrow \ v \in y)$ je příklad formule jazyka teorie množin.

Příklad 3.1.3 *Jazyk teorie grup* $\{+, 0\}$ má binární funkční symbol $+$ a konstantu 0. Výrazy x, $x + y$ a $(x + 0) + x$ jsou příklady termů v jazyce teorie grup. Jazyk $\{+, 0\}$ má smysl uvažovat pouze v predikátové logice s rovností, protože bez alespoň jednoho predikátového symbolu nelze vytvořit žádnou formuli. V tom případě $\forall x \forall y(x + y = y + x)$ a $\exists y(y + y = x \ \rightarrow \ x = 0)$ jsou příklady formulí v jazyce teorie grup.

Příklad 3.1.4 *Aritmetický jazyk* $\{+, \cdot, 0, \mathrm{S}, \leq, <\}$ má dva binární funkční symboly $+$ a $\cdot$, konstantu 0, unární funkční symbol S a dva binární predikátové symboly $\leq$ a $<$. Výrazy $\mathrm{S}(\mathrm{S}(\mathrm{S}(0)))$ a $x \cdot \mathrm{S}(y + z)$ jsou příklady termů v aritmetickém jazyce (*aritmetických termů*). Výrazy

$$x < \mathrm{S}(0) \ \vee \ \mathrm{S}(0) < x, \qquad \exists y(y + y = 0), \qquad \mathrm{S}(\mathrm{S}(0)) \cdot \mathrm{S}(\mathrm{S}(0)) = \mathrm{S}(\mathrm{S}(\mathrm{S}(0)))$$

jsou příklady formulí v aritmetickém jazyce (*aritmetických formulí*). Aritmetický jazyk budeme zpravidla vztahovat k přirozeným číslům a $\mathrm{S}(x)$ budeme chápat jako označení pro číslo $x + 1$. Symbol „S“ odkazuje k anglickému *successor* (následník).

Vidíme, že volbou jazyka je dáno, o čem se v dané teorii může mluvit. Samotnou definici pojmu teorie však odložme na později.

Uvažujme nyní aritmetickou formuli $\exists y(y + y = x)$, označme ji φ a všimněme si rozdílného postavení proměnných x a y ve φ. Formule φ vyjadřuje vlastnost objektu x (a nikoliv y). Lze ji číst číslo x je dělitelné dvěma. Proměnná y má ve formuli φ pomocný význam, podobně jako ve výrazu $\int_0^x f(y)\,\mathrm{d}y$. Budeme říkat, že proměnná x se ve formuli φ vyskytuje volně, y se ve φ vyskytuje vázaně. Následující definice umožňuje rozdělit výskyty proměnných v libovolné formuli na *volné* a *vázané*.

Definice 3.1.5 *Každý výskyt libovolné proměnné v atomické formuli je volný. Každý volný (vázaný) výskyt proměnné x ve formuli φ a ve formuli ψ je zároveň volným (vázaným) výskytem ve formulích $(\varphi \rightarrow \psi)$, $(\varphi \,\&\, \psi)$ a $(\varphi \vee \psi)$. Každý volný (vázaný) výskyt proměnné x ve formuli φ je zároveň volným (vázaným) výskytem proměnné x ve formuli $\neg\varphi$. Všechny výskyty proměnné x ve formulích $\forall x\varphi$ a $\exists x\varphi$ jsou vázané, žádný z nich není volný. Je-li y proměnná různá od proměnné x, pak každý volný (vázaný) výskyt proměnné y ve formuli φ je zároveň volným (vázaným) výskytem proměnné y ve formulích $\forall x\varphi$ a $\exists x\varphi$.*

Definice 3.1.6 *Term je* uzavřený*, jestliže neobsahuje žádné proměnné. Formule φ je* uzavřená formule *neboli* sentence*, jestliže φ neobsahuje volné výskyty proměnných. Formule φ je* otevřená*, jestliže neobsahuje kvantifikátory.*

Například když φ je formule $\exists x(x < y \ \& \ \forall y(z + \mathrm{S}(y) \neq x))$, pak proměnná z má ve φ jediný výskyt, který je volným výskytem, všechny (tři) výskyty proměnné x ve φ jsou vázané a ze tří výskytů proměnné y je první volný a další dva jsou vázané. Formule φ není sentence, formule $\forall y \forall z \varphi$ je sentence. Ze tří formulí uvedených v příkladu 3.1.4 první je otevřená, druhá je sentence a třetí je dokonce otevřená sentence. Vidíme, že „volný výskyt“ a „vázaný výskyt“ jsou komplementární pojmy, daný výskyt je volný právě tehdy, není-li vázaný. Daná proměnná ale může mít v dané formuli současně volné i vázané výskyty. „Otevřená formule“ a „uzavřená formule“ nejsou komplementární pojmy, některé formule nejsou uzavřené ani otevřené, některé jsou naopak obojí. Pokud nějaký jazyk L neobsahuje žádné konstanty, což je pravda například o jazyce teorie množin, pak v L neexistují žádné uzavřené termy ani otevřené sentence.

Než obrátíme pozornost k definici struktury, zmiňme se ještě o tom, *co přesně* jsou termy a formule. Všechny jazyky „ze života“, tj. ty, o kterých si budeme klást nějaké otázky a v souvislosti s kterými se budeme snažit řešit nějaké problémy, budou konečné nebo alespoň spočetné. To ale neznamená, že všechny jazyky, které mají aplikace, tj. které mohou pomoci řešit nějaké problémy, jsou nejvýše spočetné. Uvidíme (například v důkazu věty 3.4.5), že věty o úplnosti a kompaktnosti platí pro všechny teorie bez ohledu na mohutnost jazyka a že tento fakt může mít určité důsledky i pro teorie s konečným jazykem. Z toho důvodu většinou připouštíme, aby jazyk měl libovolnou mohutnost, a termy a formule jsou v tom případě abstraktními objekty, nejspíš konečnými posloupnostmi „symbolů“.

Uvažujeme-li však o algoritmech pracujících se syntaktickými objekty (nastane to v oddílu 3.6 a později), potřebujeme mít možnost považovat termy a formule za posloupnosti skutečných symbolů, tj. prvků nějaké konečné abecedy. V tomto případě s množinou Var všech proměnných zacházíme stejně, jako jsme v kapitole 2 zacházeli s množinou všech výrokových atomů: předpokládáme, že její prvky jsou očíslovány, $\mathrm{Var} = \{v_0, v_1, v_2, \dots\}$, že každá proměnná v_i sestává z písmene v a ze zápisu indexu i a že jsme se rozhodli, zda indexy zapisujeme unárně, binárně či dekadicky. Dále v tomto případě předpokládáme, že jazyk je nejvýše spočetný, a že je-li nekonečný, byla pro zapisování jeho prvků přijata podobná dohoda jako pro zapisování proměnných.

3.1.2 Struktury

Definice 3.1.7 Struktura pro jazyk L *je neprázdná množina* D *(*nosná množina struktury*) spolu s funkcí* r *definovanou na* L*. Když* $c \in L$ *je konstanta, pak* $r(c)$ *je prvek množiny* D*. Když* $F \in L$ *je* n*-ární funkční symbol a* $n \geq 1$*, pak* $r(F)$ *je* n*-ární operace na množině* D*, tj. funkce z* D^n *do* D*. Když* $P \in L$ *je* n*-ární predikátový symbol, pak* $r(P)$ *je* n*-ární relace na množině* D*, tj. platí* $r(P) \subseteq D^n$*. Prvku* $r(c)$*, funkci* $r(F)$ *a relaci* $r(P)$ *říkáme* realizace *symbolu* c *resp. symbolu* F *resp. symbolu* P *v dané struktuře. V predikátové logice s rovností je realizací* $r(=)$ *symbolu* $=$ *vždy diagonála na množině* D*, tj. množina* $\{\, [x, x] \,;\, x \in D \,\}$*.*

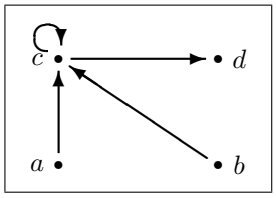
A:

$r_1(+)$	a	b
a	a	b
b	b	a

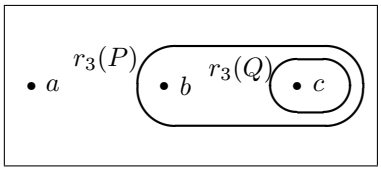
$r_1(0) = a$

$r_1(\mathrm{S})$	
a	b
b	b

B



C



Obrázek 3.1.1: Různé struktury

Příklad 3.1.8 Uvažujme jazyk $\{+, 0, \mathrm{S}\}$, kde $+$ je binární, S unární funkční symbol a 0 je konstanta. Vezměme dvouprvkovou množinu $A = \{a, b\}$ a definujme realizace $r_1(+)$, $r_1(0)$, $r_1(\mathrm{S})$ tří symbolů našeho jazyka rovností $r_1(0) = a$ a dvěma tabulkami na obrázku 3.1.1 nahoře. Výsledná struktura $\mathbf{A} = \langle \{a, b\}, r_1(+), a, r_1(\mathrm{S}) \rangle$ je opravdu strukturou pro jazyk $\{+, 0, \mathrm{S}\}$, neboť $r_1(+)$, a a $r_1(\mathrm{S})$ jsou binární, „nulární“ a unární operace na množině $\{a, b\}$. Dole na témže obrázku jsou dva další příklady struktur. Vlevo je struktura $\mathbf{B} = \langle \{a, b, c, d\}, r_2(\in) \rangle$ se čtyřprvkovou nosnou množinou $B = \{a, b, c, d\}$ a s binární relací znázorněnou šipkami. Struktura $\mathbf{B}$ je strukturou pro jazyk s jediným binárním predikátem $\in$. Vpravo je struktura $\mathbf{C}$ pro jazyk $\{P, Q\}$ se dvěma unárními predikátovými symboly. Realizace $\{b, c\}$ a $\{c\}$ symbolů P a Q jsou vyznačeny ovály.

Všechny struktury v předchozím příkladu jsou konečné. Definice struktury ale připouští libovolné mohutnosti nosných množin.

Při označování struktur budeme většinou postupovat tak, jak naznačuje předchozí příklad a jak je běžné v algebře. Strukturu označíme tučnou variantou téhož písmene, kterým je označena její nosná množina, a realizaci symbolu I ve struktuře $\mathbf{D}$ budeme značit $I^{\mathbf{D}}$ místo $r(I)$. V případě, kdy jazyk L je konečný, budeme strukturu zapisovat jako n-tici, v níž za nosnou množinou následují realizace symbolů jazyka L.

Jmenujme nyní několik *prominentních struktur* běžných v matematice. Nechť s označuje funkci $x \mapsto x + 1$, tj. přičítání jedničky, uvažovanou v množině všech přirozených nebo celých čísel. Pak struktura $\mathbf{N} = \langle \mathrm{N}, +^{\mathbf{N}}, \cdot^{\mathbf{N}}, 0^{\mathbf{N}}, \mathrm{s}, \leq^{\mathbf{N}}, <^{\mathbf{N}} \rangle$, tj. množina všech přirozených čísel s obvyklými operacemi a s neostrým a ostrým uspořádáním, je struktura pro aritmetický jazyk, kterou nazýváme *strukturou přirozených čísel*. V případech, jako je tento, kdy aritmetické symboly mají „obvyklý“ význam, si dovolíme nedůslednost a budeme psát

$$\mathbf{N} = \langle \mathrm{N}, +, \cdot, 0, \mathrm{s}, \leq, < \rangle,$$

tj. nebudeme (s výjimkou symbolu S) rozlišovat mezi symbolem a označením pro

jeho realizaci. Jinou strukturou pro aritmetický jazyk je struktura

$$\mathbf{Z} = \langle \mathrm{Z}, +, \cdot, 0, \mathrm{s}, \leq, < \rangle$$

celých čísel. Za strukturu *racionálních čísel* a *reálných čísel* považujme struktury

$$\mathbf{Q} = \langle \mathrm{Q}, +, \cdot, 0, 1, < \rangle \quad \text{a} \quad \mathbf{R} = \langle \mathrm{R}, +, \cdot, 0, 1, < \rangle$$

pro (v obou případech týž) jazyk se dvěma binárními funkčními symboly, dvěma konstantami a jedním binárním predikátem. Někdy budeme také uvažovat jiné (například menší) jazyky a mluvit třeba o struktuře $\langle \mathrm{Q}, < \rangle$ všech racionálních čísel s uspořádáním nebo o struktuře $\langle \mathrm{Z}, +, 0 \rangle$ všech celých čísel se sčítáním a s nulou. Řekne-li se ale například „struktura přirozených čísel“ nebo „struktura reálných čísel“ bez dalšího určení, myslí se tím výše definovaná struktura $\mathbf{N}$ nebo $\mathbf{R}$ pro aritmetický jazyk resp. pro jazyk $\{+, \cdot, 0, 1, <\}$. Je zřejmé, že některé symboly jsou do našich jazyků zařazeny jen pro pohodlí. Například ze dvou symbolů $\leq$ a $<$ by většinou stačilo uvažovat jen jeden a ve struktuře $\mathbf{N}$ by dokonce bylo možné se vzdát obou, neboť uspořádání přirozených čísel je definovatelné (s přesnou definicí se setkáme později) pomocí sčítání. Všechny struktury $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ a $\mathbf{R}$ považujeme za struktury pro predikátovou logiku s rovností.

Nechť L je jazyk a nechť $\mathbf{D} = \langle D, r \rangle$ je struktura pro L. *Ohodnocením proměnných* ve struktuře $\mathbf{D}$ nazvěme libovolnou funkci z množiny Var všech proměnných do nosné množiny D struktury $\mathbf{D}$. Je-li e ohodnocení proměnných ve struktuře $\langle D, r \rangle$, je-li x proměnná a je-li a prvek množiny D, výraz $e(x/a)$ označuje ohodnocení proměnných, které proměnné x přiřazuje hodnotu a a na všech ostatních proměnných se shoduje s ohodnocením e.

Máme-li strukturu $\mathbf{D}$ a ohodnocení proměnných e ve struktuře $\mathbf{D}$, můžeme se ptát, jaká je hodnota daného termu t ve struktuře $\mathbf{D}$ při ohodnocení e a zda daná formule φ je nebo není v $\mathbf{D}$ splněna ohodnocením e. Fakt, že φ je v $\mathbf{D}$ splněna ohodnocením e, značíme $\mathbf{D} \models \varphi[e]$. Symbol $\models$ tedy v predikátové logice označuje (mimo jiné, jak brzy uvidíme) ternární relaci mezi strukturami, formulemi a ohodnoceními. Ternární relaci můžeme ovšem také chápat jako ternární funkci s hodnotami v množině $\{0, 1\}$. Tato funkce se definuje rekurzí podle složitosti formule. Nejprve je třeba definovat hodnotu $t^{\mathbf{D}}[e]$ termu t ve struktuře $\mathbf{D}$, a to rovněž rekurzí podle složitosti termu t.

Definice 3.1.9 *Nechť $\mathbf{D} = \langle D, r \rangle$ je struktura pro jazyk L.*
(a) Hodnota $t^{\mathbf{D}}[e]$ *libovolného* termu t *při ohodnocení proměnných e ve struktuře $\mathbf{D}$ je určena rovnostmi*

T1: $t^{\mathbf{D}}[e] = e(t)$, *když t je proměnná,*

T2: $(F(t_1, .., t_n))^{\mathbf{D}}[e] = r(F)(t_1^{\mathbf{D}}[e], .., t_n^{\mathbf{D}}[e])$,
když $F \in L$ je n-ární funkční symbol.

(b) Relace $\models$ mezi strukturami, formulemi a ohodnoceními proměnných je určena ekvivalencemi

T3: $\mathbf{D} \models P(t_1, .., t_n)[e] \;\Leftrightarrow\; [t_1^{\mathbf{D}}[e], .., t_n^{\mathbf{D}}[e]] \in r(P)$,
když $P \in L$ *je* n*-ární predikátový symbol,*

T4: $\mathbf{D} \models (\varphi \to \psi)[e] \;\Leftrightarrow\; \mathbf{D} \not\models \varphi[e]$ *nebo* $\mathbf{D} \models \psi[e]$,

T5: $\mathbf{D} \models (\neg\varphi)[e] \;\Leftrightarrow\; \mathbf{D} \not\models \varphi[e]$,

T6: $\mathbf{D} \models (\varphi \,\&\, \psi)[e] \;\Leftrightarrow\; \mathbf{D} \models \varphi[e]$ *a* $\mathbf{D} \models \psi[e]$,

T7: $\mathbf{D} \models (\varphi \vee \psi)[e] \;\Leftrightarrow\; \mathbf{D} \models \varphi[e]$ *nebo* $\mathbf{D} \models \psi[e]$,

T8: $\mathbf{D} \models (\exists x\varphi)[e] \;\Leftrightarrow\; \exists a \in D(\mathbf{D} \models \varphi[e(x/a)])$,

T9: $\mathbf{D} \models (\forall x\varphi)[e] \;\Leftrightarrow\; \forall a \in D(\mathbf{D} \models \varphi[e(x/a)])$.

Zápis $\mathbf{D} \models \varphi[e]$ *čteme „*φ *je* splněna *ohodnocením* e *ve struktuře* $\mathbf{D}$*“ nebo „ohodnocení* e splňuje *v* $\mathbf{D}$ *formuli* φ*“.*

Tato definice je podstatnou součástí sémantiky predikátové logiky. Říká se jí *Tarského definice*, případně *definice platnosti formule ve struktuře*, někdy též *(Tarského) definice pravdy.* Písmeno „T“ v označení podmínek T1–T9 odkazuje ke jménu „Tarski“ a zároveň k anglickému slovu „true“. Všimněme si, že definice 3.1.9 opravdu korektně definuje ternární relaci. Podmínky T4–T9 převádějí otázku, zda daná formule je nebo není splněna, na tutéž otázku pro jednodušší a jednodušší formule. U atomických formulí, kterých se týká podmínka T3, záleží na hodnotách termů. Ty jsou určeny podmínkami T1 a T2. K podmínce T8 pro jistotu poznamenejme, že kvantifikátor $\exists$ je v ní užit v různých významech: vlevo je (skutečným čili formálním) symbolem, vpravo je (neformálně-jazykovou čili metamatematickou) zkratkou. Totéž platí o kvantifikátoru $\forall$ v podmínce T9.

Příklad 3.1.10 (a) Předpokládejme, že e_1 je nějaké ohodnocení proměnných ve struktuře $\mathbf{A}$ z obrázku 3.1.1, které proměnným x a z přiřazuje hodnoty b a a. Podmínka T1 říká, že b a a jsou zároveň hodnotami termů x a z. Podmínka T2 dává $(\mathrm{S}(x))^{\mathbf{A}}[e_1] = b$ a $(\mathrm{S}(x) + z)^{\mathbf{A}}[e_1] = b$. Oba termy $\mathrm{S}(x)$ a $\mathrm{S}(x) + z$ mají ve struktuře $\mathbf{A}$ při ohodnocení e_1 tutéž hodnotu b.
(b) Nechť e_2 je nějaké ohodnocení proměnných ve struktuře $\mathbf{R}$ reálných čísel, které proměnným x, y a z přiřazuje postupně hodnoty 3, 15 a 5. Podmínky T1 a T2 dávají $(z \cdot x)^{\mathbf{R}}[e_2] = 15$. Vzpomeňme si, že v predikátové logice s rovností je realizací symbolu „=“ rovnost, v našem případě na množině R. Podmínka T3 dává $\mathbf{R} \models (z \cdot x = y)[e_2]$. Podle podmínky T8 platí také $\mathbf{R} \models (\exists z(z \cdot x = y))[e_2]$, neboť ohodnocení e_2 je možné v bodě z předefinovat (dokonce to ani není nutné) tak, aby výsledné ohodnocení splňovalo formuli $z \cdot x = y$.
(c) Nechť e_3 je nějaké ohodnocení proměnných ve struktuře $\mathbf{C}$ znázorněné na obrázku 3.1.1. Platí $\mathbf{C} \models (P(x))[e_3(x/b)]$ a $\mathbf{C} \not\models (Q(x))[e_3(x/b)]$. Tedy, podle T4 a T9,

$$\mathbf{C} \not\models (P(x) \to Q(x))[e_3(x/b)] \quad \text{a} \quad \mathbf{C} \not\models (\forall x(P(x) \to Q(x)))[e_3].$$

Podobně lze ověřit $\mathbf{C} \not\models (\forall x P(x))[e_3]$ a $\mathbf{C} \models (\forall x P(x) \to \forall x Q(x))[e_3]$.
(d) Je-li $c \in L$ konstanta, podmínka T2 říká $c^{\mathbf{D}}[e] = r(c)$. To znamená, že realizace

konstanty c v libovolné struktuře $\mathbf{D}$ je zároveň hodnotou konstanty c jako termu, a to bez ohledu na ohodnocení proměnných. Například hodnotami termů 0 a S(S(0)) ve struktuře $\mathbf{A}$ z obrázku 3.1.1 jsou prvky a a b množiny A, a to při každém ohodnocení proměnných e_4.

Termům 0, S(0), S(S(0)), ... aritmetického jazyka říkáme *numerály* a značíme je $\overline{0}$, $\overline{1}$, $\overline{2}$ atd. Numerál $\overline{n}$ je tedy term tvaru S(S(..(0)..) obsahující jeden výskyt konstanty 0, dále n výskytů symbolu S a ovšem příslušné množství závorek. Termy $\overline{0}$ a 0 jsou totožné. Numerály umožňují v aritmetickém jazyce formulovat tvrzení o konkrétních (metamatematických) přirozených číslech, protože hodnotou libovolného numerálu $\overline{n}$ ve struktuře $\mathbf{N}$ je číslo n, a to při libovolném ohodnocení proměnných.

Body (c) a (d) v předchozím příkladě naznačují, že hodnota termu t při ohodnocení proměnných e závisí na hodnotách jen těch proměnných, které se v t skutečně vyskytují, a platnost vztahu $\mathbf{D} \models \varphi[e]$ závisí na ohodnocení jen těch proměnných, které se ve φ vyskytují volně. Hned dokážeme, že tomu tak skutečně je. Pro sentenci φ to znamená, že je-li φ ve struktuře $\mathbf{D}$ splněna nějakým ohodnocením e, pak je v $\mathbf{D}$ splněna *každým* ohodnocením e.

Lemma 3.1.11 *Nechť $\mathbf{D}$ je struktura pro jazyk L, nechť $x_1, .., x_n$ jsou proměnné a nechť e_1 a e_2 jsou ohodnocení proměnných ve struktuře $\mathbf{D}$, která se shodují na proměnných $x_1, .., x_n$.*
(a) Je-li t term jazyka L, jehož všechny proměnné jsou mezi $x_1, .., x_n$, pak platí $t^{\mathbf{D}}[e_1] = t^{\mathbf{D}}[e_2]$.
(b) Je-li φ formule jazyka L, jejíž všechny volné proměnné jsou mezi $x_1, .., x_n$, pak $\mathbf{D} \models \varphi[e_1] \Leftrightarrow \mathbf{D} \models \varphi[e_2]$.

Důkaz Indukcí podle složitosti termu t či formule φ lze snadno ukázat, že (a) i (b) platí pro danou strukturu $\mathbf{D}$, pro všechny seznamy $x_1, .., x_n$ proměnných obsahující všechny proměnné vyskytující se v t (resp. vyskytující se volně ve φ) a pro všechny dvojice e_1, e_2 ohodnocení shodujících se na $x_1, .., x_n$. Ukažme si podstatný případ, totiž ten, kdy formule φ v (b) je utvořena z jednodušší formule pomocí kvantifikace. Nechť tedy e_1, e_2, seznam $x_1, .., x_n$ a formule φ jsou dány a nechť φ je tvaru $\forall y\psi$. Předpokládejme, že proměnná y je různá od všech $x_1, .., x_n$. Úvaha v případě, kdy y je x_i, je podobná. Všechny volné proměnné formule ψ jsou mezi $y, x_1, .., x_n$ a pro libovolné $a \in D$ se ohodnocení $e_1(y/a)$ a $e_2(y/a)$ shodují na $y, x_1, .., x_n$. Podle indukčního předpokladu jsou podmínky $\mathbf{D} \models \psi[e_1(y/a)]$ a $\mathbf{D} \models \psi[e_2(y/a)]$ ekvivalentní. Z toho plyne druhá z následujících tří ekvivalencí:

$$\begin{aligned} \mathbf{D} \models (\forall y\psi)[e_1] &\Leftrightarrow \forall a \in D(\mathbf{D} \models \psi[e_1(y/a)]) \\ &\Leftrightarrow \forall a \in D(\mathbf{D} \models \psi[e_2(y/a)]) \\ &\Leftrightarrow \mathbf{D} \models (\forall y\psi)[e_2]. \end{aligned}$$

Zbývající dvě ekvivalence plynou bezprostředně z podmínky T9. QED

Nechť φ je formule, jejíž všechny volné proměnné jsou mezi $x_1, .., x_n$. Domluvme se, že nebude-li pochybnost o pořadí proměnných $x_1, .., x_n$, pak zápisem $\mathbf{D} \models \varphi[a_1, .., a_n]$ budeme označovat fakt, že φ je v $\mathbf{D}$ splněna některým nebo každým ohodnocením, které proměnným $x_1, .., x_n$ přiřazuje hodnoty $a_1, .., a_n$. Vzhledem k předchozímu lemmatu je tento zápis korektní. Je-li například φ formule $\exists z(z \cdot x = y)$ z příkladu 3.1.10(b), budeme psát třeba $\mathbf{R} \models \varphi[3, 15]$ a číst „formule φ je ve struktuře reálných čísel splněna dvojicí $[3, 15]$“.

3.1.3 Substituce, důsledek, logicky platné formule

Nechť s je term, $x_1, .., x_n$ jsou navzájem různé proměnné a $t_1, .., t_n$ jsou termy nějakého jazyka L. Označme $s_{x_1,..,x_n}(t_1, .., t_n)$ term, který vznikne z termu s současným nahrazením každého výskytu každé proměnné x_i termem t_i. Podobně, je-li φ formule v L, pak $\varphi_{x_1,..,x_n}(t_1, .., t_n)$ je formule, která vznikne z formule φ současným nahrazením každého *volného* výskytu každé proměnné x_i termem t_i. Operaci, která ze seznamu proměnných $x_1, .., x_n$, seznamu termů $t_1, .., t_n$ a termu s nebo formule φ vytvoří term $s_{x_1,..,x_n}(t_1, .., t_n)$ resp. formuli $\varphi_{x_1,..,x_n}(t_1, .., t_n)$, nazýváme *současnou (simultánní) substitucí (dosazením)* termů za proměnné do termu nebo do formule. Přitom se nepředpokládá, že proměnné $x_1, .., x_n$ se v s nebo ve φ skutečně vyskytují, a nepředpokládá se ani, že v s nebo φ nejsou jiné (volné) proměnné než $x_1, .., x_n$. Proměnné $x_1, .., x_n$ se mohou vyskytovat v termech $t_1, .., t_n$.

Slovo „současná“ v předchozím odstavci je důležité. Představme si, že φ je formule $x < y$, term t_1 je y a t_2 je x. Pak $\varphi_{x,y}(t_1, t_2)$ je formule $y < x$. To je ale jiná formule než $(\varphi_x(t_1))_y(t_2)$. Přes tuto potíž ale platí, že současnou substituci n termů lze nahradit několika substitucemi jednoho termu. To lze udělat následovně. Nechť φ je formule, $x_1, .., x_n$ navzájem různé proměnné a $t_1, .., t_n$ termy. Zvolme proměnné $v_1, .., v_n$, které jsou navzájem různé a nevyskytují se ve φ ani v termech $t_1, .., t_n$. Snadno lze ověřit, že substituujeme-li ve φ (po jedné) v_1 za x_1 až v_n za x_n, a pak (opět po jedné) t_1 za v_1 až t_n za v_n, dostaneme formuli $\varphi_{x_1,..,x_n}(t_1, .., t_n)$. Díky tomuto postupu vystačíme v následujícím lemmatu, a také v příštím oddílu, když budeme formulovat axiomy hilbertovského kalkulu pro predikátovou logiku, se substitucí jediného termu. Následující příklad ukazuje, že nejprve musíme překonat ještě další potíž.

Příklad 3.1.12 Nechť φ je aritmetická formule $\exists y(x < y)$. Pak formule $\forall x\varphi$ je ve struktuře $\mathbf{N}$ splněna jakýmkoliv ohodnocením, ale $\varphi_x(y)$ je formule $\exists y(y < y)$, o které to neplatí.

Definice 3.1.13 *Řekneme, že term t* není substituovatelný *za proměnnou x ve formuli φ, jestliže některý volný výskyt proměnné x ve formuli φ je součástí takové podformule $\forall v\psi$ nebo $\exists v\psi$ formule φ, že proměnná v se vyskytuje v termu t. V opačném případě term t* je substituovatelný *za x ve φ.*

Jinými slovy, term t je substituovatelný za x ve formuli φ, jestliže žádný výskyt proměnné v termu t se substitucí nestane vázaným výskytem. Krajní případy jsou

tyto: každý term je substituovatelný za libovolnou proměnnou do otevřené formule, každý term je substituovatelný ve formuli φ za libovolnou proměnnou, která se ve φ nevyskytuje, uzavřený term je substituovatelný za libovolnou proměnnou v libovolné formuli a libovolná proměnná je substituovatelná sama za sebe v libovolné formuli.

Domluvme se, že zápis $\varphi_x(t)$ pro substituci budeme nadále užívat pouze v případě, kdy term t je substituovatelný za x ve φ.

Lemma 3.1.14 *Nechť e je ohodnocení proměnných ve struktuře $\mathbf{D}$ pro jazyk L, nechť dále t je term jazyka L a x je proměnná.*
(a) Je-li s term jazyka L, pak $(s_x(t))^{\mathbf{D}}[e] = s^{\mathbf{D}}[e(x/t^{\mathbf{D}}[e])]$.
(b) Je-li φ formule jazyka L a t je substituovatelný za x ve φ, pak $\mathbf{D} \models (\varphi_x(t))[e]$, právě když $\mathbf{D} \models \varphi[e(x/t^{\mathbf{D}}[e])]$.

Důkaz Indukcí podle složitosti termu s a formule φ. Když s je proměnná x, pak $s_x(t)$ je t a $s^{\mathbf{D}}[e(x/t^{\mathbf{D}}[e])]$ je $t^{\mathbf{D}}[e]$, viz podmínku T1. Když s je proměnná y jiná než x, pak $s_x(t)$ je y a rovnost platí vzhledem k lemmatu 3.1.11, neboť ohodnocení e a $e(x/t^{\mathbf{D}}[e])$ se shodují v bodě y.

Když φ je konjunkce ψ_1 & ψ_2, pak $\varphi_x(t)$ je $(\psi_1)_x(t)$ & $(\psi_2)_x(t)$. Užitím tohoto a podobných faktů a indukčního předpokladu lze probrat všechny případy, kdy φ je sestavena z jednodušších formulí pomocí některé logické spojky a také kdy s je složeným termem. Podrobnosti přenecháváme čtenáři.

Věnujme se podrobně případu, kdy formule φ je tvaru $\exists y\psi$. Poslední případ, kdy je tvaru $\forall y\psi$, je podobný a také jej přenecháváme čtenáři.

Když y je x, pak x nemá žádné volné výskyty ve φ, $\varphi_x(t)$ je φ a ekvivalence v (b) platí podle lemmatu 3.1.11, protože ohodnocení e a $e(x/t^{\mathbf{D}}[e])$ se shodují na všech proměnných, které se ve φ vyskytují volně. Úplně stejná úvaha platí i pro případ, kdy y není x a x nemá volné výskyty ve φ.

Nechť tedy y není x a x má volné výskyty ve φ. Pak $\varphi_x(t)$ je $\exists y\psi_x(t)$ a platí

$$\begin{aligned}
\mathbf{D} \models \varphi_x(t)[e] &\Leftrightarrow \mathbf{D} \models (\exists y\psi_x(t))[e] \\
&\Leftrightarrow \exists a \in D(\mathbf{D} \models (\psi_x(t))[e(y/a)]) \\
&\Leftrightarrow \exists a \in D(\mathbf{D} \models \psi[e(y/a)(x/t^{\mathbf{D}}[e(y/a)])]) \\
&\Leftrightarrow \exists a \in D(\mathbf{D} \models \psi[e(x/t^{\mathbf{D}}[e])(y/a)]) \\
&\Leftrightarrow \mathbf{D} \models (\exists y\psi)[e(x/t^{\mathbf{D}}[e])],
\end{aligned}$$

přičemž druhá a pátá ekvivalence plynou bezprostředně z podmínky T8, třetí je indukční předpoklad a čtvrtou zdůvodněme podrobně. Složitý zápis ve třetím řádku vyjadřuje, že máme (i) v ohodnocení e hodnotu v bodě y změnit na a, při takto změněném ohodnocení určit hodnotu $t^{\mathbf{D}}[e(y/a)]$ termu t a (ii) tu pak použít ke změně hodnoty v bodě x. Protože ale term t je substituovatelný za x ve φ, a přitom x má volné výskyty ve φ, proměnná y se nevyskytuje v t. Tím ale platí rovnost $t^{\mathbf{D}}[e(y/a)] = t^{\mathbf{D}}[e]$ a kroky (i) a (ii) mohou být provedeny v opačném pořadí, jak je naznačeno ve čtvrtém řádku. QED

Definice 3.1.15 *Řekneme, že formule* φ platí *ve struktuře* $\mathbf{D}$*, a píšeme* $\mathbf{D} \models \varphi$*, jestliže* φ *je v* $\mathbf{D}$ *splněna každým ohodnocením proměnných.*

Toto je druhý význam symbolu $\models$ v predikátové logice. V zápisu $\mathbf{D} \models \varphi$ symbol $\models$ označuje binární relaci, v zápisu $\mathbf{D} \models \varphi[e]$ ternární relaci. Poznamenejme, že užívání termínů „platí“ a „splněna“ není v české literatuře úplně ustáleno. V anglické literatuře se užívají termíny *valid*, *true*, případně *satisfied*, a jejich užití možná také není zcela jednotné.

Příklad 3.1.16 (a) Formule $\forall v(v \in x \equiv v \in y) \to x = y$ neplatí ve struktuře $\mathbf{B}$ z obrázku 3.1.1, protože v $\mathbf{B}$ není splněna ohodnocením $[a, b]$.
(b) Lze ověřit (a v příkladu 3.1.10(b) to vlastně zčásti bylo provedeno), že formule $x \neq 0 \to \exists z(z \cdot x = y)$ platí ve struktuře $\mathbf{R}$ reálných čísel. Ve struktuře $\mathbf{Z}$ celých čísel tato formule některými ohodnoceními proměnných sice splněna je, ale některými není. Tedy $\mathbf{Z} \not\models \varphi$.
(c) Nechť χ je sentence $\overline{1} + \overline{2} = \overline{3}$, tj. sentence $\mathrm{S}(0) + \mathrm{S}(\mathrm{S}(0)) = \mathrm{S}(\mathrm{S}(\mathrm{S}(0)))$. Snadno lze ověřit, že pro strukturu $\mathbf{A}$ z obrázku 3.1.1 platí $\mathbf{A} \not\models \chi$ a $\mathbf{A} \models \neg\chi$.

Lemma 3.1.17 *Nechť* $\mathbf{D}$ *je struktura pro jazyk* L *a nechť* φ *je formule v* L*. Pak*
(a) Když $\mathbf{D} \models \varphi$*, pak* $\mathbf{D} \not\models \neg\varphi$*.*
(b) Když φ *je navíc sentence, pak* $\mathbf{D} \models \varphi$ *nebo* $\mathbf{D} \models \neg\varphi$*.*

Důkaz Nechť $\mathbf{D} \models \varphi$, což znamená, že φ je splněna každým ohodnocením proměnných ve struktuře $\mathbf{D}$. Protože nosná množina struktury $\mathbf{D}$ je podle definice neprázdná, znamená to také, že φ je v $\mathbf{D}$ splněna některým ohodnocením e. Z $\mathbf{D} \models \varphi[e]$ plyne dle T5, že $\mathbf{D} \not\models (\neg\varphi)[e]$. Tedy $\mathbf{D} \not\models \neg\varphi$.

Když $\mathbf{D} \not\models \varphi$, pak existuje e takové, že $\mathbf{D} \not\models \varphi[e]$. Podmínka T5 dává $\mathbf{D} \models (\neg\varphi)[e]$. Lemma 3.1.11(b) říká, že je-li sentence splněna v $\mathbf{D}$ některým ohodnocením proměnných, pak je v $\mathbf{D}$ splněna každým ohodnocením proměnných. Tedy $\mathbf{D} \models \neg\varphi$. QED

Definice 3.1.18 *Řekneme, že formule* φ *jazyka* L *je* (logickým) důsledkem *množiny formulí* Δ *nebo že* φ vyplývá *z (množiny předpokladů)* Δ *a píšeme* $\Delta \models \varphi$*, jestliže v každé struktuře* $\mathbf{D}$ *pro jazyk* L *je* φ *splněna každým ohodnocením proměnných, které v* $\mathbf{D}$ *splňuje všechny formule z* Δ*. Tedy*

$$\Delta \models \varphi \;\Leftrightarrow\; \forall \mathbf{D} \forall e(\mathbf{D} \models \Delta[e] \;\Rightarrow\; \mathbf{D} \models \varphi[e]),$$

kde $\mathbf{D} \models \Delta[e]$ *znamená* $\forall \psi \in \Delta(\mathbf{D} \models \psi[e])$*. Řekneme, že formule* φ *je* důsledkem formule ψ*, jestliže je důsledkem množiny* $\{\psi\}$*. Formule* φ *a* ψ *jsou* ekvivalentní*, jestliže* φ *je důsledkem* ψ *i* ψ *je důsledkem* φ*. Formule* φ *je* logicky platnou formulí*, jestliže* φ *vyplývá z prázdné množiny předpokladů.*

Toto je třetí (a poslední) význam symbolu $\models$ v predikátové logice. V zápisech $\mathbf{D} \models \varphi$ a $\mathbf{D} \models \varphi[e]$ vlevo stojí struktura a $\models$ znamená platnost resp. fakt, že formule

je splněna. V zápisu $\Delta \models \varphi$ vlevo stojí množina formulí a, stejně jako ve výrokové logice, $\models$ znamená důsledek. Poznamenejme, že v některých pramenech (zejména v [75]) se uvažuje trochu jiná definice důsledku, založená na podmínce $(*)$ uvedené dále na str. 160.

Je zřejmé, že — podobně jako ve výrokové logice — φ je logicky platnou formulí, právě když φ platí v každé struktuře (pro příslušný jazyk), φ je důsledkem formule ψ, právě když $\psi \to \varphi$ je logicky platnou formulí, a konečně φ a ψ jsou ekvivalentní, právě když $\varphi \equiv \psi$ je logicky platnou formulí.

Příklad 3.1.19 (a) Z formule $\forall y(y \notin x)$ vyplývá formule $\neg\exists y(y \in x)$: když pro nějakou strukturu $\mathbf{D}$ a pro každé $a \in D$ platí $\mathbf{D} \models (\neg(y \in x))[e(y/a)]$, pak neexistuje $a \in D$ takové, že $\mathbf{D} \models (y \in x)[e(y/a)]$. Tedy $\mathbf{D} \not\models (\exists y(y \in x))[e]$ a $\mathbf{D} \models (\neg\exists y(y \in x))[e]$. Naopak také formule $\forall y(y \notin x)$ vyplývá z $\neg\exists y(y \in x)$. Obě formule jsou tedy ekvivalentní.
(b) Formule $(\forall x P(x) \to \forall x Q(x)) \to \forall x(P(x) \to Q(x))$ není logicky platnou formulí, neboť v příkladu 3.1.10(c) jsme našli ohodnocení (tam označené e_3, ale hodí se jakékoliv ohodnocení), které ji nesplňuje ve struktuře $\mathbf{C}$ z obrázku 3.1.1.
(c) Formule $\overline{1} + \overline{2} = \overline{3}$ není logicky platnou formulí, viz příklad 3.1.16(c).
(d) Ve struktuře $\mathbf{C}$ z obrázku 3.1.1 existuje ohodnocení, které splňuje formuli $P(x)$, ale nesplňuje formuli $\forall v P(v)$. Formule $\forall v P(v)$ tedy nevyplývá z formule $P(x)$ a $P(x) \to \forall v P(v)$ není logicky platnou formulí.
(e) Nechť $\mathbf{D}$ je libovolná struktura pro jazyk L, nechť φ je formule v L a nechť e je ohodnocení proměnných. Když $\mathbf{D} \models (\forall x\varphi)[e]$, pak φ je v $\mathbf{D}$ splněna všemi ohodnoceními tvaru $e(x/a)$, kde $a \in D$. Mezi nimi je i původní ohodnocení e. Tím jsme ověřili, že každá formule φ vyplývá z formule $\forall x\varphi$. V bodu (a) následujícího lemmatu toto tvrzení ještě zesílíme.
(f) Je-li v nějaké struktuře $\mathbf{D}$ rovnítko realizováno rovností na množině D, pak formule

$$\gamma_n = \forall x_1 \,..\, \forall x_n \exists y(y \neq x_1 \ \&\ \,..\, \ \&\ y \neq x_n),$$

kde $n \geq 1$, ve struktuře $\mathbf{D}$ platí, kdykoliv je nosná množina D nekonečná (a také kdykoliv je konečná s alespoň $n+1$ prvky). Uvažujme jazyk $\{0, \mathrm{S}\}$ s konstantou a unární funkcí a množinu předpokladů

$$\Delta = \{\, \forall x(\mathrm{S}(x) \neq 0),\ \forall x \forall y(\mathrm{S}(x) = \mathrm{S}(y) \ \to\ x = y) \,\}.$$

Platí-li Δ v $\mathbf{D}$, pak realizace $\mathrm{S}^{\mathbf{D}}$ symbolu S v $\mathbf{D}$ musí být funkce z D do D, která je prostá a není *na*. To lze zařídit pouze v případě, je-li nosná množina struktury $\mathbf{D}$ nekonečná. Ověřili jsme, že pro každé n sentence γ_n platí v každé struktuře $\mathbf{D}$ pro jazyk $\{0, \mathrm{S}\}$, ve které platí všechny prvky množiny Δ. Každá sentence γ_n tedy v predikátové logice s rovností vyplývá z množiny Δ.

Lemma 3.1.20 *(a) Je-li t term substituovatelný za x ve φ, pak $\forall x\varphi \to \varphi_x(t)$ a $\varphi_x(t) \to \exists x\varphi$ jsou logicky platné formule.*
(b) Nechť x se nevyskytuje volně v ψ. Když $\mathbf{D} \models \psi \to \varphi$, pak $\mathbf{D} \models \psi \to \forall x\varphi$. Když $\mathbf{D} \models \varphi \to \psi$, pak $\mathbf{D} \models \exists x\varphi \to \psi$.

(c) Nechť v je proměnná substituovatelná za x ve φ a nechť v se nevyskytuje volně ve φ. Pak $\forall x\varphi$ a $\forall v\varphi_x(v)$ jsou spolu ekvivalentní a také $\exists x\varphi$ a $\exists v\varphi_x(v)$ jsou spolu ekvivalentní.
(d) Nechť φ a ψ jsou ekvivalentní formule. Pak $\forall x\varphi$ a $\forall x\psi$, a také $\exists x\varphi$ a $\exists x\psi$ jsou spolu ekvivalentní.

Důkaz Nechť $\mathbf{D}$ je struktura pro jazyk L a nechť e je ohodnocení proměnných ve struktuře $\mathbf{D}$. Když $\mathbf{D} \not\models (\forall x\varphi)[e]$, pak podle T4 máme $\mathbf{D} \models (\forall x\varphi \to \varphi_x(t))[e]$. Nechť tedy platí $\mathbf{D} \models (\forall x\varphi)[e]$. Pak podle T9 je formule φ v $\mathbf{D}$ splněna každým ohodnocením tvaru $e(x/a)$. Určeme hodnotu $t^{\mathbf{D}}[e]$ termu t a zvolme $a := t^{\mathbf{D}}[e]$. Z $\mathbf{D} \models \varphi[e(x/t^{\mathbf{D}}[e])]$ plyne díky lemmatu 3.1.14(b), že platí i $\mathbf{D} \models (\varphi_x(t))[e]$. Podmínka T4 i v tomto případě dává $\mathbf{D} \models (\forall x\varphi \to \varphi_x(t))[e]$. Ověřili jsme, že implikace $\forall x\varphi \to \varphi_x(t)$ je v $\mathbf{D}$ splněna každým ohodnocením e. To platí pro každou strukturu $\mathbf{D}$. Ověření, že každá formule tvaru $\varphi_x(t) \to \exists x\varphi$ je logicky platnou formulí, je podobné.

Nechť e je ohodnocení proměnných ve struktuře $\mathbf{D}$ takové, že $\mathbf{D} \models \psi[e]$. Chceme ověřit $\mathbf{D} \models (\forall x\varphi)[e]$. Uvažujme libovolné ohodnocení tvaru $e(x/a)$. Lemma 3.1.11 říká $\mathbf{D} \models \psi[e(x/a)]$, protože nevyskytuje-li se x v ψ volně, ohodnocení e a $e(x/a)$ se shodují na všech volných proměnných formule ψ. Protože $\mathbf{D} \models \psi \to \varphi$, máme $\mathbf{D} \models (\psi \to \varphi)[e(x/a)]$. Tedy $\mathbf{D} \models \varphi[e(x/a)]$. Ověřili jsme, že φ je v $\mathbf{D}$ splněna každým ohodnocením tvaru $e(x/a)$. Podmínka T9 dává $\mathbf{D} \models (\forall x\varphi)[e]$. Důkaz druhého tvrzení v (b) je analogický. Všimněme si, že v tomto případě jsme nepotřebovali lemma 3.1.14.

Je-li v substituovatelná za x ve φ, pak $\forall x\varphi \to \varphi_x(v)$ a $\varphi_x(v) \to \exists x\varphi$ jsou logicky platné formule podle tvrzení (a). Nevyskytuje-li se v volně ve φ, (b) říká, že i $\forall x\varphi \to \forall v\varphi_x(v)$ a $\exists v\varphi_x(v) \to \exists x\varphi$ jsou logicky platné formule. Logická platnost opačných implikací plyne z toho, že nevyskytuje-li se v volně ve φ, pak $(\varphi_x(v))_v(x)$ je φ.

Nechť $\mathbf{D}$ je libovolná struktura pro daný jazyk. Protože φ a ψ jsou ekvivalentní, platí $\mathbf{D} \models \varphi \to \psi$. Z tvrzení (a) nebo z příkladu 3.1.19(e) víme $\mathbf{D} \models \forall x\varphi \to \varphi$. Tedy $\mathbf{D} \models \forall x\varphi \to \psi$. Tvrzení (b) dává $\mathbf{D} \models \forall x\varphi \to \forall x\psi$, neboť x se nevyskytuje volně ve formuli $\forall x\varphi$. Důkaz druhého tvrzení v (d) je opět analogický. QED

Příklad 3.1.21 Označme ψ aritmetickou formuli $\overline{1} + \overline{2} = \overline{1} + \overline{3}$. Z ψ vyplývají obě formule $\exists x(x + \overline{2} = \overline{1} + \mathrm{S}(\mathrm{S}(x)))$ a $\exists x(\overline{1} + x = \overline{1} + \mathrm{S}(x))$, neboť jak z formule $x + \overline{2} = \overline{1} + \mathrm{S}(\mathrm{S}(x))$, tak z formule $\overline{1} + x = \overline{1} + \mathrm{S}(x)$ lze formuli ψ získat substitucí (substituovatelného) termu za x.

Lemma 3.1.22 *Nechť φ a χ jsou formule a nechť x se nevyskytuje volně ve formuli χ. Pak následující formule jsou logicky platné:*

(a) $\neg\forall x\varphi \equiv \exists x\neg\varphi$, $\quad \neg\exists x\varphi \equiv \forall x\neg\varphi$,
(b) $\chi \vee \forall x\varphi \equiv \forall x(\chi \vee \varphi)$, $\quad \chi \vee \exists x\varphi \equiv \exists x(\chi \vee \varphi)$,
(c) $\chi \,\&\, \forall x\varphi \equiv \forall x(\chi \,\&\, \varphi)$, $\quad \chi \,\&\, \exists x\varphi \equiv \exists x(\chi \,\&\, \varphi)$,

(d) $\chi \to \forall x\varphi \equiv \forall x(\chi \to \varphi)$, $\quad \chi \to \exists x\varphi \equiv \exists x(\chi \to \varphi)$,
(e) $\forall x\varphi \to \chi \equiv \exists x(\varphi \to \chi)$, $\quad \exists x\varphi \to \chi \equiv \forall x(\varphi \to \chi)$.

Důkaz Ověřme implikaci $\to$ v druhé formuli bodu (e). Všechny ostatní případy jsou podobné nebo jednodušší a přenecháváme je čtenáři. Nechť $\mathbf{D}$ je struktura pro příslušný jazyk a nechť e je ohodnocení proměnných splňující v $\mathbf{D}$ formuli $\exists x\varphi \to \chi$. Chceme ověřit $\mathbf{D} \models (\forall x(\varphi \to \chi))[e]$. To znamená ověřit, že $\mathbf{D} \models (\varphi \to \chi)[e(x/a)]$ platí pro každé $a \in D$. Nechť tedy $a \in D$ je dáno. Rozlišme případy $\mathbf{D} \models (\exists x\varphi)[e]$ a $\mathbf{D} \not\models (\exists x\varphi)[e]$. Když $\mathbf{D} \not\models (\exists x\varphi)[e]$, pak podle podmínky T8 pro každé $b \in D$ platí $\mathbf{D} \not\models \varphi[e(x/b)]$. Volba $b := a$ a podmínka T4 dávají $\mathbf{D} \models (\varphi \to \chi)[e(x/a)]$. Když $\mathbf{D} \models (\exists x\varphi)[e]$, předpoklad $\mathbf{D} \models (\exists x\varphi \to \chi)[e]$ a podmínka T4 dávají $\mathbf{D} \models \chi[e]$. Protože x se nevyskytuje volně v χ, lemma 3.1.11 dává $\mathbf{D} \models \chi[e(x/a)]$, ohodnocení e a $e(x/a)$ se totiž shodují na všech proměnných volných v χ. Tedy i v tomto případě platí $\mathbf{D} \models (\varphi \to \chi)[e(x/a)]$. QED

Řekneme, že formule φ je v *prenexním normálním tvaru* nebo že φ je *prenexní formule*, jestliže φ má tvar $Q_1x_1 \,..\, Q_nx_n\alpha$, kde každý ze symbolů Q_i je některý z kvantifikátorů, $x_1, \ldots, x_n$ jsou navzájem různé proměnné a α je otevřená formule. Formule φ je *existenční formule*, jestliže φ je prenexní formule, jejíž všechny kvantifikátory jsou existenční. Formule φ je naopak *univerzální formule*, jestliže φ je prenexní formule, jejíž všechny kvantifikátory jsou univerzální.

Věta 3.1.23 *Každá predikátová formule je ekvivalentní s jistou formulí v prenexním normálním tvaru.*

Důkaz indukcí podle počtu kroků, kterými je φ utvořena z atomických formulí, tj. podle souhrnného počtu logických spojek a kvantifikátorů ve φ.

Když φ neobsahuje logické spojky ani kvantifikátory, pak φ je prenexní formulí.

Nechť φ je tvaru $\forall y\psi$. Formule ψ je z atomických formulí utvořena méně kroky než φ. Podle indukčního předpokladu tedy existuje formule tvaru $Q_1x_1 \,..\, Q_nx_n\alpha$, která je ekvivalentní s ψ. Přitom $x_1, \ldots, x_n$ jsou navzájem různé a α je otevřená formule. Formule $\forall yQ_1x_1 \,..\, Q_nx_n\alpha$ je podle lemmatu 3.1.20(d) ekvivalentní s $\forall y\psi$ a je to prenexní formule, ledaže by proměnná y byla totožná s některou x_i. V tom případě jsou formule $\forall yQ_1x_1 \,..\, Q_nx_n\alpha$ a $Q_1x_1 \,..\, Q_nx_n\alpha$ ekvivalentní (cvičení), a formule $\forall y\psi$ je tedy ekvivalentní s prenexní formulí $Q_1x_1 \,..\, Q_nx_n\alpha$.

Nechť φ je tvaru $\psi_1 \to \psi_2$. Podle indukčního předpokladu existuje formule tvaru $Q_1x_1 \,..\, Q_nx_n\alpha$ ekvivalentní s ψ_1 a formule tvaru $Q_{n+1}y_1 \,..\, Q_{n+m}y_m\beta$ ekvivalentní s ψ_2. Přitom $x_1, \ldots, x_n$ jsou navzájem různé, $y_1, \ldots, y_m$ jsou navzájem různé a formule α a β jsou otevřené. Zvolme navzájem různé proměnné $v_1, \ldots, v_n$ tak, že v_i je x_i, když x_i se nevyskytuje volně ani vázaně ve formuli $Q_{n+1}y_1 \,..\, Q_{n+m}y_m\beta$, a v_i je nová proměnná v opačném případě. To lze, protože množina Var všech proměnných je nekonečná. Předpokládejme, že pro nějaké i, kde $0 < i \leq n$, platí, že formule

$$Q_{i+1}v_{i+1} \,..\, Q_nv_n\alpha_{x_{i+1},..,x_n}(v_{i+1}, \ldots, v_n) \quad \text{a} \quad Q_{i+1}x_{i+1} \,..\, Q_nx_n\alpha \qquad (*)$$

jsou spolu ekvivalentní. Ověříme, že v tom případě to platí i pro $i-1$. Ze tří formulí

$$Q_i v_i Q_{i+1} v_{i+1} \,..\, Q_n v_n \alpha_{x_i, x_{i+1}, .., x_n}(v_i, v_{i+1}, .., v_n),$$
$$Q_i x_i Q_{i+1} v_{i+1} \,..\, Q_n v_n \alpha_{x_{i+1}, .., x_n}(v_{i+1}, .., v_n),$$
$$Q_i x_i Q_{i+1} x_{i+1} \,..\, Q_n x_n \alpha$$

jsou totiž první dvě ekvivalentní vzhledem k tvrzení 3.1.20 (c) nebo (d), druhá s třetí díky předpokladu o formulích v $(*)$ a tvrzení 3.1.20(d). Pro $i = n$ jsou formule v $(*)$ totožné, tedy ekvivalentní. Sestupnou indukcí jsme dokázali, že formule v $(*)$ jsou ekvivalentní pro $i = 0$: formule $Q_1 v_1 \,..\, Q_n v_n \alpha_{\underline{x}}(\underline{v})$, kde $\underline{x}$ a $\underline{v}$ značí $x_1, .., x_n$ resp. $v_1, .., v_n$, je ekvivalentní s $Q_1 x_1 \,..\, Q_n x_n \alpha$, a tedy také s ψ_1. Nechť dále $\overline{Q_i}$ označuje kvantifikátor opačný ke Q_i. Formule $\psi_1 \to \psi_2$, tj. formule φ, je ekvivalentní s každou z formulí

$$Q_1 v_1 \,..\, Q_n v_n \alpha_{\underline{x}}(\underline{v}) \to Q_{n+1} y_1 \,..\, Q_{n+m} y_m \beta,$$
$$\overline{Q_1} v_1 (Q_2 v_2 \,..\, Q_n v_n \alpha_{\underline{x}}(\underline{v}) \to Q_{n+1} y_1 \,..\, Q_{n+m} y_m \beta),$$
$$\overline{Q_1} v_1 \overline{Q_2} v_2 (Q_3 v_3 \,..\, Q_n v_n \alpha_{\underline{x}}(\underline{v}) \to Q_{n+1} y_1 \,..\, Q_{n+m} y_m \beta),$$
$$\vdots$$
$$\overline{Q_1} v_1 \,..\, \overline{Q_n} v_n (\alpha_{\underline{x}}(\underline{v}) \to Q_{n+1} y_1 \,..\, Q_{n+m} y_m \beta),$$

neboť první s druhou je ekvivalentní vzhledem k 3.1.22(e), druhá s třetí díky 3.1.22(e) a 3.1.20(d), třetí se čtvrtou díky 3.1.22(e) a dvojímu užití 3.1.20(d) atd. Podobně, opakované užití tvrzení 3.1.22(d) a 3.1.20(d) dává ekvivalentní formuli

$$\overline{Q_1} v_1 \,..\, \overline{Q_n} v_n Q_{n+1} y_1 \,..\, Q_{n+m} y_m (\alpha_{\underline{x}}(\underline{v}) \to \beta),$$

která je v prenexním normálním tvaru.

Úvahy ve všech ostatních případech, kdy φ je utvořena z jednodušších formulí pomocí existenční kvantifikace nebo pomocí logické spojky jiné než implikace, jsou podobné. QED

Příklad 3.1.24 Nechť K, $<$ a R jsou jeden ternární a dva binární predikátové symboly. Formule

$$\exists x R(x, y) \;\to\; \exists z K(z, x, y) \;\&\; \neg \forall z (z < x)$$

je ekvivalentní s formulemi

$$\exists x R(x, y) \;\to\; \exists z K(z, x, y) \;\&\; \exists z \neg (z < x),$$
$$\exists x R(x, y) \;\to\; \exists z K(z, x, y) \;\&\; \exists v \neg (v < x),$$
$$\exists x R(x, y) \;\to\; \exists v \exists z (K(z, x, y) \;\&\; \neg (v < x)),$$
$$\forall u \exists v \exists z (R(u, y) \;\to\; K(z, x, y) \;\&\; \neg (v < x)),$$

z nichž poslední je v prenexním normálním tvaru.

Podíváme-li se znovu na důkaz věty 3.1.23, vidíme, že k převedení libovolné formule na ekvivalentní prenexní formuli jsme použili tvrzení (c) a (d) lemmatu 3.1.20 a lemma 3.1.22. Záměna vázané proměnné x novou proměnnou v popsaná v tvrzení 3.1.20(c) se nazývá *přejmenování vázané proměnné*. Souhrnné označení pro přejmenování vázaných proměnných a pro ekvivalence z lemmatu 3.1.22 použité zprava doleva je *prenexní operace*. Kromě prenexních operací jsme implicitně použili také tvrzení ze cvičení 14.

Před závěrečnými poznámkami tohoto oddílu o sémantice predikátové logiky zaveďme ještě konvenci týkající se vyznačování volných proměnných ve formulích a alternativního způsobu zapisování substitucí termů. Řekneme-li například „nechť $\varphi(x_1, \ldots, x_n)$ je formule“, míníme tím, že proměnné $x_1, \ldots, x_n$ jsou navzájem různé a že každá proměnná, která se ve φ vyskytuje volně, je některá z proměnných $x_1, \ldots, x_n$ (není ale nutné, aby všechny $x_1, \ldots, x_n$ skutečně měly ve φ volné výskyty). Mluvíme-li například o formuli $\varphi(t_1(x, y), t_2(x, y))$, rozumí se, že za nějaké (nedůležité nebo dříve specifikované) dvě různé volné proměnné byly do formule φ dosazeny (ne nutně různé) termy t_1 a t_2, ve kterých se nevyskytují jiné proměnné než x a y, a navíc že ve výsledné formuli se nevyskytují jiné volné výskyty proměnných x a y než ty, které se tam octly onou substitucí. Takto je třeba chápat také zápisy typu $\varphi(x, x)$, proměnná je také termem. Kdybychom chtěli připustit případ, kdy třeba proměnná x má ve formuli φ i jiné výskyty než ty, které se tam octly substitucí termů t_1 a t_2, mluvili bychom o formuli $\varphi(t_1(x, y), t_2(x, y), x)$. Řekneme-li například „uvažujme formuli tvaru $y < z \;\&\; \varphi(y, \underline{x})$“, rozumí se, že proměnné y a $x_1, \ldots, x_n$ mohou mít volné výskyty ve formuli φ, ale proměnná z je nemá.

Příklad 3.1.25 Ověřme, že je-li $\varphi(x, \underline{y})$ libovolná aritmetická formule, pak formule

$$\varphi(0, \underline{y}) \,\&\, \forall x(\varphi(x, \underline{y}) \to \varphi(\mathrm{S}(x), \underline{y})) \to \forall x \varphi(x, \underline{y}) \qquad (*)$$

platí ve struktuře $\mathbf{N}$ přirozených čísel. Především, formule $(*)$ neobsahuje jiné volné proměnné než případně $y_1, \ldots, y_n$ a žádná z těchto proměnných není x. Nechť $b_1, \ldots, b_n$ je ohodnocení proměnných $y_1, \ldots, y_n$ takové, že $\mathbf{N} \models \varphi(0, \underline{y})[\underline{b}]$ a zároveň $\mathbf{N} \models (\forall x(\varphi(x, \underline{y}) \to \varphi(\mathrm{S}(x), \underline{y})))[\underline{b}]$. Ověřme, že platí $\mathbf{N} \models (\forall x \varphi(x, \underline{y}))[\underline{b}]$. Nechť ne a nechť a_0 je nejmenší číslo a, pro které neplatí $\mathbf{N} \models \varphi[a, \underline{b}]$. Máme $\mathbf{N} \not\models \varphi[a_0, \underline{b}]$ a $\mathbf{N} \models \varphi[a, \underline{b}]$ pro každé $a < a_0$. Z podmínek $0^{\mathbf{N}} = 0$, $\mathbf{N} \models \varphi(0, \underline{y})[\underline{b}]$ a $\mathbf{N} \not\models \varphi[a_0, \underline{b}]$ plyne $a_0 \neq 0$. Protože $a_0 - 1 < a_0$, máme $\mathbf{N} \models \varphi[a_0 - 1, \underline{b}]$. Ale $\mathbf{N} \models \varphi[a_0 - 1, \underline{b}]$ a $\mathbf{N} \not\models \varphi[a_0, \underline{b}]$ je ve sporu s $\mathbf{N} \models (\forall x(\varphi(x, \underline{y}) \to \varphi(\mathrm{S}(x), \underline{y})))[\underline{b}]$.

Chceme-li ukázat, že nějaká formule φ nevyplývá z nějaké množiny předpokladů Δ, znamená to podle definice najít strukturu $\mathbf{D}$ a ohodnocení proměnných e takové, že $\mathbf{D} \models \Delta[e]$ a $\mathbf{D} \not\models \varphi[e]$. Máme tedy najít strukturu $\mathbf{D}$ a ohodnocení proměnných e, které v $\mathbf{D}$ splňuje všechny formule z množiny $\Gamma = \Delta \cup \{\neg\varphi\}$. Přitom by nás mohly napadnout následující otázky.

1. *Máme-li najít strukturu $\mathbf{D}$ splňující nějakou množinu formulí Γ, je někdy nutné volit strukturu $\mathbf{D}$ nekonečnou?*

2. *Je někdy nutné volit strukturu* $\mathbf{D}$ *dokonce nespočetnou?*
3. *Když* $\mathbf{D}_1$ *a* $\mathbf{D}_2$ *jsou různé struktury pro nějaký jazyk* L*, znamená to, že v* $\mathbf{D}_1$ *platí nějaká sentence, která v* $\mathbf{D}_2$ *neplatí?*
4. *Je možné, aby všechny sentence platné v nějaké struktuře byly důsledkem nějaké přehledné množiny předpokladů?*

První otázka je uvedena jen pro úplnost. Víme už totiž, že odpověď je ano: množina Δ z příkladu 3.1.19(f) je splněna například ve struktuře $\langle \mathrm{N}, 0, \mathrm{s}\rangle$, není ale splněna v žádné konečné struktuře. Chceme-li ukázat, že formule $\neg\forall x(\mathrm{S}(x) \neq 0)$ nevyplývá z formule $\forall x\forall y(\mathrm{S}(x) = \mathrm{S}(y) \to x = y)$, musíme použít nekonečnou strukturu.

Ke třetí otázce poznamenejme toto. Snadno lze dokázat (a plyne to také z lemmatu 3.2.11), že jsou-li $\mathbf{D}_1$ a $\mathbf{D}_2$ dvě izomorfní struktury pro nějaký jazyk, pak v $\mathbf{D}_1$ a v $\mathbf{D}_2$ platí tytéž sentence. Slovo „různé“ tedy čtěme „neizomorfní“. Úvahou o mohutnostech lze zdůvodnit, že i v tomto případě je obecná odpověď na třetí otázku záporná. Množin sentencí v jazyce L je totiž jen omezeně mnoho (je-li například jazyk L nejvýše spočetný, pak množina všech sentencí je nekonečná spočetná a množina všech množin sentencí má mohutnost $2^{\aleph_0}$), ale neizomorfních struktur pro jazyk L je ve smyslu mohutností neomezeně mnoho, protože struktury mohou mít libovolně velkou mohutnost. To ale stále není vyčerpávající odpověď na třetí otázku. Můžeme totiž tuto otázku klást pro konkrétní dvojici struktur. Lze například strukturu $\langle \mathrm{R}, <\rangle$ všech reálných čísel s uspořádáním a strukturu $\langle \mathrm{Q}, <\rangle$ všech racionálních čísel s uspořádáním odlišit platností nějaké sentence v jazyce $\{<\}$?

Ve čtvrté otázce může slovo „přehledná“ nejspíš znamenat „konečná“ nebo „rekurzívní“.

Úvahy o kalkulech, úplnosti a kompaktnosti v následujících oddílech vrhnou určité světlo na všechny otázky 2–4.

Všimněme si ještě, že definice logicky platné formule v predikátové logice se podobá definici tautologie ve výrokové logice. Tam, kde jsme ve výrokové logice volili pravdivostní hodnoty atomů, abychom ukázali, že nějaká formule není tautologie, v predikátové logice volíme strukturu a ohodnocení proměnných. Podstatný rozdíl je ale v tom, že sémantika predikátové logiky nenaznačuje žádný algoritmus, který by zjistil, zda daná formule je logicky platnou formulí. A na této situaci by se nic nezměnilo dokonce ani v hypotetickém případě, kdy odpověď na první otázku by byla ne: i konečných neizomorfních struktur pro daný jazyk je nekonečně mnoho.

Cvičení

Ve všech cvičeních, v nichž se vyskytuje rovnítko, předpokládejte, že pracujete v predikátové logice s rovností.

1. Určete, které z následujících formulí platí ve struktuře $\mathbf{B}$ z obrázku 3.1.1:

   $\exists x\forall v(v \notin x)$, $\qquad$ $\exists x\forall v(v \in x \equiv v \in v)$,

   $\exists x\forall v(v \in x)$, $\qquad$ $\forall x\forall y\exists z\forall v(v \in z \equiv v = x \vee v = y)$,

$\exists x \forall v (v \in x \equiv v \notin v)$, $\exists x \exists y (x \in y \ \& \ y \in x)$.

2. Nechť P a Q jsou unární a R binární predikát. Dokažte, že následující formule jsou logicky platné, ale obrátíme-li (vnější) implikaci, ve všech případech vznikne formule, která není logicky platná:
$\exists x(P(x) \,\&\, Q(x)) \to \exists x P(x) \,\&\, \exists x Q(x)$,
$\forall x P(x) \vee \forall x Q(x) \to \forall x(P(x) \vee Q(x))$,
$\exists x \forall y R(x,y) \to \forall y \exists x R(x,y)$,
$\forall x(P(x) \to Q(x)) \to (\forall x P(x) \to \forall x Q(x))$,
$\forall x(P(x) \to Q(x)) \to (\exists x P(x) \to \exists x Q(x))$.

3. (a) Najděte sentenci v jazyce $\{+, \cdot, 0, 1\}$, která platí jen v jedné ze struktur $\mathbf{R}$ a $\mathbf{Q}$.
(b) Pro každou ze tří struktur $\langle \mathrm{N}, < \rangle$, $\langle \mathrm{Z}, < \rangle$ a $\langle \mathrm{Q}, < \rangle$ najděte sentenci v jazyce $\{<\}$, která v ní platí a ve zbývajících dvou neplatí.
(c) Zdůvodněte, že také struktury $\langle \mathrm{Z}, + \rangle$ a $\langle \mathrm{Q}, + \rangle$ lze odlišit platností nějaké sentence. Lze i struktury $\langle \mathrm{R}, +, \cdot \rangle$ a $\langle \mathrm{Q}, +, \cdot \rangle$ odlišit platností nějaké sentence?

4. Nechť φ je formule, která nemá volné výskyty proměnné x (může ale mít volné výskyty proměnné v). Rozhodněte, zda každá formule tvaru

$$\exists v \varphi \ \& \ \exists x \forall v (x < v \to \neg \varphi) \to \\ \to \exists x (\forall v (x < v \to \neg \varphi) \ \& \ \forall y (y < x \to \exists v (y < v \ \& \ \varphi)))$$

platí ve struktuře $\mathbf{R}$. Řešte analogickou úlohu také pro struktury $\mathbf{Q}$ a $\mathbf{N}$.

5. Dokažte, že předpoklad v lemmatu 3.1.17(b), že φ je sentence, je podstatný, tj. nalezněte formuli φ a strukturu $\mathbf{D}$ takové, že $\mathbf{D} \not\models \varphi$ a $\mathbf{D} \not\models \neg\varphi$.

6. Určete, pro které trojice přirozených čísel n, m a k platí sentence $\overline{n} + \overline{m} = \overline{k}$ ve struktuře $\mathbf{A}$ z obrázku 3.1.1. Totéž udělejte pro strukturu $\mathbf{N}$.

7. Dokažte podrobně, že predikátová formule ψ je důsledkem formule φ, právě když $\varphi \to \psi$ je logicky platná formule.

8. Nechť φ a ψ jsou formule v jazyce L a nechť pro každou strukturu $\mathbf{D}$ pro jazyk L platí $\mathbf{D} \models \varphi$, právě když $\mathbf{D} \models \psi$. Musí být formule φ a ψ ekvivalentní?
Návod. Viz příklad 3.1.19(d).

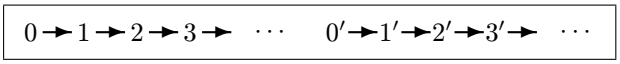
9. Najděte příklad množiny formulí Δ a formule φ takové, že $\Delta \models \varphi$ a $\Delta \models \neg\varphi$.

10. Která z formulí

$$\forall x(x = 0 \ \vee \ \exists y(\mathrm{S}(y) = x)), \qquad \forall x(\mathrm{S}(x) \neq x), \qquad \forall x \exists y(\mathrm{S}(x) \neq y)$$

vyplývá z množiny Δ z příkladu 3.1.19(f)? Které z formulí tvaru $\overline{n} = \overline{m}$ vyplývají z Δ?

Návod. Uvažujte například strukturu



,

která obsahuje dvě kopie množiny všech přirozených čísel (s následnickou funkcí vyznačenou šipkami) a kterou bychom mohli označit $\langle \mathrm{N}, 0, \mathrm{s}\rangle + \langle \mathrm{N}, \mathrm{s}\rangle$.

11. Dokažte, že každá z následujících formulí je logicky platná:

$\forall x \forall y \varphi \equiv \forall y \forall x \varphi$, $\quad \exists x \exists y \varphi \equiv \exists y \exists x \varphi$,
$\forall x \forall y \varphi \to \forall x \varphi_y(x)$, $\quad \exists x \varphi_y(x) \to \exists x \exists y \varphi$,
$\forall x \varphi \,\&\, \forall x \psi \equiv \forall x(\varphi \,\&\, \psi)$, $\quad \exists x \varphi \vee \exists x \psi \equiv \exists x(\varphi \vee \psi)$,
$\exists x \forall y \varphi \to \forall y \exists x \varphi$, $\quad \forall x \varphi \to \exists x \psi \equiv \exists x(\varphi \to \psi)$,
$\exists x(\varphi \to \forall y \varphi_x(y))$, $\quad \forall x \varphi \to \exists x \varphi$.

12. Užijte lemma 3.1.20 k důkazu, že nemá-li x volné výskyty ve formuli φ, pak formule φ, $\forall x \varphi$ a $\exists x \varphi$ jsou spolu ekvivalentní.

13. Určete, ve kterých případech je v lemmatu 3.1.22 podstatný předpoklad, že x se nevyskytuje volně ve formuli χ.

14. Nahradíme-li ve formuli φ libovolnou podformuli formulí s ní ekvivalentní, pak je výsledná formule ekvivalentní s φ. Dokažte.

15. Rozhodněte, zda platí: každá formule tvaru $(\varphi \equiv \psi) \to (\forall x \varphi \equiv \forall x \psi)$ je logicky platná formule.

16. Převeďte následující formule na prenexní normální tvar:

$\forall x(P(x) \to \forall y(Q(x,y) \to \neg \forall z R(y,z)))$,
$\exists x A(x,y) \to (B(x) \to \neg \exists u A(x,u))$,
$P(x,y) \to \exists y(Q(y) \to (\exists x Q(x) \to R(y)))$.

17. Dokažte, že každá predikátová formule délky n je ekvivalentní s jistou formulí v prenexním tvaru, jejíž délka je $\mathcal{O}(n \cdot \log n)$, zapisujeme-li indexy u proměnných binárně, a $\mathcal{O}(n^2)$, zapisujeme-li je unárně.

18. Nechť L_1 a L_2 jsou jazyky takové, že $L_1 \subseteq L_2$, nechť $\mathbf{D}_1$ je struktura pro L_1 a nechť $\mathbf{D}_2$ je struktura pro L_2, která má tutéž nosnou množinu jako $\mathbf{D}_1$ a v níž každý symbol z L_1 má tutéž realizaci jako v $\mathbf{D}_1$. Dokažte, že je-li φ formule v L_1, pak φ platí v $\mathbf{D}_1$, právě když φ platí v $\mathbf{D}_2$.

19. Nechť φ je formule v jazyce L_2 a nechť $L_1 \subseteq L_2$ je seznam všech mimologických symbolů vyskytujících se ve φ. Pak φ platí v každé struktuře pro L_1, právě když φ platí v každé struktuře pro L_2. Dokažte.

20. Struktura $\mathbf{D}_1$ je *podstruktura* struktury $\mathbf{D}_2$, jestliže platí inkluze $D_1 \subseteq D_2$ pro jejich nosné množiny a jestliže realizace $I_1^{\mathbf{D}}$ libovolného symbolu I jejich jazyka je restrikcí jeho realizace $I^{\mathbf{D}_2}$ na množinu D_1. Podstruktury struktury $\mathbf{D}_2$ lze ztotožnit s neprázdnými podmnožinami D_1 množiny D_2, které jsou uzavřeny na všechny operace (tj. pro které platí $F^{\mathbf{D}_2}(a_1, .., a_n) \in D_1$, kdykoliv F je n-ární funkční symbol a $a_1, .., a_n$ jsou prvky množiny D_1). Je-li struktura $\mathbf{D}_1$ podstrukturou struktury $\mathbf{D_2}$, říkáme také, že struktura $\mathbf{D}_2$ je *rozšíření* struktury $\mathbf{D}_1$. Nechť $\mathbf{D_1}$ je podstruktura struktury $\mathbf{D}_2$. Dokažte, že platí
(a) $\mathbf{D}_1 \models \varphi[e] \Leftrightarrow \mathbf{D}_2 \models \varphi[e]$, kdykoliv je φ otevřená formule a e ohodnocení proměnných, jehož všechny hodnoty jsou v D_1.
(b) $\mathbf{D}_1 \models \varphi \Rightarrow \mathbf{D}_2 \models \varphi$, kdykoliv je φ existenční sentence.
(c) $\mathbf{D}_2 \models \varphi \Rightarrow \mathbf{D}_1 \models \varphi$, kdykoliv je φ univerzální formule.
Najděte příklady na to, že tvrzení (a)–(c) nelze zesílit: (a) neplatí pro existenční ani univerzální sentence, implikace v (b) ani v (c) nelze obrátit a (b) neplatí pro existenční formule.

21. Použijte předchozí cvičení k důkazu, že formule $\forall x \exists y(x < y)$ není ekvivalentní s žádnou existenční ani s žádnou univerzální formulí.

22. Rozhodněte, zda platí toto tvrzení: je-li φ otevřená formule jazyka L a formule $\exists y \varphi$ je logicky platná, pak existuje term t jazyka L takový, že $\varphi_y(t)$ je logicky platná.

    Návod. Uvažujte jazyk $\{P, F\}$ a formuli $\exists y(P(F(y)) \vee \neg P(y))$.

23. Rozhodněte, zda platí toto tvrzení: je-li φ formule jazyka L a formule $\exists y \varphi$ je logicky platná, pak existují termy $t_1, .., t_n$ jazyka L takové, že také formule $\varphi_y(t_1) \vee .. \vee \varphi_y(t_n)$ je logicky platná.

    Návod. Uvažujte formuli $\exists y(P(y) \to \forall v P(v))$.

24. Najděte formuli φ takovou, že formule $\varphi_v(0) \& \forall x(\varphi_v(x) \to \varphi_v(\mathrm{S}(x))) \to \forall x \varphi_v(x)$ neplatí v $\mathbf{N}$.

    Návod. Při tomto způsobu zápisu není vyloučeno, že například formule $\varphi_v(0)$ obsahuje volné výskyty proměnné x.

25. Přepište formuli z cvičení 4 v duchu úmluvy o vyznačování volných proměnných, kterou jsme učinili před příkladem 3.1.25.

3.2 Hilbertovský predikátový kalkulus

3.2.1 Korektnost a úplnost

Důkaz a *dokazatelnost* se v predikátové logice definují stejně jako ve výrokové logice: posloupnost formulí je důkaz z množiny předpokladů Δ, jestliže každý člen

je prvkem množiny Δ, nebo je logickým axiomem kalkulu pro predikátovou logiku, nebo je odvozen z předchozích členů pomocí některého odvozovacího pravidla příslušného kalkulu. *Hilbertovský kalkulus* pro predikátovou logiku získáme tak, že k výrokovému kalkulu z oddílu 1.3 přidáme dvě axiomatická schémata a dvě pravidla týkající se kvantifikátorů:

B1: $\forall x\varphi \to \varphi_x(t)$,

B2: $\varphi_x(t) \to \exists x\varphi$,

Gen-A: $\psi \to \varphi \;/\; \psi \to \forall x\varphi$,

Gen-E: $\varphi \to \psi \;/\; \exists x\varphi \to \psi$,

kde v případě axiomů B1 a B2 je φ formule, ve které je term t substituovatelný za proměnnou x, a v případě pravidel Gen-A a Gen-E je ψ formule, která neobsahuje volné výskyty proměnné x. Výsledný kalkulus označme HK stejně jako ve výrokové logice. *Kalkulus HK* (přesněji řečeno predikátová verze hilbertovského kalkulu HK) má tedy axiomatická schémata A1–A7, B1 a B2 a tři odvozovací pravidla MP, Gen-A a Gen-E. Pravidlům Gen-A a Gen-E říkáme *pravidla generalizace* a axiomům B1 a B2 *axiomy specifikace*.

Ukažme si dva příklady důkazů v kalkulu HK. Nechť R je binární predikátový symbol. Formule

$$\forall x\forall y(R(x,y) \to \neg R(y,x)) \to \forall y(R(y,y) \to \neg R(y,y))$$

je logicky platná, téměř má tvar požadovaný ve schématu B1, *není* ale logickým axiomem, protože ve formuli $\forall y(R(x,y) \to \neg R(y,x))$ není proměnná y substituovatelná za x. Zato formule v následujících dvou řádcích

1: $\vdash \forall x\forall y(R(x,y) \to \neg R(y,x)) \to \forall y(R(x,y) \to \neg R(y,x))$

2: $\vdash \forall y(R(x,y) \to \neg R(y,x)) \to (R(x,x) \to \neg R(x,x))$

mají požadovaný tvar, a můžeme o nich tedy tvrdit, že jsou instancemi schématu B1, a tudíž dokazatelnými formulemi.

I v predikátové logice můžeme v dobrém smyslu mluvit o tautologiích. Predikátová formule v jazyce L je tautologií, jestliže ji lze získat z nějaké výrokové tautologie A substitucí predikátových formulí za atomy, tj. nahrazením všech atomů formule A predikátovými formulemi v jazyce L, přičemž všechny výskyty téhož atomu jsou nahrazeny vždy toutéž predikátovou formulí. Formule $R(x,y) \vee \neg R(x,y)$ je příklad predikátové formule, která je tautologií. Formule $\forall x\forall y R(x,y) \to \forall y\forall x R(x,y)$ je logicky platná formule, ale není to tautologie. Z hlediska výrokové logiky je to formule tvaru $p \to q$ sestavená ze dvou různých „atomů“.

Protože jsme do kalkulu HK přijali všechny axiomy a pravidla jeho výrokové varianty, tj. axiomy A1–A7 a pravidlo MP, je jasné, že substitucí predikátových formulí za atomy v libovolném výrokovém důkazu vznikne důkaz v predikátové

variantě kalkulu HK. Protože axiomy A1–A7 a pravidlo MP dohromady tvoří kalkulus úplný vůči sémantice klasické výrokové logiky, je dále jasné, že každá predikátová formule, která je tautologií, je v predikátové variantě kalkulu HK dokazatelná. Označme A formuli $\forall x \forall y(R(x,y) \to \neg R(y,x))$ a označme B formuli $\forall y(R(x,y) \to \neg R(y,x))$. Platí

3: $\vdash (A \to B) \to ((B \to (R(x,x) \to \neg R(x,x))) \to (A \to \neg R(x,x)))$.

Snadno lze totiž ověřit, že tato dlouhá formule je opravdu tautologií. Dále

4: $\vdash (B \to (R(x,x) \to \neg R(x,x))) \to (A \to \neg R(x,x))$; MP na 1, 3

5: $\vdash \forall x \forall y(R(x,y) \to \neg R(y,x)) \to \neg R(x,x)$; MP na 2, 4

6: $\vdash \forall x \forall y(R(x,y) \to \neg R(y,x)) \to \forall x \neg R(x,x)$; Gen-A na 5.

Přesvědčili jsme se, že tvrzení je-li relace R antisymetrická, pak je i antireflexivní je v kalkulu HK dokazatelné. Domluvme se, že kdybychom to měli zdůvodnit podruhé, vynechali bychom body (3) a (4) a místo toho bychom řekli, že formule (5) je *tautologickým důsledkem* formulí (1) a (2).

Nyní uvažujme unární predikát P a sentenci $\exists z(P(z) \to \forall x P(x))$. Napišme si nejprve neformální důkaz této sentence:

> Když $\neg \forall x P(x)$, vezměme za z některý z objektů, které nesplňují P. Takový objekt z splňuje každou implikaci tvaru $P(z) \to (..)$. Když naopak $\forall x P(x)$, je implikace $P(z) \to \forall x P(x)$ splněna bez ohledu na z, a za z lze tedy vzít libovolný objekt.

Použijeme-li úmluvu o vynechávání výrokových kroků, formalizací právě uvedeného neformálního důkazu můžeme získat například takovýto důkaz v kalkulu HK:

1: $(P(x) \to \forall x P(x)) \to \exists z(P(z) \to \forall x P(x))$; B2

2: $\neg \exists z(P(z) \to \forall x P(x)) \to P(x)$; Taut. důsledek formule 1

3: $\neg \exists z(P(z) \to \forall x P(x)) \to \forall x P(x)$; Gen-A na 2

4: $\neg \forall x P(x) \to \exists z(P(z) \to \forall x P(x))$; Taut. důsledek formule 3

5: $\forall x P(x) \to (P(x) \to \forall x P(x))$; Tautologie

6: $\forall x P(x) \to \exists z(P(z) \to \forall x P(x))$; Taut. důsledek formulí 1, 5

7: $\exists z(P(z) \to \forall x P(x))$; Taut. důsledek formulí 4, 6.

Všimněme si, že důkaz by bylo možno ještě zkrátit vynecháním kroků (4)–(6): formule (7) je tautologickým důsledkem formulí (1) a (3).

Lemma 3.2.1 *Nechť φ je formule neobsahující volné výskyty proměnné z. Pak formule $\exists z(\varphi_x(z) \to \forall x \varphi)$ a $\exists z(\exists x \varphi \to \varphi_x(z))$ jsou dokazatelné v HK.*

Důkaz Formule $(\varphi_x(z) \to \forall x\varphi)_z(x)$ a $\varphi \to \forall x\varphi$ jsou totožné, neboť z se nevyskytuje volně ve φ. To znamená, že nahradíme-li v řádku (1) před okamžikem sestrojeného formálního důkazu formuli $P(x)$ formulí φ a formuli $P(z)$ formulí $\varphi_x(z)$, dostaneme opět instanci axiomu B2. Provedeme-li tytéž záměny i v ostatních řádcích, dostaneme důkaz formule $\exists z(\varphi_x(z) \to \forall x\varphi)$. Přitom použití pravidla Gen-A v řádku (3) je oprávněné, neboť formule $\varphi_x(z) \to \forall x\varphi$ nemá volné výskyty proměnné x. Zdůvodnění dokazatelnosti formule $\exists z(\exists x\varphi \to \varphi_x(z))$ je podobné a ponecháváme je za cvičení. QED

Lemma 3.2.2 (věta o dedukci) *Nechť ψ je sentence a nechť $\Delta, \psi \vdash \varphi$. Pak $\Delta \vdash \psi \to \varphi$.*

Důkaz Nechť $\varphi_1, \ldots, \varphi_n (= \varphi)$ je důkaz formule φ z předpokladů Δ, ψ. Tvrdíme, že všechny implikace $\psi \to \varphi_i$ jsou dokazatelné z Δ. Věnujme se třeba případu, kdy φ_i je odvozena z některého předchozího členu pomocí pravidla Gen-E. Případ, kdy φ_i je odvozena pomocí pravidla Gen-A, je podobný a všechny ostatní případy jsou úplně stejné jako ve výrokové logice.

Je-li φ_i odvozena pravidlem Gen-E z φ_j, kde $j < i$, znamená to, že formule φ_i má tvar $\exists x\alpha \to \beta$, formule φ_j má tvar $\alpha \to \beta$ a proměnná x nemá volné výskyty v β. Indukční předpoklad říká

1: $\quad \Delta \vdash \psi \to (\alpha \to \beta)$.

Z toho snadno zdůvodníme dokazatelnost formule $\psi \to (\exists x\alpha \to \beta)$:

2: $\quad \Delta \vdash \alpha \to (\psi \to \beta)$; Taut. důsledek formule 1

3: $\quad \Delta \vdash \exists x\alpha \to (\psi \to \beta)$; Gen-E

4: $\quad \Delta \vdash \psi \to (\exists x\alpha \to \beta)$; Taut. důsledek formule 3.

Přitom v kroku (3) jsme opravdu použili předpoklad, že ψ je sentence. QED

Věta 3.2.3 (o silné korektnosti kalkulu HK) *Nechť φ je formule a nechť Δ je množina formulí v jazyce L. Když $\Delta \vdash \varphi$, pak φ platí v každé struktuře pro L, ve které platí všechny formule z Δ.*

Důkaz Nechť struktura $\mathbf{D}$ pro jazyk L je dána. Nechť e je ohodnocení proměnných ve struktuře $\mathbf{D}$. Z podmínky T4 (viz 3.1.9) plyne, že když $\mathbf{D} \models (\psi \to \chi)[e]$ a $\mathbf{D} \models \psi[e]$, pak také $\mathbf{D} \models \chi[e]$. Tím je ověřeno, že množina všech formulí, které jsou v $\mathbf{D}$ splněny *daným* ohodnocením e, je uzavřena na pravidlo MP. Podobně lze ověřit, že množina všech formulí splněných v $\mathbf{D}$ *daným* ohodnocením obsahuje všechny výrokové axiomy tvaru A1–A7. Lemma 3.1.20(a) říká, že obsahuje také všechny axiomy specifikace tvaru B1 nebo B2.

Když daným, pak také každým. Množina všech formulí splněných v $\mathbf{D}$ *každým* ohodnocením e, tj. platných v $\mathbf{D}$, obsahuje všechny formule z množiny Δ, všechny axiomy tvaru A1–A7, B1 a B2 a je uzavřena na pravidlo MP.

O pravidlech Gen-A a Gen-E lze říci pouze „každým“, ale to nám stačí a je to přesně to, co jsme dokázali v 3.1.20(b): množina všech formulí platných v $\mathbf{D}$, tj. splněných v $\mathbf{D}$ *každým* ohodnocením, je uzavřena na obě pravidla Gen-A i Gen-E.

Je-li $\varphi_1, .., \varphi_n (= \varphi)$ důkaz formule φ z množiny předpokladů Δ, předchozí úvahy a indukce podle i dávají, že každá formule φ_i platí v $\mathbf{D}$. Tedy $\mathbf{D} \models \varphi$. QED

Napišme si ještě jednou symbolicky podmínku, o které jsme v důkazu věty o silné korektnosti dokázali, že platí pro každou formuli φ dokazatelnou z množiny Δ:

$$\forall \mathbf{D}(\forall e \forall \psi \in \Delta(\mathbf{D} \models \psi[e]) \Rightarrow \forall e(\mathbf{D} \models \varphi[e])), \qquad (*)$$

a porovnejme ji s podmínkou z definice 3.1.18 vyjadřující, že φ vyplývá z Δ:

$$\forall \mathbf{D} \forall e(\forall \psi \in \Delta(\mathbf{D} \models \psi[e]) \Rightarrow \mathbf{D} \models \varphi[e]). \qquad (**)$$

Není pravda, že podmínky $(*)$ a $(**)$ jsou ekvivalentní, protipříklad je zřejmý třeba z příkladu 3.1.19(d). Podmínky $(*)$ a $(**)$ jsou ale ekvivalentní v případě, kdy všechny formule v Δ jsou uzavřené. To opravňuje následující definici a umožňuje přehlednější reformulaci věty o korektnosti, která užívá pojem důsledku a kterou vyslovíme v 3.2.8(b). Po formulaci věty 3.2.8 se pro jistotu o ekvivalenci podmínek $(*)$ a $(**)$ ještě jednou zmíníme.

Definice 3.2.4 (Axiomatická) teorie *je dvojice $\langle L, T\rangle$, kde L je jazyk a T je množina sentencí v L. Prvkům množiny T říkáme* (vlastní) axiomy *teorie $\langle L, T\rangle$. Struktura $\mathbf{D}$ pro jazyk L je* model teorie $\langle L, T\rangle$*, jestliže v $\mathbf{D}$ platí všechny prvky množiny T. Formule φ v jazyce L je* dokazatelná v (teorii) $\langle L, T\rangle$*, jestliže φ je dokazatelná z předpokladů T. Formule φ je* vyvratitelná v $\langle L, T\rangle$*, jestliže $\neg\varphi$ je dokazatelná v T. Formule φ je* nezávislá na $\langle L, T\rangle$*, jestliže φ není v $\langle L, T\rangle$ dokazatelná ani vyvratitelná.*

Příklad 3.2.5 *Teorie (ostrého) uspořádání* má jazyk $L = \{<\}$ s jedním binárním predikátem a množinu axiomů

$$T = \{\, \forall x \forall y \forall z(x < y \ \&\ y < z \rightarrow x < z), \forall x \forall y(x < y \rightarrow \neg(y < x)) \,\},$$

které postulují, že uspořádání $<$ je tranzitivní a antisymetrické. Na začátku tohoto oddílu jsme vlastně sestrojili důkaz sentence $\forall x \neg(x < x)$ z předpokladů T. Nevadí, že tranzitivitu jsme přitom nepotřebovali. To znamená, že sentence $\neg\forall x \neg(x < x)$ je v teorii $\langle L, T\rangle$ vyvratitelná a sentence $\forall x \neg(x < x)$ je v ní dokazatelná. Modelem teorie $\langle L, T\rangle$ je každá struktura $\langle D, R\rangle$, kde $D \neq \emptyset$ a $R \subseteq D^2$ je ostré uspořádání na množině D. Mezi modely teorie $\langle L, T\rangle$ jsou jak struktury $\langle D, R\rangle$, ve kterých platí sentence $\forall x \exists y(x < y)$, tak struktury, ve kterých platí její negace. Z věty 3.2.3 plyne, že $\forall x \exists y(x < y)$ je sentence nezávislá na teorii $\langle L, T\rangle$.

Je zřejmé, že daná teorie může mít více modelů a že daná struktura může být modelem více teorií.

V dalším výkladu budeme často místo $\langle L, T\rangle$ psát jen T, jako kdyby na volbě jazyka nezáleželo. A ono opravdu moc nezáleží, neboť z cvičení 19 předchozího oddílu je zřejmé, že symboly, které se nevyskytují ve formulích, neovlivňují logickou platnost ani vztah důsledku. Dále se domluvme, že kdybychom někdy nedodrželi požadavek definice 3.2.4 a řekli třeba, že axiom je $x+y = y+x$, myslíme to tak, že axiom je formule $\forall x\forall y(x+y = y+x)$. Za skutečný axiom považujeme *univerzální uzávěr* dané formule.

Zápis T, φ označuje jako obvykle množinu $T \cup \{\varphi\}$. Místo T, φ budeme také psát $(T + \varphi)$ a mluvit o *rozšíření* teorie T *o axiom* φ.

Všimněme si ještě, že o axiomech teorie T mluvíme jako o *vlastních* axiomech teorie, abychom je odlišili od *logických* axiomů daných volbou kalkulu. Ve formálním důkazu $\varphi_1, \ldots, \varphi_n$ z předpokladů T se mohou vyskytnout jak vlastní axiomy, tj. prvky množiny T, tak logické axiomy, v našem případě tvaru A1–A7, B1, B2. Volba logických axiomů je oprávněna tím, že pro příslušný kalkulus jsme schopni dokázat věty o korektnosti a úplnosti.

Definice 3.2.6 *Řekneme, že teorie T je* sporná, *jestliže existuje formule φ taková, že $T \vdash \varphi$ a $T \vdash \neg\varphi$. V opačném případě je T* bezesporná (konzistentní).

Lemma 3.2.7 *(a) Když $T \vdash \varphi$, pak φ platí v každém modelu teorie T.*
(b) Je-li teorie T sporná, pak T nemá žádný model.
(c) Teorie T je sporná, právě když každá formule ψ je v T dokazatelná.
(d) Je-li φ sentence, pak $T \vdash \varphi$, právě když $(T + \neg\varphi)$ je sporná.

Důkaz (a) plyne bezprostředně z věty 3.2.3.

(b) Nechť T je sporná, φ je formule současně dokazatelná i vyvratitelná v T a nechť $\mathbf{M}$ je model teorie T. Z tvrzení (a) plyne $\mathbf{M} \models \varphi$ a $\mathbf{M} \models \neg\varphi$. To je spor s 3.1.17(a).

(c) Jsou-li v teorii T dokazatelné všechny formule, pak je jistě mezi nimi i nějaká dvojice φ, $\neg\varphi$. Nechť naopak každá z formulí φ i $\neg\varphi$ je dokazatelná v T. Protože formule $\varphi \to (\neg\varphi \to \psi)$ je tautologie bez ohledu na formuli ψ, je dokazatelná v T. Dvojí užití pravidla MP dává $T \vdash \psi$.

(d) Nechť teorie $(T+\neg\varphi)$ je sporná. Z již dokázaného tvrzení (c) plyne $(T+\neg\varphi) \vdash \varphi$. Lemma 3.2.2 dává $T \vdash \neg\varphi \to \varphi$. Z toho plyne $T \vdash \varphi$, protože formule $(\neg\varphi \to \varphi) \to \varphi$ je tautologie, a je tedy dokazatelná v T. QED

Nechť T je teorie s jazykem L. Pro použití hlavně v následujících oddílech definujme $\mathrm{Thm}(T)$ jako množinu všech sentencí jazyka L dokazatelných v T a definujme $\mathrm{Ref}(T)$ jako množinu všech sentencí jazyka L vyvratitelných v T. Je zřejmé, že teorie T je bezesporná, právě když platí $\mathrm{Thm}(T) \cap \mathrm{Ref}(T) = \emptyset$. Dále z tvrzení 3.2.7(c) plyne, že je-li T sporná, pak $\mathrm{Thm}(T) = \mathrm{Ref}(T) = \mathrm{Sent}(L)$, kde $\mathrm{Sent}(L)$ je množina všech sentencí v L.

Věta 3.2.8 (o silné úplnosti kalkulu HK) *(a) Je-li T libovolná teorie, pak T má model, právě když T je bezesporná.*
(b) Je-li T teorie a φ formule, pak $T \vdash \varphi$, právě když $T \models \varphi$.

Větu o silné úplnosti dokázal Gödel v roce 1930. Stejně jako ve výrokové logice jsou obě implikace $\Rightarrow$ označovány (také, vedle tvrzení 3.2.3) jako věta o silné korektnosti (predikátové verze) kalkulu HK. Větou o korektnosti a větou o úplnosti (bez přívlastku) se i v predikátové logice myslí tvrzení, které bychom z věty o silné korektnosti resp. z věty o silné úplnosti dostali volbou $T := \emptyset$.

Než přistoupíme k důkazu obtížnější části věty o úplnosti, uvědomme si, že některé implikace jsou lehké. Předpokládejme $T \vdash \varphi$. Nechť $\mathbf{D}$ je struktura a e ohodnocení proměnných takové, že $\mathbf{D} \models T[e]$. Každá $\psi \in T$ je tedy sentence splněná v $\mathbf{D}$ naším ohodnocením e. Lemma 3.1.11 říká, že v tom případě je ψ splněna každým ohodnocením, neboli platí $\mathbf{D} \models \psi$. Z tvrzení 3.2.7(a) nebo z věty 3.2.3 plyne okamžitě $\mathbf{D} \models \varphi$, tedy $\mathbf{D} \models \varphi[e]$. Tím jsme ověřili implikaci $\Rightarrow$ v 3.2.8(b) a zároveň jsme podrobně dokázali, že podmínky $(*)$ a $(**)$, které jsme uvažovali na str. 160 před definicí axiomatické teorie, jsou v případě, kdy všechny předpoklady jsou sentence, spolu ekvivalentní.

Další úvahy o vztazích mezi podmínkami věty 3.2.8 jsou podobné jako ve výrokové logice. Implikaci $\Rightarrow$ v (a) jsme již zdůvodnili v 3.2.7(b). A nemá-li teorie T model, pak z T vyplývá každá formule ψ, a platí-li k tomu (b), T musí být sporná. To znamená, že implikace $\Leftarrow$ v (a) plyne z implikace $\Leftarrow$ v (b).

Důkaz věty 3.2.8 bude dokončen, dokážeme-li implikaci $\Leftarrow$ v (b). Budeme postupovat zhruba podle Barwisova Úvodu [5] k příručce [4] a dá nám to trochu práce. Použijeme pomocný pojem henkinovského rozšíření teorie, větu o kompaktnosti pro výrokovou logiku a (opět) také fakt, že každá tautologie je v HK dokazatelná, tedy větu o úplnosti výrokové varianty kalkulu HK.

Nechť T je teorie v jazyce L. Jazyk L může mít libovolnou mohutnost. Nejprve ve spočetně mnoha krocích sestrojíme rozšíření L^+ jazyka L. V kroku 0 vezměme všechny sentence tvaru $\forall x\psi$ nebo $\exists x\psi$, tj. všechny sentence v L začínající kvantifikátorem, a každé z nich přidělme konstantu $c_{\forall x\psi}$ nebo $c_{\exists x\psi}$ tak, aby všechny takto přidělené konstanty byly navzájem různé a různé od všech konstant jazyka L. Konstantám přiděleným v kroku 0 říkejme *henkinovské konstanty řádu* 0. V každém dalším kroku $m+1$ přidělme henkinovské konstanty řádu $m+1$ všem těm sentencím začínajícím kvantifikátorem, které jsou sestaveny ze symbolů jazyka L a henkinovských konstant řádu $0, \ldots, m$ a kterým dosud henkinovská konstanta nebyla přidělena, tj. které obsahují alespoň jednu henkinovskou konstantu řádu m.

Označme L^+ výsledný jazyk vzniklý přidáním henkinovských konstant všech řádů $m \in \mathrm{N}$ k jazyku L. Každá sentence jazyka L^+ tvaru $\forall x\psi$ nebo $\exists x\psi$ má v L^+ „svou“ konstantu $c_{\forall x\psi}$ resp. $c_{\exists x\psi}$.

Henkinovské axiomy jsou všechny sentence jazyka L^+ tvaru $\exists x\psi \to \psi_x(c_{\exists x\psi})$ a $\psi_x(c_{\forall x\psi}) \to \forall x\psi$, kde $\exists x\psi$ resp. $\forall x\psi$ je sentence v L^+. Označme $\mathrm{H}(L)$ množinu všech sentencí, které jsou henkinovským axiomem, nebo mají tvar $\forall x\psi \to \psi_x(t)$ či $\psi_x(t) \to \exists x\psi$, kde $\forall x\psi$ resp. $\exists x\psi$ je sentence jazyka L^+ a t je uzavřený term jazyka L^+. Každá henkinovská konstanta má tedy v množině $\mathrm{H}(L)$ „svůj“ henkinovský axiom a v $\mathrm{H}(L)$ jsou dále všechny axiomy specifikace tvaru B1 či B2, pokud jsou sentencemi jazyka L^+. Henkinovský axiom $\psi_x(c_{\forall x\psi}) \to \forall x\psi$ příslušný ke konstantě $c_{\forall x\psi}$ řádu m může obsahovat konstanty řádu nižšího než m, ale neobsahuje

jinou konstantu řádu m než $c_{\forall x\psi}$ a neobsahuje žádnou konstantu řádu $i > m$. Totéž lze říci o axiomu $\exists x\psi \to \psi_x(c_{\exists x\psi})$ a konstantě $c_{\exists x\psi}$.

Lemma 3.2.9 *Když φ je sentence v jazyce L a $T \models \varphi$, pak φ je tautologickým důsledkem množiny $T \cup \mathrm{H}(L)$.*

Důkaz Dokážeme, že pokud φ není tautologickým důsledkem množiny $T \cup \mathrm{H}(L)$, pak existuje struktura $\mathbf{D}$ pro jazyk L^+, ve které platí všechny formule z T a neplatí φ, takže $T \not\models \varphi$.

Když φ není tautologickým důsledkem množiny $T \cup \mathrm{H}(L)$, existuje pravdivostní ohodnocení, které přiřazuje hodnotu 1 všem formulím v $T \cup \mathrm{H}(L)$ a hodnotu 0 formuli φ. Označme v_0 jedno takové ohodnocení.

Strukturu $\mathbf{D}$ zkonstruujeme ze syntaktického materiálu, který máme k dispozici. Nosnou množinu D struktury $\mathbf{D}$ definujme jako množinu všech uzavřených termů jazyka L^+. Na množině D definujme realizaci symbolů jazyka L^+ následovně. Je-li $F \in L^+$ funkční symbol libovolné četnosti $n \geq 0$, jeho realizace $F^{\mathbf{D}}$ je dána předpisem

$$F^{\mathbf{D}}(s_1, .., s_n) = F(s_1, .., s_n). \tag{1}$$

Prvky $s_1, .., s_n$ množiny D jsou uzavřené termy a operace $F^{\mathbf{D}}$ jim přiřazuje uzavřený term $F(s_1, .., s_n)$. Je-li $c \in L^+$ konstanta, rovnost (1) říká $c^{\mathbf{D}} = c$. Každá konstanta je tedy svou vlastní realizací, a to bez ohledu na to, zda je nebo není v L. Všimněte si rozdílného významu závorek v (1): na pravé straně jsou závorky formálními symboly, tj. jsou součástí syntaxe termu $F(s_1, .., s_n)$. Je-li nyní $P \in L^+$ predikátový symbol (musí ovšem platit $P \in L$) libovolné četnosti $n \geq 1$, jeho realizaci $P^{\mathbf{D}}$ definujme předpisem

$$P^{\mathbf{D}} = \{\, [s_1, .., s_n] \,;\, v_0(P(s_1, .., s_n)) = 1 \,\}. \tag{2}$$

Každá n-tice $[s_1, .., s_n]$ tedy je nebo není v $P^{\mathbf{D}}$ podle toho, jakou hodnotu přiřazuje naše pravdivostní ohodnocení otevřené sentenci $P(s_1, .., s_n)$. O struktuře $\mathbf{D}$ postupně vyslovíme a dokážeme tři tvrzení, a to o hodnotách (i neuzavřených) termů, o tom, kdy jsou a nejsou v $\mathbf{D}$ splněny atomické formule, a konečně o tom, kdy jsou a nejsou v $\mathbf{D}$ splněny všechny formule.

Je-li t term jazyka L^+, jehož všechny volné proměnné jsou mezi $x_1, .., x_k$, a je-li e ohodnocení proměnných, jehož hodnoty v $x_1, .., x_k$ jsou $s_1, .., s_k$, pak

$$t^{\mathbf{D}}[e] = t_{x_1,..,x_k}(s_1, .., s_k). \tag{3}$$

Je-li t proměnná, pak t je jedna z $x_1, .., x_k$, řekněme x_i. Pak ale dosazením termů $s_1, .., s_k$ za $x_1, .., x_k$ v t dostaneme s_i, a s_i je zároveň hodnota $t^{\mathbf{D}}[e]$ termu x_i při ohodnocení e. Je-li t term tvaru $F(t_1, .., t_n)$, pak

$$\begin{aligned}(F(t_1, .., t_n))^{\mathbf{D}}[e] &= F^{\mathbf{D}}(t_1^{\mathbf{D}}[e], .., t_n^{\mathbf{D}}[e]) \\ &= F^{\mathbf{D}}((t_1)_{x_1,..,x_k}(s_1, .., s_k), .., (t_n)_{x_1,..,x_k}(s_1, .., s_k)) \\ &= F((t_1)_{x_1,..,x_k}(s_1, .., s_k), .., (t_n)_{x_1,..,x_k}(s_1, .., s_k)) \\ &= (F(t_1, .., t_n))_{x_1,..,x_k}(s_1, .., s_k),\end{aligned}$$

kde první rovnost je podmínka T2, druhá platí díky indukčnímu předpokladu pro termy $t_1, .., t_n$, třetí vzhledem k definici funkce $F^{\mathbf{D}}$ v (1) a čtvrtá je jasná z toho, jak se dosazuje za proměnné ve složeném termu.

Je-li ψ atomická formule, jejíž všechny volné proměnné jsou mezi $x_1, .., x_k$, a je-li e ohodnocení proměnných, jehož hodnoty v $x_1, .., x_k$ jsou $s_1, .., s_k$, pak

$$\mathbf{D} \models \psi[e] \Leftrightarrow v_0(\psi_{x_1,..,x_k}(s_1, .., s_k)) = 1. \tag{4}$$

Formule ψ totiž musí být tvaru $P(t_1, .., t_n)$, kde P je predikátový symbol četnosti n a $t_1, .., t_n$ jsou termy. Podmínka T3 říká

$$\mathbf{D} \models \psi[e] \Leftrightarrow [t_1^{\mathbf{D}}[e], .., t_n^{\mathbf{D}}[e]] \in P^{\mathbf{D}},$$

tedy, vzhledem k (2) a (3),

$$\mathbf{D} \models \psi[e] \Leftrightarrow v_0(P((t_1)_{x_1,..,x_k}(s_1, .., s_k), .., (t_n)_{x_1,..,x_k}(s_1, .., s_k))) = 1.$$

Zbývá uvážit, jak se substituuje za termy v atomických formulích: $(P(t_1, .., t_n))_{\underline{x}}(\underline{s})$ a $P((t_1)_{\underline{x}}(\underline{s}), .., (t_n)_{\underline{x}}(\underline{s}))$ jsou tytéž formule.

Je-li ψ libovolná formule, jejíž všechny volné proměnné jsou mezi $x_1, .., x_k$, a je-li e ohodnocení proměnných, jehož hodnoty v $x_1, .., x_k$ jsou $s_1, .., s_k$, pak

$$\mathbf{D} \models \psi[e] \Leftrightarrow v_0(\psi_{\underline{x}}(\underline{s})) = 1. \tag{5}$$

Pro případ, kdy ψ je atomická, jsme (5) již dokázali. Případy, kdy ψ je sestavena z jednodušších formulí pomocí některé logické spojky, jsou zcela rutinní a jejich důkaz ponecháváme na čtenáři. Předpokládejme, že ψ je tvaru $\exists y\chi$ a že (5) platí pro χ a pro všechna ohodnocení e. Předpokládejme dále, že proměnná y je různá od všech $x_1, .., x_k$. Pak

$$\begin{aligned}
\mathbf{D} \models (\exists y\chi)[e] &\Leftrightarrow \exists t \in D(\mathbf{D} \models \chi[e(y/t)]) \\
&\Leftrightarrow \exists t \in D(v_0(\chi_{y,\underline{x}}(t, \underline{s})) = 1) \\
&\Leftrightarrow v_0(\exists y\chi_{\underline{x}}(\underline{s})) = 1 \\
&\Leftrightarrow v_0((\exists y\chi)_{\underline{x}}(\underline{s})) = 1,
\end{aligned}$$

kde první ekvivalence je podmínka T8, druhá je indukční předpoklad pro formuli χ, čtvrtá je triviální a třetí si všimněme podrobněji. Formule $\chi_{y,\underline{x}}(t, \underline{s}) \to \exists y\chi_{\underline{x}}(\underline{s})$ je v $\mathrm{H}(L)$ pro každý term t, a pravdivostní ohodnocení v_0 jí tedy přiřazuje hodnotu 1. Když tedy $v_0(\chi_{y,\underline{x}}(t, \underline{s})) = 1$ pro nějaký term t, musí platit i $v_0(\exists y\chi_{\underline{x}}(\underline{s})) = 1$, jinak by v_0 porušovalo pravdivostní tabulku implikace. Naopak, když $v_0(\exists y\chi_{\underline{x}}(\underline{s})) = 1$, pak existuje term t, totiž $c_{\exists y\chi_{\underline{x}}(\underline{s})}$, pro který platí $v_0(\chi_{y,\underline{x}}(t, \underline{s})) = 1$, neboť v $\mathrm{H}(L)$ je implikace $\exists y\chi_{\underline{x}}(\underline{s}) \to \chi_{y,\underline{x}}(c_{\exists y\chi_{\underline{x}}(\underline{s})}, \underline{s})$, a její hodnota při ohodnocení v_0 je tedy 1. Případy, kdy y je jedna z $x_1, .., x_k$ nebo ψ je tvaru $\forall y\chi$, jsou podobné a jejich rozmyšlení necháváme na čtenáři.

Je-li ψ sentence, (5) říká, že ψ platí v $\mathbf{D}$, právě když $v_0(\psi) = 1$. V $\mathbf{D}$ tedy platí všechny formule z T a neplatí φ, tedy opravdu $T \not\models \varphi$. QED

Důkaz (zbývající části) věty o úplnosti Předpokládejme, že pro nějakou formuli φ platí $T \models \varphi$, zdůvodníme $T \vdash \varphi$. Můžeme předpokládat, že φ je sentence. Kdyby totiž φ měla volné proměnné $x_1, \ldots, x_r$, pracovali bychom se sentencí $\forall x_1 \ldots \forall x_r \varphi$ a využili bychom implikace $T \models \varphi \Rightarrow T \models \forall \underline{x} \varphi$ a $T \vdash \forall \underline{x} \varphi \Rightarrow T \vdash \varphi$.

Podle tvrzení 3.2.9 je formule φ tautologickým důsledkem množiny $T \cup \mathrm{H}(L)$. Podle věty o kompaktnosti ve výrokové logice existuje konečná množina $F \subseteq T \cup \mathrm{H}(L)$ taková, že φ je tautologickým důsledkem množiny F. Pišme F ve tvaru

$$F = \{\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_n\},$$

kde každá z formulí α_i je axiom specifikace nebo prvek množiny T a $\beta_1, \ldots, \beta_n$ jsou henkinovské axiomy. Předpokládejme, že henkinovské axiomy β_j jsou uspořádány tak, že axiomy příslušné henkinovským konstantám vyšších řádů předcházejí axiomy příslušné konstantám nižších řádů. Na pořadí henkinovských axiomů příslušných konstantám téhož řádu a na pořadí formulí α_i nezáleží. Protože φ je tautologický důsledek množiny F, formule

$$\alpha_1 \to (\alpha_2 \to (\ldots \to (\alpha_k \to (\beta_1 \to (\ldots \to (\beta_n \to \varphi) \ldots)$$

je tautologie. Zvolme navzájem různé proměnné $v_1, \ldots, v_n$, které se nevyskytují v F ani ve φ. Pro $1 \leq j \leq n$ označme c_j henkinovskou konstantu, ke které přísluší axiom β_j, a pro libovolnou formuli γ v jazyce L^+ označme γ' formuli, která vznikne z γ nahrazením všech výskytů konstant $c_1, \ldots, c_n$ proměnnými $v_1, \ldots, v_n$. Je zřejmé, že tímto nahrazením vznikne z tautologie opět tautologie, tedy formule dokazatelná v teorii T. Takže

1: $\quad T \vdash \alpha'_1 \to (\alpha'_2 \to (\ldots \to (\alpha'_k \to (\beta'_1 \to (\ldots \to (\beta'_n \to \varphi') \ldots)$.

Platí ovšem $\varphi' = \varphi$, protože φ neobsahuje henkinovské konstanty. Je-li α_i vlastní axiom teorie T, pak rovněž $\alpha'_i = \alpha_i$. Je-li α_i axiom specifikace, pak α'_i je opět axiom specifikace. V obou případech platí $T \vdash \alpha'_i$. Užijeme-li k-krát pravidlo MP, dostaneme

2: $\quad T \vdash \beta'_1 \to (\beta'_2 \to (\ldots \to (\beta'_n \to \varphi) \ldots)$.

Předpokládejme, že axiom β_1 má tvar $\psi_x(c_{\forall x \psi}) \to \forall x \psi$, kde $c_{\forall x \psi}$ je konstanta řádu m. Úvaha pro druhý případ, kdy β_1 má tvar $\exists x \psi \to \psi_x(c_{\exists x \psi})$, je téměř stejná. Máme

3: $\quad T \vdash (\psi_x(v_1) \to \forall x \psi) \to (\beta'_2 \to (\ldots \to (\beta'_n \to \varphi) \ldots)$.

Protože konstanta $c_{\forall x \psi}$ má maximální řád, nevyskytuje se ve formulích $\beta_2, \ldots, \beta_n$, a v_1 se tedy nevyskytuje v $\beta'_2, \ldots, \beta'_n$ (a ovšem ani ve φ). Jsme tedy oprávněni použít pravidlo Gen-E. Tím a užitím lemmatu 3.2.1 dostaneme

4: $\quad T \vdash \exists v_1 (\psi_x(v_1) \to \forall x \psi) \to (\beta'_2 \to (\ldots \to (\beta'_n \to \varphi) \ldots)$

5: $\quad T \vdash (\beta'_2 \to (\ldots \to (\beta'_n \to \varphi) \ldots)$.

Tím jsme se zbavili formule β'_1. Užijeme-li pravidlo Gen-E a lemma 3.2.1 ještě $(n-1)$-krát, zbavíme se i formulí β'_2 až β'_n, a dostaneme $T \vdash \varphi$. QED

Věta o úplnosti je tedy dokázána, ale zatím pouze pro predikátovou logiku bez rovnosti. Do kalkulu jsme dosud nepřijali žádné axiomy nebo pravidla o rovnítku. To neznamená, že rovnítko nesmíme užívat. Nejsme ale schopni o něm dokázat nic specifického. V predikátové logice bez rovnosti není předepsáno, že realizace symbolu „=“ je vždy rovnost. Může to být libovolná binární relace.

Příklad 3.2.10 Formule $\exists x \forall y (x = y) \rightarrow \forall y \exists x (x = y)$ platí v každé struktuře bez ohledu na realizaci rovnítka, a podle věty o úplnosti je tedy dokazatelná v HK. Je-li ale povoleno realizovat rovnítko libovolnou binární relací, snadno lze nalézt strukturu, ve které neplatí formule $\forall x \forall y (x = y \rightarrow y = x)$. Ta tedy v dosud uvažovaném kalkulu není dokazatelná.

Naším cílem je nyní stanovit modifikaci HK_e kalkulu HK tak, aby byla adekvátní pro predikátovou logiku s rovností. Chceme tedy, aby věta 3.2.8 zůstala v platnosti i v případě, kdy dokazatelností se myslí dokazatelnost v kalkulu HK_e a strukturou se myslí struktura, ve které je rovnítko povinně realizováno rovností. Uvidíme, že v důkazu věty o úplnosti pro predikátovou logiku s rovností půjde vlastně pouze o to, jak z modelu, ve kterém je rovnítko realizováno nějak, sestrojit model, v němž je realizováno rovností. Použijeme konstrukci, které se v algebře říká *faktorizace*.

Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou struktury pro jazyk L a nechť $f : A \rightarrow B$. Řekneme, že f *zachovává* (n-ární) funkční symbol $F \in L$, jestliže pro libovolnou n-tici $a_1, \ldots, a_n$ prvků z A platí rovnost

$$f(F^{\mathbf{A}}(a_1, \ldots, a_n)) = F^{\mathbf{B}}(f(a_1), \ldots, f(a_n)).$$

Řekneme, že f *zachovává* (n-ární) predikátový symbol $P \in L$, jestliže pro libovolnou n-tici $a_1, \ldots, a_n$ prvků z A platí ekvivalence

$$[a_1, \ldots, a_n] \in P^{\mathbf{A}} \Leftrightarrow [f(a_1), \ldots, f(a_n)] \in P^{\mathbf{B}}.$$

Řekneme, že f je *homomorfismus* struktur $\mathbf{A}$ a $\mathbf{B}$, jestliže f zachovává všechny (funkční i predikátové) symboly jazyka L.

Lemma 3.2.11 *(a) Homomorfismus $f : A \rightarrow B$ struktur $\mathbf{A}$ a $\mathbf{B}$ pro jazyk L zachovává všechny otevřené formule. To znamená, že pro libovolnou otevřenou formuli $\varphi(x_1, \ldots, x_n)$ a libovolnou n-tici $a_1, \ldots, a_n$ prvků z množiny A platí ekvivalence $\mathbf{A} \models \varphi[a_1, \ldots, a_n] \Leftrightarrow \mathbf{B} \models \varphi[f(a_1), \ldots, f(a_n)]$.*
(b) Pokud navíc f zobrazuje A na B, pak f zachovává všechny formule jazyka L, tj. ekvivalence z tvrzení (a) platí pro libovolnou formuli φ jazyka L.

Důkaz Je-li $t(x_1, \ldots, x_n)$ libovolný term jazyka L a jsou-li $a_1, \ldots, a_n$ prvky struktury $\mathbf{A}$, pak $f(t^{\mathbf{A}}[a_1, \ldots, a_n]) = t^{\mathbf{B}}[f(a_1), \ldots, f(a_n)]$. Jinými slovy, homomorfismus zachovává všechny termy. To se dokáže indukcí podle složitosti termu t a využitím podmínek T1 a T2 a předpokladu, že f zachovává všechny funkční symboly. Nechť

dále $P \in L$ je m-ární predikátový symbol, $t_1(x_1,..,x_n)$ až $t_m(x_1,..,x_n)$ jsou termy jazyka L a $a_1,..,a_n$ jsou prvky struktury $\mathbf{A}$. Pak

$$\begin{aligned}\mathbf{A} \models P(t_1,..,t_m)[a_1,..,a_n] &\Leftrightarrow [t_1[\underline{a}],..,t_m[\underline{a}]] \in P^{\mathbf{A}}\\ &\Leftrightarrow [f(t_1^{\mathbf{A}}[\underline{a}]),..,f(t_m^{\mathbf{A}}[\underline{a}])] \in P^{\mathbf{B}}\\ &\Leftrightarrow [t_1^{\mathbf{B}}[f(a_1),..,f(a_n)],..,t_m^{\mathbf{B}}[f(a_1),..,f(a_n)]] \in P^{\mathbf{B}}\\ &\Leftrightarrow \mathbf{B} \models P(t_1,..,t_m)[f(a_1),..,f(a_n)],\end{aligned}$$

kde první a poslední ekvivalence je podmínka T3, druhá plyne z toho, že f zachovává symbol P, a třetí je fakt, že f zachovává termy. Tím je ověřeno, že f zachovává atomické formule. Zbytek je indukce podle souhrnného počtu logických spojek (v (b) podle souhrnného počtu logických spojek a kvantifikátorů) ve formuli φ. Nechť například $\varphi(x_1,..,x_n)$ je tvaru $\exists v\psi(v,x_1,..,x_n)$ a pro ψ již tvrzení platí. Když $\mathbf{B} \models \varphi[f(a_1),..,f(a_n)]$, tj. $\mathbf{B} \models (\exists v\psi(v,\underline{x}))[f(a_1),..,f(a_n)]$, pak (dle podmínky T8) existuje $b \in B$ takové, že $\mathbf{B} \models \psi[b,f(a_1),..,f(a_n)]$. Protože f zobrazuje A na B, existuje $a \in A$ takové, že $b = f(a)$. Tedy $\mathbf{B} \models \psi[f(a),f(a_1),..,f(a_n)]$, indukční předpoklad dává $\mathbf{A} \models \psi[a,a_1,..,a_n]$ a dále $\mathbf{A} \models (\exists v\psi)[a_1,..,a_n]$. Tím jsme na ukázku provedli ten z kroků důkazu tvrzení (b), ve kterém se uplatní podmínka, že $\mathrm{Rng}(f) = B$. QED

Kalkulus HK$_\mathrm{e}$ pro predikátovou logiku s rovností definujme jako rozšíření kalkulu HK o následující axiomy:

E1: $\forall x(x = x)$,

E2: $\forall x\forall y(x = y \to y = x)$,

E3: $\forall x\forall y\forall z(x = y \;\&\; y = z \to x = z)$,

E4: $\forall \underline{x}\forall \underline{y}(x_1 = y_1 \;\&\; .. \;\&\; x_n = y_n \to F(x_1,..,x_n) = F(y_1,..,y_n))$,

E5: $\forall \underline{x}\forall \underline{y}(x_1 = y_1 \;\&\; .. \;\&\; x_n = y_n \to (P(x_1,..,x_n) \equiv P(y_1,..,y_n)))$,

kde F je libovolný funkční a P libovolný predikátový symbol. Axiomům E1–E5 říkáme *axiomy rovnosti*. E1–E3 jsou jednotlivé axiomy, E4 a E5 jsou schémata. Každý funkční a predikátový symbol (zvoleného jazyka) má jeden axiom tvaru E4 resp. E5. Kalkulus HK$_\mathrm{e}$ má tedy odvozovací pravidla MP, Gen-A a Gen-E a logické axiomy trojího druhu: výrokové axiomy tvaru A1–A7, axiomy o kvantifikátorech B1 a B2 a axiomy rovnosti E1–E5. Jednoduchý (ne zcela kompletní) důkaz v kalkulu HK$_\mathrm{e}$ může vypadat například takto:

1: $\forall x\forall y(x = y \to y = x) \to \forall y(x = y \to y = x)$; B1

2: $\forall y(x = y \to y = x) \to (x = x + y \to x + y = x)$; B1

3: $x = x + y \to x + y = x$; 1, 2, E2

4: $y = x + y \;\&\; x + y = x \to y = x$; B1, E3

5:	$y = x + y \ \&\ x = x + y \ \to\ y = x$	; 3, 4
6:	$\forall v(v = x + v) \ \to\ y = x + y$	; B1
7:	$\forall v(v = v + y) \ \to\ x = x + y$	; B1
8:	$\forall v(v = x + v) \ \&\ \forall v(v = v + y) \ \to\ y = x$	; 5, 6, 7.

Důkaz jsme opět zkrátili vynecháním výrokových kroků: formule (5) je tautologickým důsledkem formulí (3) a (4) a formule (8) je tautologickým důsledkem formulí (5)–(7). Formule (4) je z axiomu E3 odvozena trojnásobným užitím axiomu B1 podobně, jako byla formule (3) odvozena z (E2) (viz cvičení 10). Uvedený důkaz je formálním důkazem tvrzení pokud x je levý a y pravý neutrální prvek operace $+$, pak x a y se sobě rovnají. Další příklady důkazů v kalkulu $\mathrm{HK_e}$ budou uvedeny za důkazem věty 3.2.13 spolu s příklady axiomatických teorií.

V následující větě 3.2.12 dokážeme, že kalkulus $\mathrm{HK_e}$ je silně korektní i silně úplný vůči sémantice predikátové logiky s rovností. Znění věty 3.2.12, *věty o silné úplnosti kalkulu* HK_e, je do písmene stejné jako znění věty 3.2.8. Dokonce i definice relace $\models$ je stejná: $T \models \varphi$, jestliže φ platí ve všech modelech teorie T. Rozdíl je v tom, že modelem teorie T se nyní myslí struktura pro predikátovou logiku s rovností (v níž platí všechny axiomy teorie T) a dokazatelnost a bezespornost se nyní vztahují ke kalkulu $\mathrm{HK_e}$.

Věta 3.2.12 (o silné úplnosti kalkulu $\mathbf{HK_e}$) *(a) Je-li T libovolná teorie, pak T má model, právě když T je bezesporná.*
(b) Je-li T teorie a φ formule, pak $T \vdash \varphi$, právě když $T \models \varphi$.

Důkaz Obě implikace $\Rightarrow$ vyjadřují silnou korektnost kalkulu $\mathrm{HK_e}$ a jejich platnost plyne ze silné korektnosti kalkulu HK a z faktu, že axiomy E1–E5 evidentně platí v každé struktuře, ve které je rovnítko realizováno rovností. Implikace $\Leftarrow$ v (a) plyne z implikace $\Leftarrow$ v (b) stejně jako v důkazu věty 3.2.8. Zbývá tedy dokázat implikaci $\Leftarrow$ v (b).

Nechť tedy T je teorie v jazyce L a φ je formule, kterou nelze (pomocí pravidel a axiomů kalkulu $\mathrm{HK_e}$) dokázat z předpokladů T. Chceme sestrojit model $\mathbf{K}$ teorie T, který je strukturou pro predikátovou logiku s rovností a pro který platí $\mathbf{K} \not\models \varphi$. Označme E množinu všech axiomů rovnosti pro jazyk L. Nedokazatelnost formule φ v kalkulu $\mathrm{HK_e}$ z množiny předpokladů T znamená, že φ není v kalkulu HK dokazatelná z množiny předpokladů $T \cup E$. Podle věty o úplnosti 3.2.8 existuje struktura $\mathbf{M}$ taková, že $\mathbf{M} \models T$, $\mathbf{M} \models E$ a $\mathbf{M} \not\models \varphi$. Definujme na nosné množině M struktury $\mathbf{M}$ relaci $\approx$ předpisem $a_1 \approx a_2 \Leftrightarrow \mathbf{M} \models (x = y)[a_1, a_2]$. Protože v $\mathbf{M}$ platí axiomy E1–E3, relace $\approx$ je ekvivalence. Pro každé $a \in M$ označme $[a]$ třídu ekvivalence $\approx$, která obsahuje a. Tedy $[a] = \{\, a' \in M \,;\, a' \approx a \,\}$. Označme K množinu $M/\!\approx$, tj. množinu $\{\, [a] \,;\, a \in M \,\}$, a označme f funkci $a \mapsto [a]$. Funkce f zobrazuje M na K. Je-li $F \in L$ n-ární funkční symbol, definujme jeho realizaci $F^{\mathbf{K}} : K^n \to K$ předpisem

$$F^{\mathbf{K}}([a_1], .., [a_n]) = [F^{\mathbf{M}}(a_1, .., a_n)]. \qquad (*)$$

Jsou-li tedy $b_1, .., b_n$ libovolné prvky struktury $\mathbf{K}$, funkce $F^{\mathbf{K}}$ určí jejich obraz tak, že zvolí „reprezentanty“ $a_1, .., a_n$ tříd $b_1, .., b_n$, tj. prvky $a_1, .., a_n$ množiny M takové, že $a_1 \in b_1$ až $a_n \in b_n$, a za obraz n-tice $[b_1, .., b_n]$ prohlásí onu třídu ekvivalence $\approx$, která obsahuje prvek $F^{\mathbf{M}}(a_1, .., a_n)$. Protože v $\mathbf{M}$ platí axiom E4 pro symbol F, na volbě reprezentantů nezáleží, definice operace $F^{\mathbf{K}}$ je korektní. Analogicky, je-li P libovolný n-ární predikátový symbol jazyka L, z platnosti jemu příslušného axiomu E5 v $\mathbf{M}$ plyne, že předpis

$$[[a_1], .., [a_n]] \in P^{\mathbf{K}} \Leftrightarrow [a_1, .., a_n] \in P^{\mathbf{M}} \qquad (**)$$

korektně definuje n-ární relaci $P^{\mathbf{K}}$ na struktuře K. Podmínky $(*)$ a $(**)$ navíc znamenají, že funkce f zachovává všechny funkční i predikátové symboly jazyka L.

Máme tedy strukturu $\mathbf{K}$ pro jazyk L a funkci f z M na K, která je homomorfismem struktur $\mathbf{M}$ a $\mathbf{K}$. Podle lemmatu 3.2.11(b) v $\mathbf{M}$ a v $\mathbf{K}$ platí tytéž sentence. Tedy $\mathbf{K} \models T$ a $\mathbf{K} \not\models \varphi$. Když třídy $[a_1]$ a $[a_2]$ ekvivalence $\approx$ splňují v $\mathbf{K}$ formuli $x = y$, pak, protože f zachovává i symbol $=$, prvky a_1 a a_2 ve struktuře $\mathbf{M}$ také splňují formuli $x = y$. Podle definice relace $\approx$ tedy platí $a_1 \approx a_2$ a $[a_1] = [a_2]$. Tím jsme ověřili, že rovnítko je v $\mathbf{K}$ realizováno rovností.

Získali jsme model $\mathbf{K}$ teorie T, který je strukturou pro predikátovou logiku s rovností a ve kterém neplatí formule φ. Tím jsme dokázali, že φ v predikátové logice s rovností nevyplývá z T. QED

Následující věta, slabá verze Löwenheimovy-Skolemovy věty, je důsledkem důkazů vět 3.2.8 a 3.2.12. K jejímu znění poznamenejme, že mohutnost libovolné množiny X značíme $|X|$. Jsou-li κ a λ kardinální čísla a alespoň jedno z nich je nekonečné, pak $\kappa + \lambda = \max\{\kappa, \lambda\}$. Jsou-li navíc obě nenulová, platí i $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$. Součet $\aleph_0 + |L|$ ve znění věty 3.2.13 je tedy roven $|L|$ v případě, kdy jazyk L je nekonečný, a je roven $\aleph_0$ v případě, kdy je konečný. Věta 3.2.13 tedy pro žádnou teorii nezaručuje existenci konečného modelu (a z příkladu 3.1.19(f) víme, že některé bezesporné teorie s konečným jazykem a konečně mnoha axiomy žádný konečný model nemají). Nicméně bezprostředním důsledkem věty 3.2.13 je tvrzení, že každá bezesporná teorie s jazykem, který je konečný nebo spočetný (říká se nejvýše spočetný), má model, který je také nejvýše spočetný. Mohutnost modelu definujeme jako mohutnost jeho nosné množiny. V kontextu věty 3.2.13 by ale nevadilo, kdybychom uvažovali i mohutnost realizací symbolů jazyka L.

Věta 3.2.13 *Nechť T je bezesporná teorie s jazykem L. Pak T má model, jehož mohutnost je nejvýše $\aleph_0 + |L|$.*

Důkaz Označme $\kappa = \aleph_0 + |L|$ a vraťme se k důkazu lemmatu 3.2.9. Každá henkinovská konstanta $c_{\exists x\psi}$ a $c_{\forall x\psi}$ řádu 0 jednoznačně určuje sentenci $\exists x\psi$ resp. $\forall x\psi$. Počet sentencí jazyka L je omezen počtem všech konečných posloupností prvků množiny, jejíž mohutnost je nejvýše κ, tedy opět kardinálním číslem κ. Henkinovských konstant řádu 0 je tedy nejvýše κ. Indukce dle m dává, že také henkinovských

konstant řádu m je nejvýše κ, a všech henkinovských konstant (všech řádů dohromady) je tak $\aleph_0 \cdot \kappa = \kappa$. Jazyk L^+ vznikl přidáním henkinovských konstant k L a jeho mohutnost je rovněž omezena číslem κ. Také všech uzavřených termů jazyka L^+ je nejvýše κ. Tedy pro nosnou množinu D struktury $\mathbf{D}$ sestrojené v důkazu lemmatu 3.2.9 platí $|D| \leq \kappa$. V důkazu věty 3.2.12 můžeme tedy předpokládat, že $|M| \leq \kappa$. Protože f zobrazuje M na K, platí také $|K| \leq \kappa$. QED

3.2.2 Příklady důkazů a teorií

Ve zbytku tohoto oddílu uveďme několik axiomatických teorií, které pokládáme za důležité nebo za užitečné pro další výklad. Ukážeme si také další příklady formálních důkazů. Uvažujme nejprve strukturu $\langle \mathrm{N}, 0, \mathrm{s}\rangle$ přirozených čísel s nulou a s následnickou funkcí, tj. s funkcí $x \mapsto x+1$. Tato struktura je strukturou pro jazyk $\{0, \mathrm{S}\}$ s konstantou a s unárním funkčním symbolem. Snadno lze ověřit, že ve struktuře $\langle \mathrm{N}, 0, \mathrm{s}\rangle$ platí následující sentence:

Q1: $\forall x \forall y(\mathrm{S}(x) = \mathrm{S}(y) \rightarrow x = y)$,

Q2: $\forall x(\mathrm{S}(x) \neq 0)$,

Q3: $\forall x(x \neq 0 \rightarrow \exists y(x = \mathrm{S}(y)))$,

Lm: $\forall x(\mathrm{S}^{(m)}(x) \neq x), \qquad m \geq 1.$

Zápis $\mathrm{S}^{(m)}(x)$ ve čtvrtém řádku označuje term $\mathrm{S}(\mathrm{S}(\ldots(x)\ldots)$ s m výskyty symbolu S. Například sentence L3 tvrdí, že třemi skoky následnické funkce se z žádného objektu x nelze dostat zpět do x. Označme SUCC teorii s axiomy Q1–Q3 a Lm, kde $m \geq 1$. Teorie SUCC má tedy nekonečně mnoho axiomů: tři jednotlivé axiomy a dále schéma, jehož instance zakazují „konečné cykly“. Teorii SUCC říkejme *teorie následnické funkce* nebo krátce *teorie následníka*.

Každá struktura $\langle D, e, f\rangle$ taková, že $e \in D$ je vytčený prvek a $f : D \rightarrow D$ je prostá funkce, pro kterou platí $\mathrm{Rng}(f) = D - \{e\}$ a která neporušuje žádný z axiomů Lm, je modelem teorie SUCC. A naopak, každý model teorie SUCC vypadá takto. Jak už bylo řečeno, jedním z modelů teorie SUCC je struktura $\langle \mathrm{N}, 0, \mathrm{s}\rangle$. V oddílu 3.4 se dozvíme více o modelech teorie SUCC. Budeme se tam věnovat otázkám, zda teorie SUCC má i jiné modely, než je „preferovaný“ model $\langle \mathrm{N}, 0, \mathrm{s}\rangle$ (na tuto otázku dovede čtenář pravděpodobně odpovědět již nyní), jak takové modely vypadají a zda je lze vyloučit (zakázat) přidáním dalších axiomů k teorii SUCC.

Připomeňme si, viz str. 144, že term tvaru $\mathrm{S}(\mathrm{S}(\ldots(0)\ldots)$ s m výskyty symbolu S nazýváme numerál a značíme jej $\overline{m}$. Položme si otázku, zda v teorii SUCC lze dokázat sentenci $\overline{2} \neq \overline{1}$ nebo sentenci $\forall x \exists y(\mathrm{S}(y) \neq x)$. Jako obvykle, chceme-li zdůvodnit dokazatelnost nějaké formule z nějaké množiny předpokladů, může být užitečné utvořit nejprve neformální důkaz. Neformální důkaz sentence $\overline{2} \neq \overline{1}$ může vypadat například takto:

> Nechť $\mathrm{S}(\mathrm{S}(0)) = \mathrm{S}(0)$. Axiom Q1 a volba $x := \mathrm{S}(0)$ a $y := 0$ dávají $\mathrm{S}(0) = 0$.
> To je spor s Q2.

Sentenci $\forall x \exists y(\mathrm{S}(y) \neq x)$ lze neformálně dokázat takto:

> Nechť x je dáno. Platí $x = \mathrm{S}(0)$ nebo $x \neq \mathrm{S}(0)$. Když $x = \mathrm{S}(0)$, lze zvolit $y := \mathrm{S}(0)$, neboť z předchozí úvahy víme, že $\mathrm{S}(\mathrm{S}(0)) \neq \mathrm{S}(0)$. Když $x \neq \mathrm{S}(0)$, lze zvolit $y := 0$.

Neformální důkaz zpravidla umožňuje odhadnout, jaké instance logických axiomů máme použít, chceme-li sestrojit formální důkaz, tj. důkaz vyhovující definici důkazu v kalkulu HK_{e}:

1:	$\forall x(\mathrm{S}(x) \neq 0) \to \mathrm{S}(0) \neq 0$	; B1
2:	$\mathrm{S}(0) \neq 0$	; 1, Q2
3:	$\mathrm{S}(\mathrm{S}(0)) = \mathrm{S}(0) \to \mathrm{S}(0) = 0$	; Podobně z B1 a Q1
4:	$\mathrm{S}(\mathrm{S}(0)) \neq \mathrm{S}(0)$	; 2, 3
5:	$\mathrm{S}(\mathrm{S}(0)) \neq \mathrm{S}(0) \to \exists y(\mathrm{S}(y) \neq \mathrm{S}(0))$	; B2
6:	$\exists y(\mathrm{S}(y) \neq \mathrm{S}(0))$	; 4, 5
7:	$\mathrm{S}(y) = x \ \& \ x = \mathrm{S}(0) \to \mathrm{S}(y) = \mathrm{S}(0)$	; E3, B1
8:	$\mathrm{S}(y) \neq x \to \exists y(\mathrm{S}(y) \neq x)$	; B2
9:	$\mathrm{S}(y) \neq \mathrm{S}(0) \to (x = \mathrm{S}(0) \to \exists y(\mathrm{S}(y) \neq x))$	; 7, 8
10:	$\exists y(\mathrm{S}(y) \neq \mathrm{S}(0)) \to (x = \mathrm{S}(0) \to \exists y(\mathrm{S}(y) \neq x))$	; Gen-E
11:	$x = \mathrm{S}(0) \to \exists y(\mathrm{S}(y) \neq x)$	; 10, 6
12:	$\mathrm{S}(0) = x \to x = \mathrm{S}(0)$	; E2, B1
13:	$\mathrm{S}(0) \neq x \to \exists y(\mathrm{S}(y) \neq x)$	; B2
14:	$\exists y(\mathrm{S}(y) \neq x)$	; 11, 12, 13
15:	$\mathrm{S}(0) \neq 0 \to \exists y(\mathrm{S}(y) \neq x)$	; 14
16:	$\mathrm{S}(0) \neq 0 \to \forall x \exists y(\mathrm{S}(y) \neq x)$	; Gen-A, 15
17:	$\forall x \exists y(\mathrm{S}(y) \neq x)$	; 16, 2.

Při odvození formulí (6), (9), (11) a (14) jsme opět použili úmluvu o vynechání výrokových kroků. Odvození formulí (3), (7) a (12) jsme zkrátili v duchu cvičení 10. Ve cvičení 5 se pracuje s pravidlem Gen tvaru $\varphi \,/\, \forall x \varphi$. Při odvození formule (17) jsme ukázali, jak lze pravidlo Gen simulovat pomocí pravidla Gen-A a libovolné dokazatelné sentence, tj. naznačili jsme část řešení cvičení 5.

Protože tvrdíme, že je pouze věcí zkušenosti, jak správný a dostatečně podrobný neformální důkaz přepsat (přeložit) na důkaz v kterémkoliv (korektním a úplném)

kalkulu, a protože jistou zkušenost s formálními důkazy již máme, v dalším textu budeme neformální důkazy užívat velmi často. K jejich odlišení od ostatního textu užíváme bezpatkové písmo. Bezpatkovým písmem je tedy zapsána úvaha, kterou lze *formalizovat*, tj. zapsat pomocí formulí daného jazyka tak, aby se vyhovělo definici důkazu v daném kalkulu. Někdy bezpatkovým písmem vyznačujeme také podmínky vyjadřující vlastnosti formálních objektů nebo tvrzení o formálních objektech. I v těchto případech platí, že čtenář si za nimi má představit formule příslušného jazyka. V některých případech (zejména v kapitole 2) užíváme bezpatkové písmo také k zápisu algoritmů. I tam označuje něco, co může být (má být) formalizováno.

Lze také argumentovat, že neformální důkaz je vlastně ověření faktu, že daná formule je v každé struktuře splněna všemi ohodnoceními, která splňují všechny předpoklady, a že tedy existenci formálního důkazu, který je překladem našeho neformálního, zaručuje věta o úplnosti 3.2.12.

V některých případech lze dokazatelnost nějaké formule φ z množiny předpokladů Δ rychle zdůvodnit přímým užitím věty o úplnosti, tj. úvahou o strukturách, o které *ne*tvrdíme, že je neformálním důkazem. Pěkný a v dalším textu užitečný příklad je tento: každá sentence tvaru

$$\forall x_1 \,..\, \forall x_k \exists y (\mathrm{S}^{(m)}(y) \neq x_1 \ \&\ \,..\, \ \&\ \mathrm{S}^{(m)}(y) \neq x_k) \qquad (*)$$

vyplývá z axiomů Q1 a Q2 teorie SUCC, a je tedy v teorii SUCC dokazatelná. Všimněme si, že sentence $\forall x \exists y (\mathrm{S}(y) \neq x)$, kterou jsme dokázali, je speciálním případem schématu $(*)$. Vyplývání každé sentence tvaru $(*)$ se zdůvodní následovně. Nechť $\mathbf{D}$ je libovolná struktura pro jazyk $\{0, \mathrm{S}\}$, ve které platí sentence Q1 a Q2, a nechť $a_1, .., a_k$ je ohodnocení proměnných $x_1, .., x_k$ ve struktuře $\mathbf{D}$. V množině D existuje nejvýše jedno ohodnocení b proměnné y takové, že ohodnocení $a_1, .., a_k, b$ splňuje formuli $\mathrm{S}^{(m)}(y) = x_i$, a tedy v D existuje nejvýše k prvků b takových, že ohodnocení $a_1, .., a_k, b$ splňuje disjunkci $\mathrm{S}^{(m)}(y) = x_1 \vee \,..\, \vee \mathrm{S}^{(m)}(y) = x_k$. Nekonečně mnoho prvků $d \in D$ tedy splňuje její negaci $\mathrm{S}^{(m)}(y) \neq x_1 \ \&\ \,..\, \ \&\ \mathrm{S}^{(m)}(y) \neq x_k$, neboť struktura $\mathbf{D}$ musí být nekonečná (viz 3.1.19(f)). Tím je ověřeno, že ke každému ohodnocení proměnných $x_1, .., x_k$ lze zvolit ohodnocení proměnné y tak, aby výsledné ohodnocení splňovalo v $\mathbf{D}$ formuli $\mathrm{S}^{(m)}(y) \neq x_1 \ \&\ \,..\, \ \&\ \mathrm{S}^{(m)}(y) \neq x_k$.

Teorie ostrého lineárního uspořádání má jazyk $\{<\}$ s jediným binárním predikátem a axiomy

LO1: $\forall x \forall y \forall z (x < y \ \&\ y < z \ \rightarrow\ x < z)$,

LO2: $\forall x \forall y (x < y \ \rightarrow\ \neg(y < x))$,

LO3: $\forall x \forall y (x < y \ \vee\ x = y \ \vee\ y < x)$,

které vyjadřují, že relace $<$ je tranzitivní, antisymetrická a lineární. Teorii s axiomy LO1–LO3 značíme LO. Teorie LO vznikla přidáním axiomu LO3 k *teorii ostrého uspořádání* z příkladu 3.2.5. Modely teorie ostrého uspořádání jsou všechny (ostře) uspořádané množiny, a nic jiného. Modely teorie LO jsou všechny lineárně ostře uspořádané množiny (tj. takové, které jsou uspořádané a ve kterých každé dva prvky

jsou srovnatelné), a nic jiného. Důležité příklady modelů teorie LO jsou struktury $\langle \mathrm{N}, < \rangle$, $\langle \mathrm{Q}, < \rangle$ nebo $\langle \mathrm{R}, < \rangle$ přirozených (racionálních, reálných) čísel s (obvyklým) uspořádáním.

Teorie DNO, *teorie hustého lineárního uspořádání bez minima a maxima*, má jazyk $\{<\}$, axiomy LO1–LO3 teorie LO a dále axiomy

Dn1: $\forall x \forall y (x < y \rightarrow \exists z (x < z \ \& \ z < y))$,

Dn2: $\forall x \exists y_1 \exists y_2 (y_1 < x \ \& \ x < y_2)$.

Je zřejmé, že struktury $\langle \mathrm{Q}, < \rangle$ a $\langle \mathrm{R}, < \rangle$ nebo třeba reálný interval $(0, 1)$ s obvyklým uspořádáním jsou modely teorie DNO. Na druhé straně struktury $\langle \mathrm{Z}, < \rangle$ a $\langle \mathrm{N}, < \rangle$ jsou příklady struktur, které nejsou modely teorie DNO.

Teorie neostrého lineárního uspořádání má rovněž jazyk s jediným binárním predikátem, který se v tomto případě píše $\leq$, a axiomy

$$\forall x \forall y \forall z (x \leq y \ \& \ y \leq z \rightarrow x \leq z),$$

$$\forall x (x \leq x),$$

$$\forall x \forall y (x \leq y \ \& \ y \leq x \rightarrow x = y),$$

$$\forall x \forall y (x \leq y \ \vee \ y \leq x),$$

které postulují, že relace $\leq$ je tranzitivní, reflexivní, slabě antisymetrická a lineární. Snadno lze ověřit (cvičení), že pokládáme-li formuli $x \leq y$ za zkratku pro formuli $x < y \ \vee \ x = y$, všechny axiomy teorie neostrého lineárního uspořádání lze dokázat v teorii LO. Teorii neostrého lineárního uspořádání lze tedy pokládat za obsaženou v teorii LO v tom smyslu, že každá její formule je vlastně současně formulí teorie LO a každý důkaz v ní je vlastně současně důkazem v teorii LO.

V teorii neostrého lineárního uspořádání označme $D_n(x_1, .., x_n, y)$ formuli

$$x_1 \leq y \ \& \ .. \ \& \ x_n \leq y \ \& \ (x_1 = y \ \vee \ .. \ \vee \ x_n = y),$$

kde $n \geq 1$. Formuli $D_n(x_1, .., x_n, y)$ lze číst objekt y je maximální mezi $x_1, .., x_n$. Sentence $\forall x_1 .. \forall x_n \exists y D_n(x_1, .., x_n, y)$ tedy tvrdí, že mezi každými n objekty (ne nutně různými) existuje maximální objekt. Je jasné, že tato sentence platí v každé neostře lineárně uspořádané množině. Dle věty 3.2.12 je tedy dokazatelná v teorii neostrého lineárního uspořádání a ve smyslu předchozího odstavce je dokazatelná také v teorii LO. Abychom ještě jednou ukázali, jak fungují pravidla a axiomy kalkulu $\mathrm{HK_e}$, dokážeme existenci důkazu sentence $\forall x_1 .. \forall x_n \exists y D_n(x_1, .., x_n, y)$ přímo, indukcí podle n. Přesněji řečeno, předvedeme pouze indukční krok. Sestrojíme tedy (víceméně kompletní) důkaz sentence $\forall x_1 .. \forall x_{n+1} \exists y D_{n+1}(x_1, .., x_{n+1}, y)$ z axiomů teorie neostrého uspořádání za podmínky, že je již sestrojen důkaz sentence $\forall x_1 .. \forall x_n \exists y D_n(x_1, .., x_n, y)$. Pišme $\underline{x}$ místo $x_1, .., x_n$.

1: $\forall x_1 .. \forall x_n \exists y D_n(\underline{x}, y)$; Již dokázáno

2:	$\forall x(x \leq x) \to x_{n+1} \leq x_{n+1}$	; B1
3:	$\forall x(x = x) \to x_{n+1} = x_{n+1}$	; B1
4:	$x_{n+1} \leq x_{n+1}$	; 2, axiom
5:	$x_{n+1} = x_{n+1}$	; 3, E1
6:	$x_1 \leq y \ \& \ y \leq x_{n+1} \to x_1 \leq x_{n+1}$	; B1, axiom
$\vdots$	$\vdots$	
$n+5$:	$x_n \leq y \ \& \ y \leq x_{n+1} \to x_n \leq x_{n+1}$	; …
$n+6$:	$y \leq x_{n+1} \ \& \ D_n(\underline{x}, y) \to D_{n+1}(\underline{x}, x_{n+1}, x_{n+1})$	; 6 až $n+5$, 4 a 5
$n+7$:	$y \leq x_{n+1} \ \& \ D_n(\underline{x}, y) \to \exists y D_{n+1}(\underline{x}, x_{n+1}, y)$	; $n+6$, B2
$n+8$:	$x_{n+1} \leq y \ \& \ D_n(\underline{x}, y) \to D_{n+1}(\underline{x}, x_{n+1}, y)$	; Tautologie
$n+9$:	$x_{n+1} \leq y \ \& \ D_n(\underline{x}, y) \to \exists y D_{n+1}(\underline{x}, x_{n+1}, y)$	; $n+8$, B2
$n+10$:	$\forall x \forall y(x \leq y \vee y \leq x) \to x_{n+1} \leq y \vee y \leq x_{n+1}$	; B1
$n+11$:	$x_{n+1} \leq y \vee y \leq x_{n+1}$	; $n+10$, axiom
$n+12$:	$D_n(\underline{x}, y) \to \exists y D_{n+1}(\underline{x}, x_{n+1}, y)$	; $n+11$, $n+9$, $n+7$
$n+13$:	$\exists y D_n(\underline{x}, y) \to \exists y D_{n+1}(\underline{x}, x_{n+1}, y)$	; Gen-E
$n+14$:	$\forall \underline{x} \exists y D_n(\underline{x}, y) \to \exists y D_n(\underline{x}, y)$	; B1
$n+15$:	$\forall \underline{x} \exists y D_n(\underline{x}, y) \to \exists y D_{n+1}(\underline{x}, x_{n+1}, y)$	; $n+14$, $n+13$
$n+16$:	$\forall \underline{x} \exists y D_n(\underline{x}, y) \to \forall \underline{x} \forall x_{n+1} \exists y D_{n+1}(\underline{x}, x_{n+1}, y)$	; $n+15$, Gen-A
$n+17$:	$\forall x_1 \,.\, \forall x_{n+1} \exists y D_{n+1}(\underline{x}, x_{n+1}, y)$	; $n+16$, 1.

Je samozřejmé, že při odvození formule $n+14$ a při odvození formule $n+16$ z formule $n+15$ je třeba axiom B1 resp. pravidlo Gen-A užít n-násobně.

Je-li $\mathbf{D}$ libovolná struktura pro nějaký jazyk L, definujme množinu $\mathrm{Th}(\mathbf{D})$ jako množinu všech sentencí platných v $\mathbf{D}$. Množině $\mathrm{Th}(\mathbf{D})$ říkáme *teorie struktury* $\mathbf{D}$. Naše ostatní příklady axiomatických teorií uvedené v tomto oddílu mají vždy množinu axiomů tvaru konečně mnoho sentencí plus případně konečně mnoho schémat. Teorie $\mathrm{Th}(\mathbf{D})$ nějaké struktury $\mathbf{D}$ se od těchto příkladů liší tím, že množina všech sentencí φ, které jsou jejími axiomy, netvoří „úhledný seznam“, nýbrž je určena podmínkou, totiž podmínkou $\mathbf{D} \models \varphi$. To však definice axiomatické teorie připouští. Pro libovolnou strukturu $\mathbf{D}$ platí $\mathrm{Thm}(\mathrm{Th}(\mathbf{D})) = \mathrm{Th}(\mathbf{D})$, každá sentence dokazatelná v teorii $\mathrm{Th}(\mathbf{D})$ je současně jejím axiomem.

Zermelova-Fraenkelova teorie množin ZF má jazyk $\{\in\}$ sestávající z jediného binárního predikátového symbolu. Objektům teorie ZF se říká *množiny*. Teorie ZF má (tj. obvykle se formuluje tak, že má) šest jednotlivých axiomů (axiom existence, extenzionality, dvojice, sumy, potence a nekonečna) a dvě axiomatická schémata (schéma vydělení a schéma nahrazení). Na ukázku uveďme axiom dvojice:

$$\forall x \forall y \exists z \forall v (v \in z \equiv v = x \vee v = y),$$

který postuluje, že k libovolným dvěma množinám x a y existuje množina z, jejímiž prvky jsou x a y, a nic jiného. Ostatní axiomy neuvádíme, lze je nalézt v libovolné učebnici věnované teorii množin (doporučujeme například [2]). Kromě vyjmenovaných axiomů a schémat se k teorii ZF obvykle přidávají další více nebo méně „volitelné“ axiomy, jako je axiom regularity nebo axiom výběru AC.

Vedle Zermelovy-Fraenkelovy teorie množin se často lze setkat také s *Gödelovou-Bernaysovou teorií množin* GB. Objektům teorie GB se říká *třídy*, množina je v GB definována jako třída, která je prvkem nějaké (jiné nebo stejné) třídy. Třídám, které nejsou množiny, se říká vlastní třídy. V GB lze dokázat existenci vlastních tříd. Teorie ZF a GB spolu úzce souvisejí, neboť se shodují v tom, jaká tvrzení o množinách v nich lze dokázat. Důležitým metamatematickým rozdílem mezi teoriemi ZF a GB je to, že při formulaci axiomů teorie GB se lze obejít bez axiomatických schémat. Gödelova-Bernaysova teorie množin je konečně axiomatizovatelná.

Význam různých variant teorie množin (ZF, GB nebo ještě dalších) je v tom, že všechny matematické pojmy (čísla, funkce, prostory, struktury, ...) lze redukovat na pojem množiny a v důkazech tvrzení o těchto pojmech lze vystačit s axiomy teorie množin. To znamená, že teorie množin je světem matematiky[1] v tom smyslu, že o veškeré matematice si můžeme myslet, že se děje uvnitř teorie množin. Říká se také, že matematika je nebo může být *formalizována* v teorii množin. Zajímavá otázka z hlediska logického i filozofického zní, zda roli metamatematiky, tj. roli teorie, která je světem matematiky, by nemohla nebo dokonce neměla hrát jiná teorie než ZF nebo GB, které jsou pro tento účel nejčastěji přijímány.

V knihách jako je tato, věnovaných logice, tedy teorie množin hraje dvojakou úlohu. Jako v každé jiné matematice je arbitrem, který určuje, co platí o zkoumaných objektech (což v případě logiky jsou struktury, axiomatické teorie, algoritmy, ...), a zároveň je jako jedna z řady axiomatických teorií předmětem zkoumání.

Rozmysleme si podrobně, že teorie ZF nemá žádné konečné modely. Nejprve si uvědomme, že struktura pro jazyk s jedním binárním predikátem je přesně to, čemu jsme v dřívějších kapitolách říkali orientovaný graf. Modely teorie ZF tvoří tedy podtřídu třídy všech orientovaných grafů. Dále si připomeňme, že acyklický graf je definován jako orientovaný graf neobsahující cykly a že je to takový graf, v němž z žádného vrcholu c nevede sled nenulové délky zpět do c. Postupujme sporem, předpokládejme, že $\mathbf{G} = \langle G, R \rangle$ je konečný model teorie ZF. Definujme dočasně, že vrchol d grafu $\mathbf{G}$ je *fundovaný*, jestliže d není v $\mathbf{G}$ dosažitelný z žádného vrcholu c

[1] Tento obrat známe od P. Vopěnky.

takového, že z c do c vede sled nenulové délky. Například v grafu **B** na str. 141 jsou vrcholy a a b fundované, zbývající vrcholy shodou okolností pojmenované c a d fundované nejsou. Protože v ZF lze dokázat sentenci existuje množina, která nemá žádné prvky, v našem grafu **G** existuje (alespoň jeden) vrchol, do kterého nevedou žádné hrany. Je zřejmé, že každý vrchol, do kterého nevedou hrany, je fundovaný, a dále je zřejmé, že existuje-li sled nenulové délky z c do c, pak c není fundovaný. Označme G_0 množinu všech fundovaných vrcholů grafu **G** a označme R_0 restrikci relace R na množinu G_0. Graf $\langle G_0, R_0\rangle$ je (neprázdný) acyklický podgraf grafu **G**. Lze dokázat (cvičení), že každý konečný acyklický graf má maximální vrchol, tj. vrchol, ze kterého nevedou žádné hrany. Označme c_0 (některý) maximální vrchol grafu $\langle G_0, R_0\rangle$. V grafu $\langle G_0, R_0\rangle$ z vrcholu c_0 nevedou hrany, v **G** mohou vést, ale jen do vrcholů, které nejsou fundované. Aplikujme axiom dvojice na $x := c_0$ a $y := c_0$. V grafu **G** k vrcholu c_0 existuje vrchol d, který v **G** splňuje formuli množina c_0 je jediným prvkem množiny d. Vrchol d je fundovaný, neboť kdyby existoval vrchol c, sled nenulové délky z c do c a sled z c do d, pak tento sled z c do d by nemohl minout vrchol c_0, a c_0 by nebyl fundovaný. Současně ale d není fundovaný, neboť z c_0 nevedou hrany do fundovaných vrcholů. Tím jsme dospěli ke sporu.

Na našem zdůvodnění, že teorie ZF nemá žádné konečné modely, je snad zajímavé také to, že jsme se v něm obešli bez většiny axiomů teorie ZF včetně axiomu extenzionality.

Čtenář by mohl namítnout, že existuje jednodušší postup, jak dokázat neexistenci konečných modelů teorie ZF: v ZF lze dokázat, že existují nekonečné množiny, musí to tedy platit v každém modelu; do prvku modelu, o kterém v takovém modelu platí, že je nekonečnou množinou, musí vést nekonečně mnoho hran, tj. musí do něj vést hrany z nekonečně mnoha různých vrcholů. Pokud by ale takovýto argument měl být bez dalšího přijat jako správný, proč nepřijmout i tento argument: v ZF lze dokázat i existenci nespočetných množin, a do vrcholu, o kterém v grafu $\langle G, R\rangle$ platí, že je nespočetnou množinou, musí vést nespočetně mnoho různých hran. Tento druhý argument ale rozhodně správný není, neboť má-li ZF jakékoliv modely, pak podle Löwenheimovy-Skolemovy věty má i spočetné modely.

Modelem teorie ZF je každý orientovaný graf, ve kterém platí všechny axiomy ZF, a takové modely existují, je-li ZF bezesporná teorie. V tom případě existují i spočetné (nutně nekonečné) modely ZF. Žádná přímá konstrukce modelu ZF není známa. K tomuto faktu se ještě vrátíme v souvislosti s Druhou Gödelovou větou o neúplnosti v kapitole 4. Tvrzení, že ZF má spočetné modely, je známo jako *Skolemův paradox*. Nic paradoxního na něm ale není. Je-li $a \in G$ a $\langle G, R\rangle \models \mathsf{ZF}$, může se stát, že množina všech vrcholů, ze kterých vede hrana do a, je spočetná, a přitom žádný prvek $f \in G$ nesplňuje v $\langle G, R\rangle$ formuli množina f je funkce, která prostě zobrazuje množinu a do množiny všech přirozených čísel. V tom případě vrchol a v grafu $\langle G, R\rangle$ splňuje formuli množina a je nespočetná.

Teorie komutativních těles má jazyk $\{+, \cdot, 0, 1\}$ se dvěma binárními funkčními symboly a se dvěma konstantami 0 a 1, a axiomy

R1: $\quad \forall x \forall y \forall z (x + (y + z) = (x + y) + z),$

R2: $\forall x \forall y (x + y = y + x)$,

R3: $\forall x (x + 0 = x)$,

R4: $\forall x \exists y (x + y = 0)$,

R5: $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$,

R6: $\forall x \forall y (x \cdot y = y \cdot x)$,

R7: $\forall x (x \cdot 1 = x)$,

R8: $\forall x (x \neq 0 \rightarrow \exists y (x \cdot y = 1))$,

R9: $\forall x \forall y \forall z (x \cdot (y + z) = x \cdot y + x \cdot z)$,

R10: $0 \neq 1$.

Objektům teorie komutativních těles říkejme *čísla*. Číslo y takové, že $x + y = 0$, nazýváme číslem *opačným* k x a číslo y takové, že $x \cdot y = 1$, nazýváme číslem *inverzním* k x. V teorii komutativních těles lze snadno dokázat, že číslo 0 je jediné číslo neutrální vůči sčítání a že číslo 1 je jediné číslo neutrální vůči násobení. To vyjadřují sentence (e) a (f) v následujícím lemmatu. Ze sentencí (a)–(c) snadno plyne, že ke každému x existuje jediné číslo opačné k x, ke každému nenulovému x existuje jediné číslo inverzní k x a žádné číslo není inverzní k nule.

Přestože v jazyce teorie komutativních těles nemáme symbol „S“ pro označení následnické funkce, můžeme v něm definovat *numerály* $\overline{0}$, $\overline{1}$, $\overline{2}$, ..., a to jako termy 0, $(0 + 1)$, $((0 + 1) + 1)$ atd. Například zápis $\overline{4}$ tedy v teorii komutativních těles označuje term $((((0 + 1) + 1) + 1) + 1)$.

Lemma 3.2.14 *Následující sentence (a)–(f) lze dokázat v teorii komutativních těles. Sentence (g) a (h) lze v teorii komutativních těles dokázat pro každou dvojici čísel n a m.*

(a) $\forall x \forall y \forall z (y + x = z + x \rightarrow y = z)$,
(b) $\forall x \forall y \forall z (x \neq 0 \ \& \ y \cdot x = z \cdot x \rightarrow y = z)$,
(c) $\forall x (x \cdot 0 = 0)$,
(d) $\forall x \forall y (x \cdot y = 0 \rightarrow x = 0 \vee y = 0)$,
(e) $\forall x (\forall v (v + x = v) \rightarrow x = 0)$,
(f) $\forall x (\forall v (v \cdot x = v) \rightarrow x = 1)$,
(g) $\overline{n} + \overline{m} = \overline{n + m}$,
(h) $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$.

Důkaz Důkazy sentencí (a)–(f) jsou známé z algebry. Připomeňme z nich pouze důkazy sentencí (a), (c) a (d), ostatní přenecháváme čtenáři:

Nechť čísla x, y a z jsou dána. Podle axiomu R4 existuje v takové, že $x + v = 0$. Nechť $y + x = z + x$. Užití tohoto předpokladu, dvojí užití axiomu R3 a dvojí užití axiomu R1 dává $y = y + 0 = y + (x + v) = (y + x) + v = (z + x) + v = z + (x + v) = z + 0 = z$.

Nechť x je dáno. Platí $0 + x \cdot 0 = x \cdot 0 + 0 = x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Již dokázané tvrzení (a) dává $0 = x \cdot 0$.

Nechť $x \cdot y = 0$. Z již dokázaného tvrzení (c) a axiomu R6 plyne $x \cdot y = 0 \cdot y$. Je-li $y \neq 0$, tvrzení (b) dává $x = 0$.

Existence důkazů sentencí (f) a (g) se snadno dokáže indukcí podle m. Protože $\overline{0}$, 0 a $\overline{n \cdot 0}$ jsou tytéž termy a také $\overline{n+0}$ a $\overline{n}$ jsou tytéž termy, sentenci $\overline{n}+\overline{0} = \overline{n+0}$ lze odvodit užitím axiomu R3 a sentenci $\overline{n}\cdot\overline{0} = \overline{0}$ lze odvodit z již dokázané sentence (d). Dále se snadno dokáže sentence $\overline{n}+\overline{m+1} = \overline{n+m+1}$, máme-li již důkaz sentence $\overline{n}+\overline{m} = \overline{n+m}$ a uvědomíme-li si, že $\overline{m+1}$ je týž term jako $(\overline{m}+1)$, a $\overline{n+m+1}$ je týž term jako $(\overline{n+m}+1)$. Podobně se dokáže $\overline{n}\cdot\overline{m+1} = \overline{n\cdot m}+\overline{n}$ užitím axiomů R9 a R7, máme-li již dokázáno $\overline{n}\cdot\overline{m} = \overline{n\cdot m}$. Rovnost $\overline{n\cdot m}+\overline{n} = \overline{n\cdot(m+1)}$ lze odvodit z již dokázané sentence (g). QED

V souladu s předchozími komentáři k větě o úplnosti jsme se v důkazu lemmatu 3.2.14 spokojili s neformálními důkazy. Připomeňme si, že formální důkaz podobné sentence jako je 3.2.14(e), totiž sentence každý levý neutrální prvek je roven každému pravému, jsme dříve také sestrojili.

Nadále budeme vypouštět nadbytečné závorky: místo $(x+y)+z$ nebo $x+(y+z)$ píšeme pouze $x+y+z$, místo $(x\cdot y)\cdot z$ nebo $x\cdot(y\cdot z)$ píšeme pouze $x\cdot y\cdot z$. Dále se domluvme, že t^n značí term $t\cdot t\cdot\ldots\cdot t$ s n výskyty (téhož) termu t. A konečně, násobení má přednost před sčítáním. Zápis $x^2+y\cdot z$ je tedy zkratka za $(x\cdot x)+(y\cdot z)$.

Lemma 3.2.15 *Nechť $t(x,y_1,\ldots,y_r)$ je term v jazyce teorie komutativních těles. Pak existuje číslo n a termy $s_0(\underline{y}),\ldots,s_n(\underline{y})$ neobsahující x takové, že rovnost*

$$\forall\underline{y}\forall x(t(x,\underline{y}) = s_0(\underline{y})\cdot x^n + s_1(\underline{y})\cdot x^{n-1} + \ldots + s_n(\underline{y}))$$

je dokazatelná v teorii komutativních těles.

Důkaz Indukcí podle složitosti termu t. Když t je konstanta 0 nebo 1 nebo některá z proměnných y_i, lze za n zvolit nulu a za s_0 zvolit t. Když t je proměnná x, zvolme $n=1$, za s_0 zvolme term 1 a za s_1 zvolme term 0.

Nechť t je tvaru $t_1(x,\underline{y})+t_2(x,\underline{y})$ a nechť pro term t_1 již máme číslo n_1 a termy $q_0(\underline{y}),\ldots,q_{n_1}(\underline{y})$ a pro term t_2 již máme číslo n_2 a termy $u_0(\underline{y}),\ldots,u_{n_2}(\underline{y})$. Lze předpokládat, že $n_1=n_2$, neboť tu z posloupností $q_0(\underline{y}),\ldots,q_{n_1}(\underline{y})$ a $u_0(\underline{y}),\ldots,u_{n_2}(\underline{y})$, která je kratší, můžeme doplnit nulami. K termu t volme $n=n_1$ (čili $n=n_2$) a pro $0\le i\le n_1$ volme $q_i(\underline{y})+u_i(\underline{y})$ za term $s_i(\underline{y})$.

Nechť t má tvar $t_1(x,\underline{y})\cdot t_2(x,\underline{y})$ a nechť pro t_1 a t_2 máme čísla n_1 a n_2 a termy $q_0(\underline{y}),\ldots,q_{n_1}(\underline{y})$ a $u_0(\underline{y}),\ldots,u_{n_2}(\underline{y})$ jako výše. Opět předpokládejme $n_1=n_2$. Volme $n=2n_1$, za termy $s_0(\underline{y}),\ldots,s_n(\underline{y})$ volme termy tvaru $\sum_{j=0}^{i} q_j(\underline{y})\cdot u_{i-j}(\underline{y})$, tj. termy

$$q_0\cdot u_0,\qquad q_0\cdot u_1+q_1\cdot u_0,\qquad q_0\cdot u_2+q_1\cdot u_1+q_2\cdot u_0,\qquad \ldots$$

Snadno lze ověřit, že rovnost $t(x,\underline{y}) = \sum_{i=0}^{2n_1}(\sum_{j=0}^{i} q_j(\underline{y})\cdot u_{i-j}(\underline{y}))\cdot x^i$ vyplývá z předpokladu $t_1(x,\underline{y}) = \sum_{i=0}^{n_1} q_i(\underline{y})\cdot x^i$ a z předpokladu $t_2(x,\underline{y}) = \sum_{i=0}^{n_2} u_i(\underline{y})\cdot x^i$. QED

Lemma 3.2.15 tvrdí, že zvolíme-li proměnnou x, můžeme se na libovolný term v jazyce komutativních těles dívat jako na polynom v x s koeficienty neobsahujícími x. V důkazu lemmatu 3.2.15 se uplatnily známé vědomosti o tom, že součet

polynomů se stupni n_1 a n_2 je polynom stupně $\max\{n_1, n_2\}$ a jejich součin je polynom stupně $n_1 + n_2$.

Modely teorie komutativních těles jsou ovšem všechna komutativní tělesa, a nic jiného. Snadno lze nalézt dvouprvkové komutativní těleso, ve kterém platí $1+1 = 0$. Sentence $\overline{2} \neq \overline{0}$ tedy není v teorii komutativních těles dokazatelná. Dalšími příklady modelů teorie komutativních těles jsou struktury $\langle \mathrm{Q}, +, \cdot, 0, 1\rangle$ a $\langle \mathrm{R}, +, \cdot, 0, 1\rangle$, kde Q a R jsou jako obvykle množiny všech racionálních resp. reálných čísel. V oddílu 3.5 přidáme k axiomům R1–R10 další axiomy R11–R16 týkající se uspořádání. Modelem výsledné teorie bude struktura $\langle \mathrm{R}, +, \cdot, 0, 1, <\rangle$, modelem ale nebude struktura $\langle \mathrm{Q}, +, \cdot, 0, 1, <\rangle$ a nebude jím ani žádná konečná struktura. K získání dalších informací o teorii s axiomy R1–R16 se uplatní úvahy ve směru, který naznačuje lemma 3.2.15, totiž úvahy o počtu kořenů polynomu stupně n a o jejich poloze.

V tomto oddílu jsme zjistili, že volba pravidel a (logických) axiomů kalkulu $\mathrm{HK_e}$ je zdůvodněná a oprávněná: v žádné teorii T nelze z jejích (vlastních, tj. mimologických) axiomů odvodit žádný nesprávný závěr, tj. závěr, který z T nevyplývá, a naopak lze odvodit každý správný závěr, tj. závěr, který vyplývá z T. Užitečným nástrojem, chceme-li se přesvědčit, že nějaký závěr je dokazatelný z určitých předpokladů, je neformální důkaz. Skutečné, tj. formální důkazy vyhovující definici kalkulu $\mathrm{HK_e}$, jsou užitečné do okamžiku, než dokážeme větu o úplnosti. Sestrojení formálního důkazu je užitečné také tehdy, chceme-li o něm tvrdit něco víc, třeba odpovědět na otázky o počtu nebo složitosti formulí, které se v něm vyskytují. Například díky důkazu sentence $\forall \underline{x} \exists y D_n(\underline{x}, y)$ v teorii neostrého lineárního uspořádání, který jsme sestrojili, můžeme tvrdit, že tato sentence má důkaz obsahující $\mathcal{O}(n^2)$ formulí. Složitost formulí vyskytujících se v nějakém důkazu bude jednou z otázek, kterými se budeme zabývat v příštím oddílu při úvahách o gentzenovském kalkulu pro predikátovou logiku. Chceme-li se ale pouze přesvědčit o existenci důkazu určitého závěru z určitých předpokladů a máme-li už větu o úplnosti, je neformální důkaz stejně dobrý jako formální.

V tomto oddílu jsme si dále ukázali několik příkladů axiomatických teorií. Viděli jsme, že teorie T může vzniknout například tak, že zvolíme nějakou strukturu $\mathbf{D}$ a za axiomy teorie T pak zvolíme některé ze sentencí platných v $\mathbf{D}$. Struktura $\mathbf{D}$ je pak jedním z modelů teorie T. I v případě, kdy T nevznikne takto, tj. vypozorováním axiomů z nějaké předem zvolené struktury (což je případ teorie množin), nic nám nebrání uvažovat o modelech teorie T.

Na začátku oddílu 3.1, když jsme poprvé mluvili o volbě jazyka, tj. o volbě mimologických symbolů, jsme řekli, že volbou jazyka je dáno, o čem se v dané teorii může mluvit. Na příkladech teorií z tohoto oddílu vidíme, že někdy lze v dané teorii mluvit opisně i o takových vlastnostech a operacích, kterým bezprostředně neodpovídají symboly zvoleného jazyka. Například v teorii LO lze mluvit o maximu objektů x a y, v teorii komutativních těles lze mluvit o kořenech polynomu s danými koeficienty. Dokonce ještě víc: pro každé n můžeme v teorii LO vyslovit (a dokázat) sentenci v každé n-tici objektů je některý z objektů maximální a v teorii komutativních těles bychom mohli vyslovit sentenci každý netriviální polynom stupně n má nejvýše n různých kořenů. To by opět byla pro každé n jiná sentence (delší pro větší n).

Není ale vidět, jak bychom v teorii komutativních těles mohli mluvit najednou o všech polynomech, a není také vidět, jak v teorii LO vyjádřit jednou sentencí, že každá konečná množina má maximální prvek. V oddílu 3.4 uvidíme, že existují metody, které dovolují dokázat, že určitá vlastnost struktury není v daném jazyce vyjádřitelná.

Pro některé teorie T můžeme snadno nalézt nezávislou sentenci, tj. sentenci, kterou v T nelze dokázat ani vyvrátit. Pro některé teorie, například pro teorii SUCC, nezávislou sentenci uvést nedokážeme. Také problémem, jak lze pro danou teorii T dokázat, že neexistuje sentence nezávislá na T, se v dalším výkladu, v oddílech 3.4 a 3.5, budeme zabývat. Oddíly 3.4 a 3.5 lze číst nezávisle na oddílu 3.3 a téměř nezávisle na sobě.

Cvičení

1. Zdůvodněte bez užití věty o úplnosti, že všechny formule z cvičení 2 předchozího oddílu jsou v kalkulu HK dokazatelné.

2. Zdůvodněte přímo, bez užití věty o úplnosti, dokazatelnost druhé formule z lemmatu 3.2.1.

3. Je-li x libovolná proměnná a φ formule dokazatelná v HK z množiny předpokladů Δ, pak i $\forall x\varphi$ je dokazatelná z Δ. Dokažte.

4. Uvažujte modifikovaný kalkulus HK$'$, který má místo pravidla Gen-E třetí axiomatické schéma

   B3: $\quad \exists x\varphi \equiv \neg\forall x\neg\varphi.$

   Dokažte, že kalkulus HK$'$ je ekvivalentní s kalkulem HK.

5. Uvažujte kalkulus HK$''$, který má místo pravidel Gen-A a Gen-E schéma B3, a dále axiom a pravidlo:

   B4: $\quad \forall x(\psi \to \varphi) \to (\psi \to \forall x\varphi),$ $\qquad$ pokud x není volně ve ψ,

   Gen: $\quad \varphi \,/\, \forall x\varphi.$

   Dokažte, že i kalkulus HK$''$ je ekvivalentní s kalkulem HK.

6. Ke každé predikátové formuli φ existuje důkaz v kalkulu HK, jehož délka je polynomiální ve $|\varphi|$ a který je důkazem formule $\varphi \equiv \varphi'$, kde φ' je v prenexním tvaru. Dokažte. Zdůvodněte, že přitom nezáleží na tom, zda délka $|\varphi|$ formule φ je definována jako souhrnný počet všech výskytů logických a predikátových symbolů ve φ, nebo jako počet *všech* symbolů ve φ (včetně funkčních symbolů a číslic v indexech proměnných).

7. Nalezněte příklad na to, že tvrzení 3.2.7(d) by neplatilo bez předpokladu, že φ je sentence.

8. Zdůvodněte, že v lemmatu 3.2.9 platí i opačná implikace: je-li sentence φ tautologickým důsledkem množiny $T \cup \mathrm{H}(L)$, pak $T \models \varphi$.

9. Zdůvodněte podrobně obě implikace v prvním odstavci důkazu věty 3.2.8.

10. Formulujte zobecnění definice substituovatelného termu pro simultánní substituci (tj. pro případ, kdy za n-tici proměnných se dosazuje n-tice termů). Dokažte bez užití věty o úplnosti, že jsou-li termy $t_1, .., t_n$ substituovatelné za proměnné $x_1, .., x_n$ ve formuli φ, pak formule $\varphi_{x_1,..,x_n}(t_1, .., t_n)$ je dokazatelná z předpokladu $\forall x_1 .. \forall x_n \varphi$.

    Návod. Užijte „nové“ proměnné tak, jak bylo naznačeno na začátku pododdílu 3.1.3.

11. Rozmyslete si, že lemma 3.2.7 platí i pro predikátovou logiku s rovností.

12. Zdůvodněte, že každá formule tvaru

$$\forall \underline{x} \forall \underline{y} (x_1 = y_1 \ \& \ .. \ \& \ x_n = y_n \ \to \ (\varphi(x_1, .., x_n) \ \equiv \ \varphi(y_1, .., y_n)))$$

    je dokazatelná v kalkulu $\mathrm{HK_e}$.

13. Dokažte, že kdybychom axiom E3 nahradili axiomem

    E3′: $\quad \forall x \forall y \forall z (x = y \ \& \ x = z \ \to \ y = z)$,

    mohli bychom axiom E2 vypustit.

14. Dokažte, že je-li schéma E5 myšleno tak, že se vztahuje na všechny predikátové symboly včetně rovnítka, pak lze vypustit i axiom E3′.

15. Zdůvodněte bez užití věty 3.2.12, že sentence

$$\forall x (L(x) \ \& \ \exists y R(y) \ \to \ \forall z (L(z) \ \to \ x = z))$$

    je v kalkulu $\mathrm{HK_e}$ dokazatelná z předpokladu $\forall x \forall y (L(x) \ \& \ R(y) \ \to \ x = y)$. Toto cvičení navazuje na jeden z našich příkladů formálních důkazů. Pokud $L(x)$ znamená objekt x je levý neutrální prvek a $R(y)$ znamená objekt y je pravý neutrální prvek, máte dokázat, že je-li každý levý neutrální objekt roven každému pravému neutrálnímu objektu a existují-li pravé neutrální objekty, pak existuje nejvýše jeden levý neutrální objekt.

16. Zdůvodněte bez užití věty 3.2.12, že sentence $\forall x \exists y (\mathrm{S}(y) \neq x)$ je v kalkulu $\mathrm{HK_e}$ dokazatelná z axiomu L1 teorie SUCC (bez užití zbývajících axiomů).

17. Nalezněte model teorie SUCC, který není izomorfní se strukturou $\langle \mathrm{N}, 0, \mathrm{s} \rangle$.

18. Dokažte, že žádný z axiomů Q1–Q3 není dokazatelný z ostatních axiomů teorie SUCC a že z Q1–Q3 a L1–Lm nelze dokázat žádnou sentenci Ln pro $n > m$.

19. Dokažte, že značí-li $x \leq y$ formuli $x < y \ \vee \ x = y$, pak všechny axiomy teorie neostrého lineárního uspořádání jsou dokazatelné v teorii LO.

20. Dokažte, že značí-li naopak $x < y$ formuli $x \leq y \ \& \ x \neq y$, pak všechny axiomy teorie LO jsou dokazatelné v teorii neostrého lineárního uspořádání.

21. Nechť teorie T má jazyk teorie množin a axiomy
$\forall x \forall y(\forall v(v \in x \equiv v \in y) \rightarrow x = y)$,
$\exists x \forall v \neg(v \in x)$,
$\forall x \forall y \exists z \forall v(v \in x \vee v = y \rightarrow v \in z)$.

    (a) Dokažte pomocí konečných modelů, že v T nelze dokázat žádnou ze sentencí $\forall x(x \notin x)$ a $\neg \exists x \forall v(v \in x)$.
    (b) Dokažte, že žádný ze tří axiomů teorie T není dokazatelný z ostatních dvou.

22. Dokažte, že každý konečný acyklický graf má vrchol, ze kterého nevedou žádné hrany.

    Návod. Postupujte indukcí podle počtu vrcholů grafu. V tomto případě se nepokoušejte sestavit formální důkaz.

23. Zdůvodněte, že existuje pouze jedno dvouprvkové komutativní těleso.

3.3 Gentzenovský predikátový kalkulus

Máme-li důkaz $\varphi_1, \ldots, \varphi_m$, kde φ_m je φ, formule φ z množiny předpokladů Σ v hilbertovském kalkulu HK, je dobře možné, že některé z formulí φ_i jsou mnohem delší nebo v nějakém smyslu složitější než kterákoliv formule z množiny $\Sigma \cup \{\varphi\}$. Jinými slovy, definice důkazu v hilbertovském kalkulu připouští, abychom při důkazu nějaké formule z nějaké množiny předpokladů postupovali oklikou, přes formule, které nemají „nic společného“ ani s dokazovanou formulí, ani s množinou předpokladů.

Uvědomme si, že ve výrokové variantě gentzenovského kalkulu GK, kterou jsme popsali v oddílu 1.4, je pravidlo řezu pravidlem, které umožňuje dokazovat oklikou: chceme-li dokázat sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$, máme právo vymyslet si libovolnou formuli θ, dokázat zvlášť sekventy $\langle\, \Gamma \Rightarrow \theta \,\rangle$ a $\langle\, \theta \Rightarrow \Delta \,\rangle$, a formuli θ pak odstranit užitím pravidla Cut.

V tomto oddílu stanovíme predikátovou variantu gentzenovského kalkulu GK a rozmyslíme si, že pravidlo Cut je v jistém smyslu jediným pravidlem, které při dokazování umožňuje postupovat oklikou. Pak se budeme zabývat větou o eliminovatelnosti řezů a některými jejími souvislostmi. Budeme tedy především řešit otázku, zda v definici důkazu je nutné připustit okliky.

Do *gentzenovského kalkulu GK* pro (klasickou) predikátovou logiku přijměme všechna pravidla uvedená na str. 41 s tím, že φ a ψ nyní označují predikátové formule a Γ atd. jsou množiny predikátových formulí. Dále přijměme čtyři kvantifikátorová pravidla:

$\exists$-r: $\quad \langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle \ / \ \langle\, \Gamma \Rightarrow \Delta, \exists x \varphi \,\rangle$,

$\forall$-l: $\quad \langle\, \Gamma, \varphi_x(t) \Rightarrow \Delta \,\rangle \ / \ \langle\, \Gamma, \forall x \varphi \Rightarrow \Delta \,\rangle$,

$\exists$-l: $\quad \langle\, \Gamma, \varphi_x(y) \Rightarrow \Delta \,\rangle \;/\; \langle\, \Gamma, \exists x\varphi \Rightarrow \Delta \,\rangle,$

$\forall$-r: $\quad \langle\, \Gamma \Rightarrow \Delta, \varphi_x(y) \,\rangle \;/\; \langle\, \Gamma \Rightarrow \Delta, \forall x\varphi \,\rangle,$

kde v případě pravidel $\exists$-r a $\forall$-l je term t substituovatelný za x ve φ a v případě pravidel $\exists$-l a $\forall$-r je proměnná y substituovatelná za x ve φ a nemá žádné volné výskyty v množině $\Gamma \cup \Delta \cup \{\exists x\varphi\}$ resp. v množině $\Gamma \cup \Delta \cup \{\forall x\varphi\}$. Výsledný kalkulus má tedy devět výrokových pravidel (pravidlo A a jedno „levé“ a jedno „pravé“ pravidlo pro každou ze čtyř logických spojek), čtyři kvantifikátorová pravidla a dále dvě strukturální pravidla W a Cut. Všimněme si, že u všech čtyř kvantifikátorových pravidel máme co dělat s dosazením za proměnnou a že dosazení vždy směřuje „proti směru úvahy“. Abychom ověřili, že formule $\forall x\varphi$ nebo $\exists x\varphi$ je správně odvozena ze vstupní formule ψ, musíme ověřit, že formuli ψ lze získat z formule φ (tj. z té formule, kterou získáme z principální formule odstraněním nejvnějšnějšího kvantifikátoru) dosazením za x (tj. za tu proměnnou, která je určena oním nejvnějšnějším kvantifikátorem). Například každý ze sekventů $\langle\, \Gamma \Rightarrow \Delta, \exists x(x < \mathrm{S}(v)) \,\rangle$ a $\langle\, \Gamma \Rightarrow \Delta, \exists x(\mathrm{S}(x) < x) \,\rangle$ je pomocí pravidla $\exists$-r správně odvozen ze sekventu $\langle\, \Gamma \Rightarrow \Delta, \mathrm{S}(\mathrm{S}(v)) < \mathrm{S}(v) \,\rangle$, a to bez ohledu na formule v $\Gamma \cup \Delta$. Viz též příklad 3.1.21.

Pravidlům $\exists$-l a $\forall$-r říkejme pravidla *generalizace*, pravidlům $\exists$-r a $\forall$-l říkejme pravidla *specifikace* (*konkretizace*). Pravidlo $\exists$-l je formalizací následujícího kroku v nějakém neformálním důkazu:

> ... Máme zdůvodnit, že platí Δ, přičemž víme, že existuje objekt s vlastností φ. Zvolme takový objekt a označme jej y. Stačí zdůvodnit, že Δ platí za předpokladu $\varphi_x(y)$.

Analogicky je pravidlo $\forall$-r formalizací takovéhoto kroku:

> ... Máme zdůvodnit, že všechny objekty mají vlastnost φ. Nechť je tedy dán nějaký objekt, označme jej y. Stačí zdůvodnit $\varphi_x(y)$.

Oba kroky jsou správné za předpokladu, že y zatím (v předchozí úvaze naznačené tečkami) nic neoznačuje. Tomu odpovídá podmínka u pravidel generalizace, že y se nevyskytuje volně v množinách Γ a Δ ani ve formuli $\exists x\varphi$ resp. $\forall x\varphi$. Tato podmínka bývá v literatuře označena německo-anglickým názvem *eigenvariable condition*. V našem textu jí říkejme *podmínka EVC*. Všimněme si ještě, že pravidla generalizace připouštějí, aby x a y byla tatáž proměnná. V tom případě se pravidla $\exists$-l a $\forall$-r podobají pravidlům Gen-E a Gen-A hilbertovského kalkulu a je automaticky splněno, že proměnná y nemá volné výskyty ve formuli $\exists x\varphi$ resp. $\forall x\varphi$.

Na obrázku 3.3.1 nahoře je příklad důkazu v kalkulu GK. Všimněme si na levé straně, že formule $\forall y P(y)$ byla odvozena z formule $P(v)$ až poté, kdy byl užitím pravidla $\exists$-l odstraněn druhý volný výskyt proměnné v (ve formuli $P(v) \to \forall y P(y)$). Použít pravidla $\forall$-l a $\exists$-l v opačném pořadí by nebylo možné, to by nebyla splněna podmínka EVC. Finální sekvent je odvozen užitím pravidla Cut. Také finální sekvent spodního důkazu je odvozen řezem. V tomto důkazu si všimněme, že u

$$\dfrac{\dfrac{\dfrac{\dfrac{\langle\, P(v) \;\Rightarrow\; P(v), \forall y P(y) \,\rangle}{\langle\, \Rightarrow\; P(v), P(v) \to \forall y P(y) \,\rangle}}{\langle\, \Rightarrow\; P(v), \exists x (P(x) \to \forall y P(y)) \,\rangle} \quad \dfrac{\dfrac{\langle\, \forall y P(y), P(z) \;\Rightarrow\; \forall y P(y) \,\rangle}{\langle\, \forall y P(y) \;\Rightarrow\; P(z) \to \forall y P(y) \,\rangle}}{\langle\, \forall y P(y) \;\Rightarrow\; \exists x (P(x) \to \forall y P(y)) \,\rangle}}{\langle\, \Rightarrow\; \forall y P(y), \exists x (P(x) \to \forall y P(y)) \,\rangle}}{\langle\, \Rightarrow\; \exists x (P(x) \to \forall y P(y)) \,\rangle}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\langle\, P(x) \,\&\, Q(x) \;\Rightarrow\; P(x) \,\&\, Q(x) \,\rangle}{\langle\, \forall y (P(x) \,\&\, Q(y)) \;\Rightarrow\; P(x) \,\&\, Q(x) \,\rangle}}{\langle\, \forall x \forall y (P(x) \,\&\, Q(y)) \;\Rightarrow\; P(x) \,\&\, Q(x) \,\rangle} \quad \dfrac{\dfrac{\langle\, P(y) \;\Rightarrow\; P(y) \,\rangle}{\langle\, P(y) \,\&\, Q(y) \;\Rightarrow\; P(y) \,\rangle}}{\langle\, \forall x (P(x) \,\&\, Q(x)) \;\Rightarrow\; P(y) \,\rangle}}{\langle\, \forall x \forall y (P(x) \,\&\, Q(y)) \;\Rightarrow\; \forall x (P(x) \,\&\, Q(x)) \,\rangle}}{\langle\, \forall x \forall y (P(x) \,\&\, Q(y)) \;\Rightarrow\; P(y) \,\rangle}$$

Obrázek 3.3.1: Příklady důkazu v kalkulu GK

pravidel specifikace nevadí, obsahuje-li term t proměnné, které jsou volné v ostatních formulích. Formule $\forall y(P(x) \,\&\, Q(y))$ v levé větvi důkazu je správně odvozena z formule $P(x) \,\&\, Q(x)$. V důkazu z obrázku 3.3.2 nahoře si všimněme, že pravidlo $\exists$-r je užito dvakrát, přičemž term t má v jednom případě tvar x a v druhém tvar $F(x)$. Principální formule $\exists x \varphi$ je ale v obou případech táž. Všimněme si také, že o formuli $\exists x(P(F(x)) \vee \neg P(x))$ již byla řeč ve cvičení 22 oddílu 3.1. Na tomtéž obrázku dole jsou ještě dva příklady důkazů. Útvar úplně vpravo důkazem není, neboť v prvním za dvou kroků je porušena podmínka EVC. Rozšíříme-li definici logicky platné formule i na sekventy, snadno užitím věty o korektnosti 3.3.1 dokážeme, že sekvent $\langle\, \exists x P(x) \;\Rightarrow\; \forall y P(y) \,\rangle$ nemá v kalkulu GK žádný důkaz.

Důkaz formule φ v kalkulu GK definujme jako důkaz sekventu $\langle\, \Rightarrow\; \varphi \,\rangle$. *Důkaz* formule φ *z množiny předpokladů* Σ definujme jako důkaz sekventu tvaru $\langle\, F \;\Rightarrow\; \varphi \,\rangle$, kde $F \subseteq \Sigma$ je konečná množina. Nechť zápis $\Sigma \vdash_{\mathrm{GK}} \varphi$ označuje, že formule φ je v kalkulu GK dokazatelná z množiny předpokladů Σ. Řekneme, že struktura $\mathbf{D}$ je *protipříklad* na sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$, jestliže existuje ohodnocení e proměnných ve struktuře $\mathbf{D}$, které v $\mathbf{D}$ splňuje všechny formule z Γ a nesplňuje žádnou formuli z Δ. Sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ *platí* ve struktuře $\mathbf{D}$, jestliže $\mathbf{D}$ není protipříklad na sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$, tj. jestliže pro každé ohodnocení proměnných e splňující v $\mathbf{D}$ všechny formule z Γ existuje formule $\psi \in \Delta$ taková, že $\mathbf{D} \models \psi[e]$. Sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je *logicky platný*, platí-li v každé struktuře (pro příslušný předem zvolený jazyk). Sekventy $\langle\, \exists x P(x) \;\Rightarrow\; \forall y P(y) \,\rangle$ a $\langle\, \Rightarrow\; \rangle$ jsou příklady sekventů, které nejsou logicky platné. Je zřejmé, že sekvent $\langle\, \Gamma \;\Rightarrow\; \varphi \,\rangle$ je logicky platný právě tehdy, platí-li $\Gamma \models \varphi$.

Věta 3.3.1 *Každý sekvent $\mathcal{S}$ dokazatelný v kalkulu GK je logicky platný. Když $\Sigma \vdash_{\mathrm{GK}} \varphi$, pak $\Sigma \models \varphi$.*

Důkaz Když je sekvent tvaru $\langle\, F \;\Rightarrow\; \varphi \,\rangle$ logicky platný, pak $F \models \varphi$. Když navíc $F \subseteq \Sigma$, pak i $\Sigma \models \varphi$. Stačí tedy dokázat první část věty. Nechť tedy $\mathcal{P}$ je důkaz

v kalkulu GK a nechť $\mathbf{D}$ je struktura. Ověříme indukcí dle počtu kroků v důkazu $\mathcal{P}$, že každý sekvent v důkazu $\mathcal{P}$ platí ve struktuře $\mathbf{D}$.

Ukažme si úvahu například pro pravidlo $\exists$-l. Všechny ostatní úvahy jsou analogické a ponecháváme je za cvičení. Nechť tedy sekvent $\langle\, \Gamma, \exists x\varphi \;\Rightarrow\; \Delta \,\rangle$ je užitím pravidla $\exists$-l odvozen ze sekventu $\langle\, \Gamma, \varphi_x(y) \;\Rightarrow\; \Delta \,\rangle$ a nechť e je ohodnocení proměnných ve struktuře $\mathbf{D}$, které v $\mathbf{D}$ splňuje všechny formule z množiny Γ a formuli $\exists x\varphi$. Pišme zkráceně $\mathbf{D} \models \Gamma[e]$ atd. Z podmínky $\mathbf{D} \models (\exists x\varphi)[e]$ plyne existence prvku $a \in D$ takového, že $\mathbf{D} \models \varphi[e(x/a)]$. Uvažujme ohodnocení $e(y/a)$ a předpokládejme složitější případ, kdy x a y jsou různé proměnné. Platí

$$\begin{aligned} \mathbf{D} \models \varphi[e(x/a)] &\Leftrightarrow \mathbf{D} \models (\varphi_x(y))_y(x)[e(x/a)] \\ &\Leftrightarrow \mathbf{D} \models \varphi_x(y)[e(x/a, y/a)] \\ &\Leftrightarrow \mathbf{D} \models \varphi_x(y)[e(y/a)]. \end{aligned}$$

Nemá-li proměnná volné výskyty ve formuli $\forall x\varphi$, a to nemá, formule $\varphi_x(y)$ obsahuje pouze takové výskyty proměnné y, které se v ní ocitly substitucí za proměnnou x, a $(\varphi_x(y))_y(x)$ a φ jsou tedy stejné formule. Tím je zdůvodněna první ze tří ekvivalencí. Druhá plyne z lemmatu 3.1.14(b), třetí z lemmatu 3.1.11(b). Ohodnocení $e(y/a)$ tedy splňuje všechny formule v antecedentu sekventu $\langle\, \Gamma, \varphi_x(y) \;\Rightarrow\; \Delta \,\rangle$. Protože podle indukčního předpokladu tento sekvent platí v $\mathbf{D}$, existuje formule ψ v množině Δ taková, že $\mathbf{D} \models \psi[e(y/a)]$. Proměnná y nemá volné výskyty ve formuli ψ. Tedy $\mathbf{D} \models \psi[e]$. QED

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\langle\, P(F(x)) \;\Rightarrow\; P(F(x)) \,\rangle}{\langle\, \Rightarrow\; P(F(x)), \neg P(F(x)) \,\rangle}}{\langle\, \Rightarrow\; P(F(x)) \vee \neg P(x), \neg P(F(x)) \,\rangle}}{\langle\, \Rightarrow\; \exists x(P(F(x)) \vee \neg P(x)), \neg P(F(x)) \,\rangle}}{\langle\, \Rightarrow\; \exists x(P(F(x)) \vee \neg P(x)), P(F(F(x))) \vee \neg P(F(x)) \,\rangle}}{\langle\, \Rightarrow\; \exists x(P(F(x)) \vee \neg P(x)) \,\rangle}$$

$$\dfrac{\dfrac{\langle\, P(x) \;\Rightarrow\; P(x) \,\rangle}{\langle \forall x P(x) \;\Rightarrow\; P(x) \,\rangle}}{\langle \forall x P(x) \;\Rightarrow\; \forall y P(y) \,\rangle} \qquad \dfrac{\dfrac{\langle\, P(x) \;\Rightarrow\; P(x) \,\rangle}{\langle \forall x P(x) \;\Rightarrow\; P(x) \,\rangle}}{\langle \forall x P(x) \;\Rightarrow\; \exists y P(y) \,\rangle} \qquad \dfrac{\dfrac{\langle\, P(x) \;\Rightarrow\; P(x) \,\rangle}{\langle \exists x P(x) \;\Rightarrow\; P(x) \,\rangle}}{\langle \exists x P(x) \;\Rightarrow\; \forall y P(y) \,\rangle}$$

Obrázek 3.3.2: Další důkazy (?) v kalkulu GK

Neuvádíme přímý důkaz věty o úplnosti kalkulu GK, a to přestože je — alespoň v případě jazyka bez funkčních symbolů — spíše jednodušší a názornější než důkaz věty o úplnosti kalkulu HK. Místo toho ukážeme, že kalkuly GK a HK jsou ekvivalentní a vzájemně polynomiálně simulovatelné. Z ekvivalence kalkulů GK a HK a úplnosti kalkulu HK ovšem plyne úplnost kalkulu GK.

Nejprve stanovme, jaké množiny předpokladů připouštíme, a rozšiřme definici polynomiální simulovatelnosti uvedenou v závěru oddílu 1.4. Kalkuly GK a HK nejsou ekvivalentní v nejobecnějším možném smyslu: platí $\{P(x)\} \vdash_{\mathrm{HK}} \forall x P(x)$, neplatí ale $\{P(x)\} \vdash_{\mathrm{GK}} \forall x P(x)$. Jako předpoklady tedy připusťme pouze sentence, tj. mluvme pouze o dokazatelnosti v (axiomatických) teoriích. Dále definujme, že kalkulus $\mathcal{C}_2$ *polynomiálně simuluje* kalkulus $\mathcal{C}_1$, jestliže existuje polynom p takový, že ke každému důkazu délky nejvýše n libovolné formule φ z libovolné teorie T v kalkulu $\mathcal{C}_1$ existuje důkaz délky nejvýše $p(n)$ téže formule z téže teorie v kalkulu $\mathcal{C}_2$. Délku formule φ, množiny formulí T, sekventu $\mathcal{S}$ či důkazu $\mathcal{P}$ značíme $|\varphi|$, $|T|$, $|\mathcal{S}|$ resp. $|\mathcal{P}|$ a definujeme ji jako souhrnný počet výskytů všech logických spojek, kvantifikátorů a predikátových symbolů v oné formuli, množině formulí, sekventu či důkazu. Atomické formule tedy mají délku 1. Lze si rozmyslet, že při podrobnějším počítání délek, například kdybychom brali v úvahu i funkční symboly a délku zápisu indexů proměnných, by se nic nepokazilo na polynomiální simulovatelnosti.

V kapitole 1 jsme vlastně uvažovali dvě varianty kalkulu HK: s důkazy-posloupnostmi a se stromovými důkazy. Lze říci, že posloupnost $\varphi_1, \ldots, \varphi_n$ je stromový důkaz v kalkulu HK, jestliže pro každé i existuje nejvýše jedno $j > i$ takové, že formule φ_j je z formule φ_i (a případně dalších formulí) odvozena jedním užitím nějakého pravidla. Také u kalkulu GK lze uvažovat dvě varianty: se stromovými důkazy a s důkazy-posloupnostmi (sekventů). Ve cvičeních oddílu 1.4 jsme se zmínili, že výroková varianta kalkulu HK s důkazy-posloupnostmi a výroková varianta kalkulu GK s důkazy-posloupnostmi jsou navzájem polynomiálně simulovatelné a že totéž platí pro kalkuly HK a GK se stromovými důkazy. Nyní uvidíme, že stejná tvrzení platí i pro predikátovou logiku. Ukážeme si také obtížnější výsledek, totiž že jak v kalkulu HK, tak v kalkulu GK lze důkazy-posloupnosti polynomiálně simulovat pomocí stromových důkazů. Po dokončení důkazu věty 3.3.2 budeme důkazy v kalkulu GK považovat za stromy.

Věta 3.3.2 *Následující kalkuly jsou navzájem polynomiálně simulovatelné:*
(i) Kalkulus HK s důkazy-posloupnostmi,
(ii) Kalkulus HK se stromovými důkazy,
(iii) Kalkulus GK s důkazy-posloupnostmi,
(iv) Kalkulus GK se stromovými důkazy,
(v) Kalkulus GK se stromovými důkazy a navíc s omezením, že jako principální formule iniciálních sekventů se připouštějí pouze atomické formule.

Důkaz Nejprve simulujme kalkulus (i) pomocí kalkulu (ii). Nechť $\varphi_1, \ldots, \varphi_m$, kde φ_m je φ, je daný důkaz délky nejvýše n formule φ z množiny sentencí T v kalkulu HK. Máme sestrojit důkaz téže formule z téže množiny předpokladů, který je stromový a jehož délka navíc není o mnoho větší než délka n daného důkazu $\varphi_1, \ldots, \varphi_m$. Definujme formuli $\forall\varphi_i$ jako univerzální uzávěr formule φ_i, tj. jako formuli $\forall v_1 \ldots \forall v_r \varphi_i$, kde $v_1, \ldots, v_r$ je seznam všech volných proměnných formule φ_i. Dále pro $1 \leq i \leq m$ definujme formuli θ_i jako konjunkci

$$((\ldots(\forall\varphi_1 \,\&\, \forall\varphi_2) \,\&\, \ldots) \,\&\, \forall\varphi_{i-1}) \,\&\, \forall\varphi_i.$$

Formule θ_i je tedy konjunkcí univerzálních uzávěrů formulí $\varphi_1, \ldots, \varphi_i$ s tím, že závorky se kumulují doleva. Mysleme si chvíli, že $i < m$ je pevné, a konstruujme stromový důkaz implikace $\theta_i \to \theta_{i+1}$. Předpokládejme například, že formule φ_{i+1} je v původním důkazu odvozena pravidlem MP, a to například z formule φ_1 a z formule φ_i, která má tvar $\varphi_1 \to \varphi_{i+1}$. Uvažujme formule

1: $\quad \forall\varphi_1 \,\&\, \forall(\varphi_1 \to \varphi_{i+1}) \to \forall\varphi_{i+1}$

2: $\quad \forall\varphi_1 \,\&\, \forall(\varphi_1 \to \varphi_{i+1}) \to (\forall\varphi_1 \,\&\, \forall\varphi_i) \,\&\, \forall\varphi_{i+1}$

3: $\quad (\forall\varphi_1 \,\&\, \forall\varphi_2) \,\&\, \forall\varphi_i \to ((\forall\varphi_1 \,\&\, \forall\varphi_2) \,\&\, \forall\varphi_i) \,\&\, \forall\varphi_{i+1}$

$\qquad\vdots$

i: $\quad (\ldots(\forall\varphi_1 \,\&\, \forall\varphi_2) \,\&\, \ldots) \,\&\, \forall\varphi_i \to ((\ldots(\forall\varphi_1 \,\&\, \forall\varphi_2) \,\&\, \ldots) \,\&\, \forall\varphi_i) \,\&\, \forall\varphi_{i+1}.$

Formule (2) a (3) mají tvar $A\&B\to(A\&B)\&C$ a $(A\&D)\&B\to((A\&D)\&B)\&C$. Formuli (3) tedy můžeme získat z formule (2) tak, že vezmeme (výrokový stromový) důkaz tautologie

$$(p \,\&\, q \to (p \,\&\, q) \,\&\, r) \to ((p \,\&\, s) \,\&\, q) \to ((p \,\&\, s) \,\&\, q) \,\&\, r), \qquad (*)$$

dosadíme do něj formule $\forall\varphi_1$, $\forall\varphi_i$, $\forall\varphi_{i+1}$ a $\forall\varphi_2$ za atomy p, q, r a s, a na finální formuli výsledného důkazu a na formuli (2) pak použijeme pravidlo MP. *Tentýž důkaz* tautologie $(*)$ použijeme ještě $(i-3)$-krát (k odvození formule (4) z formule (3) atd.), přičemž za p postupně dosazujeme formule $\forall\varphi_1 \,\&\, \forall\varphi_2$ až $\forall\varphi_1 \,\&\, \ldots \,\&\, \forall\varphi_{i-2}$, za s postupně dosazujeme formule $\forall\varphi_3$ až $\forall\varphi_{i-1}$, za q a r dosazujeme vždy tutéž formuli $\forall\varphi_i$ resp. $\forall\varphi_{i+1}$. Dosazením vznikne vždy fragment predikátového důkazu délky $\mathcal{O}(n)$. Celý důkaz formule v i-tém řádku, tj. formule $\theta_i \to \theta_{i+1}$, z formule (3) má tedy délku $\mathcal{O}(n^2)$. Vezmeme-li v úvahu i důkaz formule (2) z formule (1) a důkaz formule (1), pořád máme důkaz délky $\mathcal{O}(n^2)$. Kdyby ony dvě formule v daném důkazu, na které se aplikuje pravidlo MP, byly jiné než φ_1 a φ_i, kromě tautologie $(*)$ by se uplatnily ještě tautologie

$$(p \,\&\, q \to (p \,\&\, q) \,\&\, r) \to ((s \,\&\, p) \,\&\, q \to ((s \,\&\, p) \,\&\, q) \,\&\, r),$$
$$(p \,\&\, q \to (p \,\&\, q) \,\&\, r) \to ((p \,\&\, q) \,\&\, s \to ((p \,\&\, q) \,\&\, s) \,\&\, r).$$

Úvahy v případě, kdy φ_{i+1} je odvozena některým pravidlem generalizace, je logickým axiomem nebo je prvkem množiny předpokladů, jsou podobné. Z důkazů formulí θ_1, $\theta_1 \to \theta_2$ až $\theta_{m-1} \to \theta_m$, z nichž každý má délku $\mathcal{O}(n^2)$, můžeme sestavit stromový důkaz formule θ_m a pak i důkaz formule φ_m, jejichž délka je $\mathcal{O}(n^3)$.

Nyní simulujme kalkulus (iii) pomocí kalkulu (i). Nechť $\mathcal{P}$ je daný důkaz délky nejvýše n formule θ z množiny předpokladů T v kalkulu GK. Je-li $\mathcal{S}$ libovolný sekvent tvaru $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$, definujme formuli $f(\mathcal{S})$ následovně. Když $\Gamma \neq \emptyset$ a $\Delta \neq \emptyset$, pak $f(\mathcal{S})$ je $\bigwedge\Gamma \to \bigvee\Delta$. Když $\Gamma \neq \emptyset$ a $\Delta = \emptyset$, pak $f(\mathcal{S})$ je $\bigwedge\Gamma \to \bot$, kde $\bot$ je předem zvolená vyvratitelná sentence. Když $\Gamma = \emptyset$ a $\Delta \neq \emptyset$, pak $f(\mathcal{S})$ je $\bigvee\Delta$, a konečně když $\Gamma = \Delta = \emptyset$, pak $f(\mathcal{S})$ je $\bot$. Lze ověřit, že je-li sekvent $\mathcal{S}$ v důkazu $\mathcal{P}$ odvozen jedním krokem ze sekventu $\mathcal{S}_1$ nebo ze dvou sekventů $\mathcal{S}_1$ a $\mathcal{S}_2$, pak formuli $f(\mathcal{S})$ lze

v kalkulu HK odvodit z formule $f(\mathcal{S}_1)$ resp. z formulí $f(\mathcal{S}_1)$ a $f(\mathcal{S}_2)$ důkazem délky $\mathcal{O}((|\mathcal{S}_1|+|\mathcal{S}|)^2)$ resp. $\mathcal{O}((|\mathcal{S}_1|+|\mathcal{S}_2|+|\mathcal{S}|)^2)$. Uvažujme podrobněji třeba o případu, kdy $\Gamma \neq \emptyset$, $\Delta \neq \emptyset$, x a y jsou různé proměnné a sekvent $\mathcal{S}$ tvaru $\langle\, \Gamma \;\Rightarrow\; \Delta, \forall x \varphi \,\rangle$ je v důkazu $\mathcal{P}$ jedním krokem odvozen ze sekventu $\mathcal{S}_1$ tvaru $\langle\, \Gamma \;\Rightarrow\; \Delta, \varphi_x(y) \,\rangle$. V příslušném místě důkazu v kalkulu HK se uplatní formule

1: $\bigwedge \Gamma \to \bigvee \Delta \vee \varphi_x(y)$

2: $\bigwedge \Gamma \,\&\, \neg \bigvee \Delta \to \varphi_x(y)$

3: $\bigwedge \Gamma \,\&\, \neg \bigvee \Delta \to \forall y \varphi_x(y)$

4: $\forall y \varphi_x(y) \to \forall x \varphi$

5: $\bigwedge \Gamma \,\&\, \neg \bigvee \Delta \to \forall x \varphi$

6: $\bigwedge \Gamma \to \bigvee \Delta \vee \forall x \varphi$.

Přitom formule (3) je z formule (2) odvoditelná pomocí pravidla Gen-A a formule (4) je dokazatelná, neboť nemá-li y volné výskyty ve φ, pak $(\varphi_x(y))_y(x)$ je φ. Souhrnná délka těchto šesti formulí je $\mathcal{O}(|\mathcal{S}_1|+|\mathcal{S}_2|)$. Indukční předpoklad ale nezaručuje, že v disjunkci $\bigvee \Delta \vee \varphi_x(y)$ jsou závorky a pořadí členů tak, jak potřebujeme, s formulí $\varphi_x(y)$ vpravo na nejvyšší úrovni. Abychom formuli $\varphi_x(y)$ dostali na požadovanou pozici, můžeme potřebovat až $\mathcal{O}(|\mathcal{S}_1| + |\mathcal{S}|)$ formulí, jejichž délka je stále $\mathcal{O}(|\mathcal{S}_1| + |\mathcal{S}|)$. Také mezi formulemi (2) a (3) a mezi formulemi (5) a (6) je ve skutečnosti $\mathcal{O}(|\mathcal{S}_1| + |\mathcal{S}|)$ takových formulí. Máme tedy fragment důkazu, jehož velikost je $\mathcal{O}((|\mathcal{S}_1| + |\mathcal{S}|)^2)$. Celkově to vypadá tak, že původní důkaz $\mathcal{P}$ délky n byl rozdělen na fragmenty (v podstatě jednotlivé formule), z nichž každý se při překladu do kalkulu HK kvadraticky prodloužil. Dohromady to dává důkaz v kalkulu HK velikosti $\mathcal{O}(n^2)$. Finální sekvent důkazu $\mathcal{P}$ má tvar $\langle\, F \;\Rightarrow\; \theta \,\rangle$, kde $F \subseteq T$ je konečná. V kalkulu HK pokračujeme od formule $\bigwedge F \to \theta$ k formuli θ. Na odhadu $\mathcal{O}(n^2)$ se přitom již nic nezmění.

Uvažujme o simulaci kalkulu (ii) pomocí kalkulu (iv). Nechť $\theta_1, \ldots, \theta_m$, kde θ_m je θ, je daný stromový důkaz délky nejvýše n formule θ z teorie T v kalkulu HK. Nechť F je množina těch prvků množiny T, které jsou v důkazu $\theta_1, \ldots, \theta_m$ skutečně použity. Platí $|F| \leq n$. Konstruujme postupně důkazy sekventů $\langle\, F \;\Rightarrow\; \theta_i \,\rangle$ a všímejme si jejich délky. Důkaz sekventu $\langle\, F \;\Rightarrow\; \theta_m \,\rangle$ je hledaným důkazem formule θ v kalkulu GK. Když $\theta_i \in F$, pak $\langle\, F \;\Rightarrow\; \theta_i \,\rangle$ je iniciální sekvent. Když θ_i je logickým axiomem, například axiomem B1 tvaru $\forall x \varphi \to \varphi_x(t)$, pak sekvent $\langle\, F \;\Rightarrow\; \theta_i \,\rangle$ je dokazatelný dvěma kroky:

$$\dfrac{\dfrac{\langle\, F, \varphi_x(t) \;\Rightarrow\; \varphi_x(t) \,\rangle}{\langle\, F, \forall x \varphi \;\Rightarrow\; \varphi_x(t) \,\rangle}}{\langle\, F \;\Rightarrow\; \forall x \varphi \to \varphi_x(t) \,\rangle}.$$

Ostatní úvahy o logických axiomech kalkulu HK jsou podobné. Když formule θ_i je tvaru $\exists x \varphi \to \psi$ a je z některé předchozí formule θ_j tvaru $\varphi \to \psi$ odvozena generalizací,

pak v kalkulu GK můžeme utvořit takovýto důkaz:

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathcal{P}_j}{\langle\, F \;\Rightarrow\; \varphi \to \psi \,\rangle} \qquad \dfrac{\langle\, \varphi \;\Rightarrow\; \varphi \,\rangle \quad \langle\, \psi \;\Rightarrow\; \psi \,\rangle}{\langle\, \varphi, \varphi \to \psi \;\Rightarrow\; \psi \,\rangle}}{\langle\, F, \varphi \;\Rightarrow\; \psi \,\rangle}}{\langle\, F, \exists x \varphi \;\Rightarrow\; \psi \,\rangle}}{\langle\, F \;\Rightarrow\; \exists x \varphi \to \psi \,\rangle},$$

kde $\mathcal{P}_j$ je již sestrojený důkaz sekventu $\langle\, F \;\Rightarrow\; \theta_j \,\rangle$, sekvent $\langle\, F, \varphi \;\Rightarrow\; \psi \,\rangle$ je z předchozích dvou odvozen řezem, následující sekvent je (oprávněně) odvozen pomocí pravidla $\exists$-l a nakonec je užito pravidlo $\to$-r. Když je formule θ_i z některých předchozích formulí θ_j a θ_k, kde θ_k je tvaru $\theta_j \to \theta_i$, odvozena pravidlem MP, v kalkulu GK užijeme dva řezy:

$$\dfrac{\dfrac{\mathcal{P}_k}{\langle\, F \;\Rightarrow\; \theta_j \to \theta_i \,\rangle} \qquad \dfrac{\dfrac{\mathcal{P}_j}{\langle\, F \;\Rightarrow\; \theta_j \,\rangle} \qquad \dfrac{\langle\, \theta_j \;\Rightarrow\; \theta_j \,\rangle \quad \langle\, \theta_i \;\Rightarrow\; \theta_i \,\rangle}{\langle\, \theta_j, \theta_j \to \theta_i \;\Rightarrow\; \theta_i \,\rangle}}{\langle\, F, \theta_j \to \theta_i \;\Rightarrow\; \theta_i \,\rangle}}{\langle\, F \;\Rightarrow\; \theta_i \,\rangle}.$$

K již sestrojeným důkazům $\mathcal{P}_j$ a $\mathcal{P}_k$ jsme v tomto případě přidali pět nových sekventů. V předchozím případě, kdy jsme se zabývali simulací pravidla Gen-E, to bylo šest nových sekventů. Jejich celková délka je v obou případech $\mathcal{O}(n)$. Protože (přinejhorším) toto se děje pro každé i, máme důkaz v kalkulu GK délky $\mathcal{O}(n^2)$.

Nakonec simulujme kalkulus (iv) pomocí kalkulu (v). Tím bude důkaz dokončen, protože simulace (v) $\Rightarrow$ (iv) a (iv) $\Rightarrow$ (iii) jsou triviální, každý stromový důkaz s dodatečnou podmínkou na iniciální sekventy je stromovým důkazem a každý stromový důkaz je zároveň důkazem-posloupností. Lze dokázat indukcí dle $|\varphi|$, že každý sekvent $\mathcal{S}$ tvaru $\langle\, \Gamma, \varphi \;\Rightarrow\; \Delta, \varphi \,\rangle$ má důkaz, v němž jsou všechny iniciální sekventy atomické a v němž je nejvýše $4|\varphi| + 1$ sekventů, z nichž každý má délku $\mathcal{O}(|\mathcal{S}|)$. V případech, kdy φ je tvaru $\forall x \psi$ nebo $\psi \vee \chi$, postupujeme takto:

$$\dfrac{\dfrac{\langle\, \Gamma, \psi_x(y) \;\Rightarrow\; \Delta, \psi_x(y) \,\rangle}{\langle\, \Gamma, \forall x \psi \;\Rightarrow\; \Delta, \psi_x(y) \,\rangle}}{\langle\, \Gamma, \forall x \psi \;\Rightarrow\; \Delta, \forall x \psi \,\rangle} \qquad \dfrac{\dfrac{\langle\, \Gamma, \psi \;\Rightarrow\; \Delta, \psi \,\rangle}{\langle\, \Gamma, \psi \;\Rightarrow\; \Delta, \psi \vee \chi \,\rangle} \quad \dfrac{\langle\, \Gamma, \chi \;\Rightarrow\; \Delta, \chi \,\rangle}{\langle\, \Gamma, \chi \;\Rightarrow\; \Delta, \psi \vee \chi \,\rangle}}{\langle\, \Gamma, \psi \vee \chi \;\Rightarrow\; \Delta, \psi \vee \chi \,\rangle},$$

kde proměnnou y volíme tak, aby se nevyskytovala v Γ, Δ ani $\forall x \psi$. V prvním případě platí $|\psi_x(y)| = |\varphi| - 1$, sekvent $\langle\, \Gamma, \psi_x(y) \;\Rightarrow\; \Delta, \psi_x(y) \,\rangle$ má dle indukčního předpokladu důkaz se $4(|\varphi| - 1) + 1$ sekventy, a sekvent $\langle\, \Gamma, \varphi \;\Rightarrow\; \Delta, \varphi \,\rangle$ má tedy důkaz se $4(|\varphi| - 1) + 1 + 2 \leq 4|\varphi| + 1$ sekventy. V druhém případě pro délku a počet sekventů platí $|\psi \vee \chi| = |\psi| + |\chi| + 1$ a $(4|\psi| + 1) + (4|\chi| + 1) + 3 = 4|\psi \vee \chi| + 1$. Podobně se uvažuje v případě ostatních logických symbolů. Máme-li důkaz délky n

a nahradíme-li v něm každý iniciální sekvent $\mathcal{S}$, jehož principální formule není atomická, jeho důkazem délky $\mathcal{O}(|\mathcal{S}|^2)$, v němž principální formule všech iniciálních sekventů už jsou atomické, dostaneme důkaz délky $\mathcal{O}(n^2)$. QED

Tvrzení o polynomiální simulovatelnosti důkazů-posloupností pomocí stromových důkazů dokázal J. Krajíček. Důkaz, který jsme uvedli, je převzat z jeho knihy [50]. Vzájemná simulovatelnost (nikoliv polynomiální) kalkulů GK a HK je dokázána například v [49].

Řekneme, že důkaz v kalkulu GK je *bezřezový*, není-li v něm použito pravidlo Cut. V oddílu 1.4 jsme viděli, že v bezřezovém důkazu se mohou vyskytnout jen podformule formulí obsažených ve finálním sekventu daného důkazu. Něco podobného platí i v predikátové logice.

Následující rekurzí definujme vztah *býti s-podformulí* mezi predikátovými formulemi. S-podformulemi formule $\forall x\varphi$ (nebo formule $\exists x\varphi$) jsou jednak sama formule $\forall x\varphi$ (resp. $\exists x\varphi$), dále každá s-podformule kterékoliv formule tvaru $\varphi_x(t)$, kde t je term substituovatelný za x ve φ, a nic jiného. S-podformulemi formule $\varphi \to \psi$ (nebo formule $\varphi\&\psi$, nebo formule $\varphi\vee\psi$) jsou jednak sama formule $\varphi\to\psi$ (resp. $\varphi\&\psi$, resp. $\varphi \vee \psi$), dále každá s-podformule formule φ, každá s-podformule formule ψ, a nic jiného. S-podformulemi formule $\neg\varphi$ jsou jednak sama formule $\neg\varphi$ a dále každá s-podformule formule φ. Atomická formule je sama svou jedinou s-podformulí.

Příklad 3.3.3 Uvažujme jazyk $\{P, Q\}$ se dvěma unárními predikáty. Jedinými termy jsou v tomto případě proměnné. Uvažujme formuli $\forall x\forall y(P(x)\ \&\ Q(y))$. Termy substituovatelné za x ve formuli $\forall y(P(x)\,\&\,Q(y))$ jsou právě ty proměnné z, které jsou různé od proměnné y. S-podformulemi formule $\forall x\forall y(P(x)\ \&\ Q(y))$ jsou tedy, kromě ní samé, formule $\forall y(P(z)\ \&\ Q(y))$, $P(z)\ \&\ Q(v)$, $P(z)$ a $Q(v)$, kde proměnná z je jiná než y (může to být x) a proměnná v je libovolná.

Věta 3.3.4 *Každá formule v bezřezovém důkazu $\mathcal{P}$ je s-podformulí některé formule ve finálním sekventu důkazu $\mathcal{P}$. Není-li v bezřezovém důkazu $\mathcal{P}$ užito žádné z pravidel pro implikaci a negaci, pak každá formule obsažená v antecedentu (sukcedentu) kteréhokoliv sekventu důkazu $\mathcal{P}$ je s-podformulí některé formule obsažené v antecedentu (sukcedentu) finálního sekventu důkazu $\mathcal{P}$.*

Důkaz Je-li například sekvent $\langle\, \Gamma \Rightarrow \Delta, \varphi \to \psi \,\rangle$ odvozen jedním krokem ze sekventu $\langle\, \Gamma, \varphi \Rightarrow \Delta, \psi \,\rangle$, pak formule φ a ψ jsou s-podformulemi formule $\varphi \to \psi$ a každá formule v $\Gamma \cup \Delta$ je svou vlastní s-podformulí, tedy s-podformulí některé formule v sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \to \psi \,\rangle$. Podobně lze prověřit všechna ostatní pravidla kalkulu GK kromě pravidla Cut (které je vyloučené). QED

Příklad 3.3.5 Nechť $\mathcal{S}$ je sekvent $\langle\, \forall x\forall y(P(x)\&Q(y)) \Rightarrow P(y) \,\rangle$ a nechť $\mathcal{P}$ je jeho bezřezový důkaz. Protože ve finálním sekventu důkazu $\mathcal{P}$ se nevyskytují symboly $\to$ a $\neg$, v $\mathcal{P}$ není užito žádné z pravidel pro implikaci a negaci. Můžeme tedy užít druhou část věty 3.3.4. Uvažujme (kterýkoliv) iniciální sekvent $\langle\, \Gamma, \varphi \Rightarrow \Delta, \varphi \,\rangle$ důkazu $\mathcal{P}$. Formule φ musí být s-podformulí některé formule v sukcedentu a současně

s-podformulí některé formule v antecedentu sekventu $\mathcal{S}$. Formule $P(y)$ je jedinou s-podformulí (jediné) formule obsažené v sukcedentu sekventu $\mathcal{S}$. V příkladu 3.3.3 jsme ale zjistili, že formule $P(y)$ není s-podformulí žádné formule obsažené v antecedentu sekventu $\mathcal{S}$. Tím jsme dokázali, že sekvent $\mathcal{S}$ nemá žádný bezřezový důkaz. Připomeňme, že důkaz sekventu $\mathcal{S}$, který není bezřezový, je na obr. 3.3.1 dole.

Příklad 3.3.6 Sekvent $\langle \Rightarrow \rangle$ nemá žádný bezřezový důkaz.

O sekventu $\langle \Rightarrow \rangle$ ovšem víme, že nemá žádný důkaz (protože není logicky platný). Zajímavé ale je, že neexistenci bezřezových důkazů jsme v příkladech 3.3.5 a 3.3.6 dokázali bez užití jakékoliv sémantiky.

Definujme, že *formule* je *regulární*, jestliže žádná proměnná v ní nemá současně volné i vázané výskyty. Definujme dále, že *sekvent* je *regulární*, jestliže žádná proměnná v něm nemá současně volné i vázané výskyty. *Důkaz* $\mathcal{P}$ v kalkulu GK je *regulární*, jestliže žádná proměnná nemá v $\mathcal{P}$ současně volné i vázané výskyty a jestliže navíc pro každý sekvent $\langle \Gamma \Rightarrow \Delta, \forall x\varphi \rangle$ a $\langle \Gamma, \exists x\varphi \Rightarrow \Delta \rangle$ důkazu $\mathcal{P}$, který je v $\mathcal{P}$ odvozen jedním krokem z bezprostředně předchozího sekventu $\langle \Gamma \Rightarrow \Delta, \varphi_x(y) \rangle$ resp. $\langle \Gamma, \varphi_x(y) \Rightarrow \Delta \rangle$, platí, že proměnná y se v $\mathcal{P}$ nevyskytuje nikde mimo příslušný podstrom důkazu $\mathcal{P}$, tj. nikde kromě sekventů, do kterých vede v $\mathcal{P}$ cesta (nahoru) z onoho sekventu $\langle \Gamma \Rightarrow \Delta, \forall x\varphi \rangle$ či $\langle \Gamma, \exists x\varphi \Rightarrow \Delta \rangle$. Například důkaz na obrázku 3.3.1 nahoře je regulární. Na obrázku 3.3.2 jsou celkem tři důkazy, z nichž žádný není regulární. Jsou to ale důkazy regulárních sekventů. Na obrázku 3.3.1 dole je dokázán sekvent, který není regulární. Postupně chceme dospět k větě o eliminovatelnosti řezů pro kalkulus GK, která tvrdí, že každý regulární sekvent dokazatelný v kalkulu GK má v kalkulu GK i bezřezový důkaz.

Definujme *hloubku* $\mathrm{d}(\varphi)$ formule φ jako délku nejdelší větve ve formuli φ chápané jako strom. Jinak řečeno, $\mathrm{d}(\varphi \bowtie \psi) = 1 + \max\{\mathrm{d}(\varphi), \mathrm{d}(\psi)\}$, kde $\bowtie$ je kterákoliv ze spojek $\rightarrow$, $\&$ nebo $\vee$, dále $\mathrm{d}(\neg\varphi) = 1 + \mathrm{d}(\varphi)$ a konečně $\mathrm{d}(\varphi) = 0$, je-li φ atomická. Dále definujme *hloubku* $\mathrm{d}(\mathcal{P})$ důkazu $\mathcal{P}$ jako délku nejdelší větve v $\mathcal{P}$. Například na obrázku 3.3.1 nahoře je důkazem hloubky 4 dokázána formule, jejíž hloubka je 3. A konečně definujme *(řezovou) hodnost* $\mathrm{r}(\mathcal{P})$ (anglicky *cut rank*) důkazu $\mathcal{P}$ jako maximální z čísel $1 + \mathrm{d}(\varphi)$, kde φ je formule, na kterou je v důkazu $\mathcal{P}$ užit řez, a jako nulu v případě, kdy důkaz $\mathcal{P}$ je bezřezový. Podmínka $\mathrm{r}(\mathcal{P}) = 0$ tedy platí právě tehdy, není-li v $\mathcal{P}$ užito pravidlo Cut. Důkazy na obrázcích 3.3.1 mají hodnost 2 a 3. Důkaz na obrázku 3.3.2 nahoře má hodnost 0.

Lemma 3.3.7 *Ke každému důkazu regulárního sekventu existuje regulární důkaz téhož sekventu, který nemá větší hloubku ani hodnost.*

Důkaz Nechť $\mathcal{P}$ je daný důkaz regulárního sekventu $\mathcal{S}$. Nechť $x_1, \ldots, x_n$ je seznam těch proměnných, které mají volné výskyty v sekventu $\mathcal{S}$ a současně mají vázané výskyty kdekoliv v důkazu $\mathcal{P}$. Zvolme navzájem různé proměnné $v_1, \ldots, v_n$, které se v $\mathcal{P}$ nevyskytují (volně ani vázaně). Pišme v $\mathcal{P}$ všude $v_1, \ldots, v_n$ místo vázaných výskytů proměnných $x_1, \ldots, x_n$, a označme $\mathcal{P}^{(1)}$ výsledek této záměny. Probráním všech pravidel kalkulu GK lze ověřit, že $\mathcal{P}^{(1)}$ je opět důkazem. Například je-li v $\mathcal{P}$

užit krok $\langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle \;/\; \langle\, \Gamma \Rightarrow \Delta, \exists x\varphi \,\rangle$, na odpovídajícím místě v $\mathcal{P}^{(1)}$ je krok tvaru $\langle\, \Gamma^{(1)} \Rightarrow \Delta^{(1)}, (\varphi_x(t))^{(1)} \,\rangle \;/\; \langle\, \Gamma^{(1)} \Rightarrow \Delta^{(1)}, (\exists x\varphi)^{(1)} \,\rangle$. Je-li x některá z proměnných x_i, platí $(\exists x\varphi)^{(1)} = \exists v_i(\varphi_x(v_i))^{(1)}$ a $(\varphi_x(t))^{(1)} = ((\varphi_x(v_i))^{(1)})_{v_i}(t)$. Není-li, platí $(\exists x\varphi)^{(1)} = \exists x\varphi^{(1)}$ a $(\varphi_x(t))^{(1)} = (\varphi^{(1)})_x(t)$. V obou případech máme v $\mathcal{P}^{(1)}$ legální krok, tj. krok v souladu s pravidlem $\exists$-r. Protože finální sekvent $\mathcal{S}$ důkazu $\mathcal{P}$ je regulární, $\mathcal{P}^{(1)}$ je důkazem téhož sekventu $\mathcal{S}$.

Označme dále $x_{n+1}, .., x_{n+m}$ proměnné, které se v důkazu $\mathcal{P}^{(1)}$ vyskytují současně volně i vázaně. Vzhledem k již provedeným úpravám (kterými jsme důkaz $\mathcal{P}$ přepracovali na důkaz $\mathcal{P}^{(1)}$) žádná z těchto proměnných nemá volné výskyty v sekventu $\mathcal{S}$. Může tam ale mít vázané výskyty. Opět zvolme navzájem různé proměnné $v_{n+1}, .., v_{n+m}$, které se nevyskytují v $\mathcal{P}^{(1)}$, a pišme v $\mathcal{P}^{(1)}$ všude $v_{n+1}, .., v_{n+m}$ místo volných výskytů proměnných $x_{n+1}, .., x_{n+m}$. Opět lze probíráním všech pravidel kalkulu GK ověřit, že výsledek $\mathcal{P}^{(2)}$ této záměny je důkazem, a to důkazem stále téhož sekventu $\mathcal{S}$.

Nechť v důkazu $\mathcal{P}^{(2)}$ je právě r-krát použito některé z pravidel generalizace, a to na proměnné $y_1, .., y_r$ (tentokrát ne nutně různé). Zvolme navzájem různé proměnné $z_1, .., z_r$ nevyskytující se v důkazu $\mathcal{P}^{(2)}$. Pro $1 \leq i \leq r$ označme $\mathcal{P}_i$ ten podstrom důkazu $\mathcal{P}^{(2)}$, v jehož posledním kroku je generalizována proměnná y_i, a označme $\mathcal{S}_i$ finální sekvent důkazu $\mathcal{P}_i$. Zvolme takové j, že sekvent $\mathcal{S}_j$ je v důkazu $\mathcal{P}^{(2)}$ maximální, tj. takové, že důkaz $\mathcal{P}_j$ neobsahuje jako podstrom žádný z ostatních důkazů $\mathcal{P}_i$ pro $i \neq j$. Všude v $\mathcal{P}_j$ pišme z_j místo y_j. Všechny kroky uvnitř podstromu $\mathcal{P}_j$ zůstanou legální díky důvodům, které byly naznačeny v předchozím odstavci. Podmínka EVC (viz str. 183) zaručuje, že proměnná y_j nemá volné výskyty v sekventu $\mathcal{S}_j$. Se sekventem $\mathcal{S}_j$ se tedy nic neděje. Všechny kroky v důkazu $\mathcal{P}^{(2)}$ mimo podstrom $\mathcal{P}_j$, včetně onoho, který je aplikován na sekvent $\mathcal{S}_j$, zůstávají, jak byly, tedy legální. Popsaný postup opakujme s ostatními podstromy $\mathcal{P}_i$ s tím, že pro záměnu proměnných volíme vždy ten z nich, jehož finální sekvent je maximální z dosud neuvažovaných. Výsledkem je regulární důkaz $\mathcal{P}^{(3)}$ původního sekventu. Důkaz $\mathcal{P}^{(3)}$ nemá větší (má stejnou) hloubku a hodnost. QED

Lemma 3.3.8 (o substituci) *Nechť $\mathcal{P}$ je důkaz, nechť z je proměnná, která v důkazu $\mathcal{P}$ není generalizována, nechť s je term, jehož žádná proměnná není v důkazu $\mathcal{P}$ generalizována ani kvantifikována. Pak $\mathcal{P}_z(s)$, výsledek substituce termu s za všechny volné výskyty proměnné z v důkazu $\mathcal{P}$, je opět důkazem.*

Důkaz Plný důkaz lze provést pečlivým probráním všech pravidel kalkulu GK. Ponecháváme jej za cvičení, uvádíme ale hlavní myšlenky. Není-li žádná proměnná termu s v důkazu $\mathcal{P}$ kvantifikována, pak term s je v každé formuli důkazu $\mathcal{P}$ substituovatelný za z. Pravidla generalizace umožňují generalizovat proměnné, nikoliv termy. Na tom se ale nic nepokazí, neboť term s nedosazujeme za proměnnou, která je kdekoliv v důkazu $\mathcal{P}$ generalizována. Protože žádná proměnná termu s není v důkazu $\mathcal{P}$ generalizována, substituce termu s nezanese nežádoucí volné proměnné do žádného místa, kde je v $\mathcal{P}$ použito pravidlo generalizace, tj. nikde nepokazí platnost podmínky EVC. QED

Lemma 3.3.9 (o oslabení) *Nechť $\mathcal{P}$ je důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ a nechť Π a Λ jsou množiny formulí takové, že žádná proměnná, která má volný výskyt v některé formuli v $\Pi \cup \Lambda$, není v důkazu $\mathcal{P}$ generalizována. Pak přidáním všech formulí z množiny Π do všech antecedentů a přidáním všech formulí z množiny Λ do všech sukcedentů vznikne opět důkaz.*

Důkaz je zřejmý.

Pravidlem &-r lze odvodit sekvent $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle$ ze sekventů $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$ a $\langle\, \Gamma \Rightarrow \Delta, \psi \,\rangle$. Myslitelné a korektní by bylo i opačné pravidlo, které by dovolilo odvodit například sekvent $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$ ze sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle$. Do kalkulu GK ale takové pravidlo z dobrých důvodů nebylo přijato. Jednak by přestala platit věta 3.3.4 a jednak takové pravidlo ani není potřeba. Máme-li totiž důkaz $\mathcal{P}$ sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle$, snadno z něj utvoříme důkaz $\mathcal{P}'$ sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$:

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{P}\\ \vdots\\ \langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle\end{array} \qquad \dfrac{\langle\, \varphi \Rightarrow \varphi \,\rangle}{\langle\, \varphi \,\&\, \psi \Rightarrow \varphi \,\rangle}}{\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle.}}$$

Přitom takto sestrojený důkaz $\mathcal{P}'$ má větší hloubku než důkaz $\mathcal{P}$ a jeho hodnost $\max\{\mathrm{r}(\mathcal{P}), 1 + \mathrm{d}(\varphi \,\&\, \psi)\}$ také může být větší. Následující lemma, lemma o inverzi, tvrdí, že existuje jiný důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$, který nemá větší hloubku ani hodnost, a že podobným způsobem lze „obrátit“ všechna ostatní pravidla kalkulu GK s výjimkou pravidel specifikace. Cvičení 22 oddílu 3.2 ukazuje, že je-li sekvent tvaru $\langle\, \Gamma \Rightarrow \Delta, \exists x \varphi \,\rangle$ dokazatelný, nemusí to znamenat dokazatelnost žádného sekventu tvaru $\langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle$. Pro pravidla specifikace lemma o inverzi neplatí. E

Domluvme se, že nadále nepřipouštíme, aby principální formule iniciálních sekventů byly neatomické. Kalkulem GK tedy nadále rozumíme kalkulus z bodu (d) věty 3.3.2. E

Lemma 3.3.10 (o inverzi) *(a) Má-li kterýkoliv sekvent v levém sloupci následující tabulky regulární důkaz $\mathcal{P}$, pak (každý) sekvent v tomtéž řádku vpravo má důkaz, jehož hloubka a hodnost není větší než hloubka a hodnost důkazu $\mathcal{P}$:*

$\langle\, \Gamma \Rightarrow \Delta, \varphi \to \psi \,\rangle$	$\langle\, \Gamma, \varphi \Rightarrow \Delta, \psi \,\rangle$
$\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle$	$\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle, \langle\, \Gamma \Rightarrow \Delta, \psi \,\rangle$
$\langle\, \Gamma \Rightarrow \Delta, \varphi \vee \psi \,\rangle$	$\langle\, \Gamma \Rightarrow \Delta, \varphi, \psi \,\rangle$
$\langle\, \Gamma \Rightarrow \Delta, \neg\varphi \,\rangle$	$\langle\, \Gamma, \varphi \Rightarrow \Delta \,\rangle$
$\langle\, \Gamma, \varphi \to \psi \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle, \langle\, \Gamma, \psi \Rightarrow \Delta \,\rangle$
$\langle\, \Gamma, \varphi \,\&\, \psi \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma, \varphi, \psi \Rightarrow \Delta \,\rangle$
$\langle\, \Gamma, \varphi \vee \psi \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma, \varphi \Rightarrow \Delta \,\rangle, \langle\, \Gamma, \psi \Rightarrow \Delta \,\rangle$
$\langle\, \Gamma, \neg\varphi \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$.

(b) Nechť $\mathcal{P}$ je regulární důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \forall x \varphi \,\rangle$ nebo $\langle\, \Gamma, \exists x \varphi \Rightarrow \Delta \,\rangle$ a nechť žádná proměnná vyskytující se v termu t není v důkazu $\mathcal{P}$ kvantifikována ani generalizována. Pak sekvent $\langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle$ resp. $\langle\, \Gamma, \varphi_x(t) \Rightarrow \Delta \,\rangle$ má důkaz, jehož hloubka a hodnost není větší než hloubka a hodnost důkazu $\mathcal{P}$.

Důkaz V tvrzení (a) uvažujme například o druhém řádku. Máme tedy regulární důkaz $\mathcal{P}$ sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle$ a chceme získat důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$, který nemá větší hloubku ani hodnost. Postupujme indukcí dle hloubky důkazu $\mathcal{P}$. Platí-li $\varphi \,\&\, \psi \in \Delta$, pak sekvent $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$ lze ze sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle$ získat pouhým přidáním formule φ do sukcedentu. Protože důkaz $\mathcal{P}$ je regulární, žádná proměnná volná ve formuli φ není v $\mathcal{P}$ generalizována. Lemma 3.3.9 v tomto případě zaručuje, že přidáním formule φ do sukcedentů všech sekventů důkazu $\mathcal{P}$ vznikne důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$. Přidání formule φ do všech sukcedentů ovšem nezvýší hloubku ani hodnost. Nadále tedy předpokládejme, že $\varphi \,\&\, \psi \notin \Delta$.

Rozlišme případy, kdy formule $\varphi \,\&\, \psi$ je a kdy není principální formulí v posledním kroku důkazu $\mathcal{P}$. Přitom počítejme s tím, že je-li principální, může současně být také postranní. Nechť tedy formule $\varphi \,\&\, \psi$ není principální v posledním kroku důkazu $\mathcal{P}$. Důkaz $\mathcal{P}$ tedy může mít tvar například

$$\dfrac{\begin{array}{c}\mathcal{P}_1\\ \vdots\\ \langle\, \Pi, \Sigma_1 \Rightarrow \Lambda, \Omega_1 \,\rangle\end{array}}{\langle\, \Pi, \Sigma \Rightarrow \Lambda, \Omega \,\rangle,}$$

kde Π a Λ jsou množiny postranních formulí, $\Sigma \cup \Omega$ je množina všech principálních formulí (takže jedna z množin Σ a Ω je prázdná a druhá je jednoprvková), $\Sigma_1 \cup \Omega_1$ je množina všech vstupních formulí (takže každá z nich je nejvýše jednoprvková) a platí $\mathrm{d}(\mathcal{P}_1) < \mathrm{d}(\mathcal{P})$. Musí platit $\Gamma = \Pi \cup \Sigma$ a $\Delta \cup \{\varphi \,\&\, \psi\} = \Lambda \cup \Omega$. Protože formule $\varphi \,\&\, \psi$ není principální, máme $\varphi \,\&\, \psi \notin \Omega$ a $\varphi \,\&\, \psi \in \Lambda$. Indukční předpoklad užitý na důkaz $\mathcal{P}_1$ dává důkaz $\mathcal{P}_1'$ sekventu $\langle\, \Pi, \Sigma_1 \Rightarrow \Lambda - \{\varphi \,\&\, \psi\}, \varphi, \Omega_1 \,\rangle$, pro který platí $\mathrm{d}(\mathcal{P}_1') \leq \mathrm{d}(\mathcal{P}_1) = \mathrm{d}(\mathcal{P}) - 1$ a $\mathrm{r}(\mathcal{P}_1') \leq \mathrm{r}(\mathcal{P}_1) = \mathrm{r}(\mathcal{P})$. Pak

$$\dfrac{\begin{array}{c}\mathcal{P}_1'\\ \vdots\\ \langle\, \Pi, \Sigma_1 \Rightarrow \Lambda - \{\varphi \,\&\, \psi\}, \varphi, \Omega_1 \,\rangle\end{array}}{\langle\, \Pi, \Sigma \Rightarrow \Lambda - \{\varphi \,\&\, \psi\}, \varphi, \Omega \,\rangle}$$

je požadovaný důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle$. V případech, kdy v posledním kroku důkazu $\mathcal{P}$ je užito pravidlo se dvěma předpoklady nebo kdy v posledním (a jediném) kroku je užito pravidlo A, se uvažuje naprosto analogicky.

Nechť nyní formule $\varphi \& \psi$ je principální v posledním kroku důkazu $\mathcal{P}$. Je-li posledním krokem důkazu $\mathcal{P}$ užití pravidla W, můžeme jednoduše opět užít pravidlo W s tím, že jím přidáme formuli φ místo formule $\varphi \,\&\, \psi$. Protože jsme se domluvili, že

jako principální formule iniciálních sekventů připouštíme pouze atomické formule, zbývá pouze případ, kdy v posledním kroku důkazu $\mathcal{P}$ je formule $\varphi \,\&\, \psi$ odvozena pravidlem &-r. Protože $\varphi \,\&\, \psi \notin \Delta$, množinou postranních formulí v sukcedentu je množina Δ nebo množina $\Delta \cup \{\varphi \,\&\, \psi\}$, a důkaz $\mathcal{P}$ má podle toho jeden z tvarů

$$\dfrac{\begin{array}{cc}\mathcal{P}_1 & \mathcal{P}_2 \\ \langle\, \Gamma \Rightarrow \Delta, \varphi \,\rangle & \langle\, \Gamma \Rightarrow \Delta, \psi \,\rangle\end{array}}{\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle,} \qquad \dfrac{\begin{array}{cc}\mathcal{P}_1 & \mathcal{P}_2 \\ \langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi, \varphi \,\rangle & \langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi, \psi \,\rangle\end{array}}{\langle\, \Gamma \Rightarrow \Delta, \varphi \,\&\, \psi \,\rangle.}$$

V prvním případě je $\mathcal{P}_1$ hledaný důkaz, v druhém případě užijme indukční předpoklad na důkaz $\mathcal{P}_1$ a nahraďme formuli $\varphi \,\&\, \psi$ v jeho finálním sekventu formulí φ.

K tvrzení (b) poznamenejme, že term t je substituovatelný za x ve formuli φ, a dále postupujme podobně jako v (a). Nechť $\mathcal{P}$ je důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \forall x\varphi \,\rangle$. Není-li formule $\forall x\varphi$ principální formulí v posledním kroku důkazu $\mathcal{P}$, užijme indukční předpoklad na sekvent nebo sekventy vstupující do posledního kroku, tj. nahraďme v množině postranních formulí formuli $\forall x\varphi$ formulí $\varphi_x(t)$, a pak proveďme poslední krok tak, jak byl. Formule $\varphi_x(t)$ může oproti formuli $\forall x\varphi$ obsahovat navíc nějaké volné proměnné, nikoliv ale takové, které jsou v důkazu $\mathcal{P}$ generalizovány. To znamená, že poslední krok důkazu $\mathcal{P}$ zůstane legálním krokem i v případě, je-li užitím pravidla generalizace. Je-li formule $\forall x\varphi$ principální a současně postranní v posledním kroku důkazu $\mathcal{P}$, pak důkaz $\mathcal{P}$ má tvar

$$\dfrac{\begin{array}{c}\mathcal{P}_1 \\ \langle\, \Gamma \Rightarrow \Delta, \forall x\varphi, \varphi_x(y) \,\rangle\end{array}}{\langle\, \Gamma \Rightarrow \Delta, \forall x\varphi \,\rangle,}$$

kde důkaz $\mathcal{P}_1$ je regulární. Lemma 3.3.8 dovoluje dosadit term t za proměnnou y. Výsledný důkaz $(\mathcal{P}_1)_y(t)$ sekventu $\langle\, \Gamma \Rightarrow \Delta, \forall x\varphi, \varphi_x(t) \,\rangle$ má hloubku menší než důkaz $\mathcal{P}$, je regulární a žádná proměnná termu t v něm není generalizována ani kvantifikována. Indukční předpoklad dává požadovaný důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle$. QED

Lemma 3.3.11 (o redukci) *Nechť $\mathcal{P}_1$ je důkaz sekventu $\langle\, \Gamma \Rightarrow \Delta, \theta \,\rangle$, nechť $\mathcal{P}_2$ je důkaz sekventu $\langle\, \Pi, \theta \Rightarrow \Lambda \,\rangle$ a nechť následující důkaz $\mathcal{P}_0$:*

$$\dfrac{\begin{array}{cc}\mathcal{P}_1 & \mathcal{P}_2 \\ \langle\, \Gamma \Rightarrow \Delta, \theta \,\rangle & \langle\, \Pi, \theta \Rightarrow \Lambda \,\rangle\end{array}}{\langle\, \Gamma, \Pi \Rightarrow \Delta, \Lambda \,\rangle}$$

(v jehož posledním kroku je užito pravidlo Cut na formuli θ) je regulární. Nechť dále platí $\mathrm{r}(\mathcal{P}_1) \leq \mathrm{d}(\theta)$ a $\mathrm{r}(\mathcal{P}_2) \leq \mathrm{d}(\theta)$. Pak sekvent $\langle\, \Gamma, \Pi \Rightarrow \Delta, \Lambda \,\rangle$ má důkaz hodnosti nejvýše $\mathrm{d}(\theta)$ a hloubky nejvýše $\mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2)$.

Důkaz Nejprve poznamenejme, že důkaz $\mathcal{P}_0$ není hledaným důkazem, neboť pro jeho hodnost platí $\mathrm{r}(\mathcal{P}_0) = 1 + \mathrm{d}(\theta)$. Můžeme předpokládat $\theta \notin \Delta$ a $\theta \notin \Pi$, jinak bychom mohli důkaz sekventu $\langle\, \Gamma, \Pi \;\Rightarrow\; \Delta, \Lambda \,\rangle$ získat přidáním formulí do všech sekventů důkazu $\mathcal{P}_1$ nebo do všech sekventů důkazu $\mathcal{P}_2$, tj. užitím lemmatu 3.3.9. Postupujme indukcí podle $\mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2)$, tj. podle součtu hloubek obou daných důkazů. Rozebereme řadu různých případů.

Nechť alespoň jeden z důkazů $\mathcal{P}_1$ a $\mathcal{P}_2$ je takový, že má nenulovou hloubku a formule θ není principální v jeho posledním kroku. Nechť tímto důkazem je například $\mathcal{P}_2$. Předpokládejme například, že poslední krok důkazu $\mathcal{P}_2$ je $\vee$-l, přičemž principální formule je $\varphi \vee \psi$. Množinu levých postranních formulí v posledním kroku důkazu $\mathcal{P}_2$ můžeme psát ve tvaru $\Sigma \cup \{\theta\}$, kde $\theta \notin \Sigma$. Důkaz $\mathcal{P}_2$ má tedy tvar

$$\dfrac{\begin{array}{cc}\mathcal{P}_3 & \mathcal{P}_4 \\ \langle\, \Sigma, \theta, \varphi \;\Rightarrow\; \Lambda \,\rangle & \langle\, \Sigma, \theta, \psi \;\Rightarrow\; \Lambda \,\rangle\end{array}}{\langle\, \Sigma, \theta, \varphi \vee \psi \;\Rightarrow\; \Lambda \,\rangle,}$$

kde $\Sigma \cup \{\theta, \varphi \vee \psi\} = \Pi \cup \{\theta\}$. Platí $\mathrm{d}(\mathcal{P}_3) < \mathrm{d}(\mathcal{P}_2)$ a $\mathrm{d}(\mathcal{P}_4) < \mathrm{d}(\mathcal{P}_2)$. To znamená, že lze užít indukční předpoklad na dvojice $[\mathcal{P}_1, \mathcal{P}_3]$ a $[\mathcal{P}_1, \mathcal{P}_4]$. Existuje tedy důkaz $\mathcal{P}'_3$ sekventu $\langle\, \Gamma, \Sigma, \varphi \;\Rightarrow\; \Delta, \Lambda \,\rangle$ a důkaz $\mathcal{P}'_4$ sekventu $\langle\, \Gamma, \Sigma, \psi \;\Rightarrow\; \Delta, \Lambda \,\rangle$, pro které platí

$$\begin{aligned}\mathrm{d}(\mathcal{P}'_3) &\leq \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_3) < \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2),\\ \mathrm{d}(\mathcal{P}'_4) &\leq \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_4) < \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2).\end{aligned}$$

Přitom $\mathrm{r}(\mathcal{P}'_3) \leq \mathrm{d}(\theta)$ a $\mathrm{r}(\mathcal{P}'_4) \leq \mathrm{d}(\theta)$. Pak ale

$$\dfrac{\begin{array}{cc}\mathcal{P}'_3 & \mathcal{P}'_4 \\ \langle\, \Gamma, \Sigma, \varphi \;\Rightarrow\; \Delta, \Lambda \,\rangle & \langle\, \Gamma, \Sigma, \psi \;\Rightarrow\; \Delta, \Lambda \,\rangle\end{array}}{\langle\, \Gamma, \Sigma, \varphi \vee \psi \;\Rightarrow\; \Delta, \Lambda \,\rangle}$$

je hledaný důkaz hloubky nejvýše $\mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2)$ a hodnosti nejvýše $\mathrm{d}(\theta)$, neboť z $\theta \notin \Pi$, $\theta \notin \Sigma$, z rovnosti $\Sigma \cup \{\theta, \varphi \vee \psi\} = \Pi \cup \{\theta\}$ a z faktu, že $\varphi \vee \psi$ a θ jsou různé formule, plyne $\Sigma \cup \{\varphi \vee \psi\} = \Pi$.

Nechť alespoň jeden z důkazů $\mathcal{P}_1$ a $\mathcal{P}_2$ má nulovou hloubku. Nechť je to například $\mathcal{P}_1$. Pak platí $\Gamma \cap \Delta \neq \emptyset$ nebo $\theta \in \Gamma$. Když $\theta \in \Gamma$, pak sekvent $\langle\, \Gamma, \Pi \;\Rightarrow\; \Delta, \Lambda \,\rangle$ lze získat ze sekventu $\langle\, \Pi, \theta \;\Rightarrow\; \Lambda \,\rangle$ přidáním jistých formulí, a regularita důkazu $\mathcal{P}_0$ a lemma 3.3.9 zaručují, že přidáním těchže formulí do všech sekventů důkazu $\mathcal{P}_2$ vznikne důkaz $\mathcal{P}$ splňující $\mathrm{d}(\mathcal{P}) = \mathrm{d}(\mathcal{P}_2) = \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2)$ a $\mathrm{r}(\mathcal{P}) = \mathrm{r}(\mathcal{P}_2)$. Když $\Gamma \cap \Delta \neq \emptyset$, pak sekvent $\langle\, \Gamma, \Pi \;\Rightarrow\; \Delta, \Lambda \,\rangle$ je iniciální. Má tedy bezřezový důkaz hloubky nula.

Podobně jako v předchozím odstavci lze uvažovat i v případě, kdy formule θ je alespoň v jednom z důkazů $\mathcal{P}_1$ a $\mathcal{P}_2$ principální formulí pravidla W. Nadále tedy

předpokládejme, že oba důkazy $\mathcal{P}_1$ a $\mathcal{P}_2$ mají nenulovou hloubku a že formule θ je v obou z nich principální formulí posledního kroku. V tom případě nemůže být formule θ atomickou formulí. Uvažujme, jaký může mít tvar.

Nechť θ je tvaru $\varphi \to \psi$. Jak v posledním kroku důkazu $\mathcal{P}_1$, tak v posledním kroku důkazu $\mathcal{P}_2$ může nebo nemusí být formule θ zároveň postranní formulí. Předpokládejme, že v obou důkazech je postranní formulí — úvahy v ostatních případech jsou podobné, jen jednodušší. Důkazy $\mathcal{P}_1$ a $\mathcal{P}_2$ mají tedy tvar

$$\dfrac{\begin{array}{c}\mathcal{P}_3\\ \langle\, \Gamma, \varphi \;\Rightarrow\; \Delta, \varphi \to \psi, \psi \,\rangle\end{array}}{\langle\, \Gamma \;\Rightarrow\; \Delta, \varphi \to \psi \,\rangle,} \qquad \dfrac{\begin{array}{c}\mathcal{P}_4\\ \langle\, \Pi_1, \varphi \to \psi \;\Rightarrow\; \Lambda_1, \varphi \,\rangle\end{array} \quad \begin{array}{c}\mathcal{P}_5\\ \langle\, \Pi_2, \varphi \to \psi, \psi \;\Rightarrow\; \Lambda_2 \,\rangle\end{array}}{\langle\, \Pi, \varphi \to \psi \;\Rightarrow\; \Lambda \,\rangle,}$$

přičemž důkaz $\mathcal{P}_3$ má hloubku $\mathrm{d}(\mathcal{P}_1) - 1$, důkazy $\mathcal{P}_4$ a $\mathcal{P}_5$ mají hloubku nejvýše $\mathrm{d}(\mathcal{P}_2) - 1$, všechny tři důkazy mají hodnost nejvýše $\mathrm{d}(\theta)$ a $\Pi_1 \cup \Pi_2 = \Pi$ a $\Lambda_1 \cup \Lambda_2 = \Lambda$. Protože θ je $\varphi \to \psi$, platí také $\mathrm{d}(\varphi) < \mathrm{d}(\theta)$ a $\mathrm{d}(\psi) < \mathrm{d}(\theta)$. Užijme lemma 3.3.10 na sekvent $\langle\, \Gamma, \varphi \;\Rightarrow\; \Delta, \varphi \to \psi, \psi \,\rangle$ a na formuli $\varphi \to \psi$. Existuje důkaz $\mathcal{P}'_3$ sekventu $\langle\, \Gamma, \varphi \;\Rightarrow\; \Delta, \psi \,\rangle$, jehož hloubka je nejvýše $\mathrm{d}(\mathcal{P}_1) - 1$ a jehož hodnost je nejvýše $\mathrm{d}(\theta)$. Ze stejného důvodu existuje důkaz $\mathcal{P}'_4$ sekventu $\langle\, \Pi_1 \;\Rightarrow\; \Lambda_1, \varphi \,\rangle$ a důkaz $\mathcal{P}'_5$ sekventu $\langle\, \Pi_2, \psi \;\Rightarrow\; \Lambda_2 \,\rangle$, přičemž oba tyto důkazy mají hloubku nejvýše $\mathrm{d}(\mathcal{P}_2) - 1$ a hodnost nejvýše $\mathrm{d}(\theta)$. Utvořme z důkazů $\mathcal{P}'_3$ až $\mathcal{P}'_5$ a dvojího užití pravidla řezu důkaz $\mathcal{P}$:

$$\dfrac{\begin{array}{c}\mathcal{P}'_4\\ \langle\, \Pi_1 \;\Rightarrow\; \Lambda_1, \varphi \,\rangle\end{array} \qquad \dfrac{\begin{array}{c}\mathcal{P}'_3\\ \langle\, \Gamma, \varphi \;\Rightarrow\; \Delta, \psi \,\rangle\end{array} \quad \begin{array}{c}\mathcal{P}'_5\\ \langle\, \Pi_2, \psi \;\Rightarrow\; \Lambda_2 \,\rangle\end{array}}{\langle\, \Gamma, \Pi_2, \varphi \;\Rightarrow\; \Delta, \Lambda_2 \,\rangle}}{\langle\, \Gamma, \Pi \;\Rightarrow\; \Delta, \Lambda \,\rangle.}$$

Pro hloubku a hodnost důkazu $\mathcal{P}$ platí

$$\begin{aligned}\mathrm{d}(\mathcal{P}) &\leq 1 + \max\{\mathrm{d}(\mathcal{P}_2) - 1, 1 + \max\{\mathrm{d}(\mathcal{P}_1) - 1, \mathrm{d}(\mathcal{P}_2) - 1\}\} \leq \\ &\leq 1 + \max\{\mathrm{d}(\mathcal{P}_1), \mathrm{d}(\mathcal{P}_2)\}, \\ \mathrm{r}(\mathcal{P}) &\leq \max\{\mathrm{d}(\theta), 1 + \mathrm{d}(\varphi), 1 + \mathrm{d}(\psi)\} = \mathrm{d}(\theta).\end{aligned}$$

Platí $1 + \max\{\mathrm{d}(\mathcal{P}_1), \mathrm{d}(\mathcal{P}_2)\} \leq \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2)$, protože oba důkazy $\mathcal{P}_1$ a $\mathcal{P}_2$ mají nenulovou hloubku. Důkaz $\mathcal{P}$ je tedy hledaným důkazem.

Nechť formule θ je tvaru $\forall x \varphi$. Máme důkazy tvaru

$$\dfrac{\begin{array}{c}\mathcal{P}_1\\ \langle\, \Gamma \;\Rightarrow\; \Delta, \forall x \varphi \,\rangle,\end{array}} \qquad \dfrac{\begin{array}{c}\mathcal{P}_3\\ \langle\, \Pi, \forall x \varphi, \varphi_x(t) \;\Rightarrow\; \Lambda \,\rangle\end{array}}{\langle\, \Pi, \forall x \varphi \;\Rightarrow\; \Lambda \,\rangle,}$$

kde $\mathrm{d}(\mathcal{P}_3) = \mathrm{d}(\mathcal{P}_2) - 1$ a $\mathrm{r}(\mathcal{P}_3) \leq \mathrm{d}(\theta)$. Přitom opět předpokládáme složitější případ, kdy formule $\forall x\varphi$, která je principální v posledním kroku důkazu $\mathcal{P}_2$, je v tomto kroku zároveň postranní formulí. Protože důkaz $\mathcal{P}_0$ je regulární, žádná proměnná vyskytující se v termu t není generalizována ani kvantifikována v důkazu $\mathcal{P}_1$. Dle lemmatu 3.3.10(b) existuje důkaz $\mathcal{P}_1'$ sekventu $\langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle$ splňující podmínky $\mathrm{d}(\mathcal{P}_1') \leq \mathrm{d}(\mathcal{P}_1)$ a $\mathrm{r}(\mathcal{P}_1') \leq \mathrm{r}(\mathcal{P}_1)$. Důkaz $\mathcal{P}_1'$ na chvíli odložme a vzpomeňme si, že dokazujeme indukcí podle $\mathrm{d}(\mathcal{P}_1)+\mathrm{d}(\mathcal{P}_2)$. Protože $\mathrm{d}(\mathcal{P}_1)+\mathrm{d}(\mathcal{P}_3) = \mathrm{d}(\mathcal{P}_1)+\mathrm{d}(\mathcal{P}_2)-1$, můžeme užít indukční předpoklad na důkazy $\mathcal{P}_1$ a $\mathcal{P}_3$ a na formuli $\forall x\varphi$: existuje důkaz $\mathcal{P}_4$ sekventu $\langle\, \Gamma, \Pi, \varphi_x(t) \Rightarrow \Delta, \Lambda \,\rangle$, jehož hloubka je nejvýše $\mathrm{d}(\mathcal{P}_1)+\mathrm{d}(\mathcal{P}_2)-1$ a jehož hodnost je nejvýše $\mathrm{d}(\theta)$. Užití řezu na formuli $\varphi_x(t)$:

$$\dfrac{\begin{array}{cc}\mathcal{P}_1' & \mathcal{P}_4 \\ \langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle & \langle\, \Gamma, \Pi, \varphi_x(t) \Rightarrow \Delta, \Lambda \,\rangle\end{array}}{\langle\, \Gamma, \Pi \Rightarrow \Delta, \Lambda \,\rangle}$$

dává důkaz $\mathcal{P}$, pro jehož hloubku a hodnost platí

$$\begin{aligned}\mathrm{d}(\mathcal{P}) &\leq 1 + \max\{\mathrm{d}(\mathcal{P}_1), \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2) - 1\} = \mathrm{d}(\mathcal{P}_1) + \mathrm{d}(\mathcal{P}_2),\\ \mathrm{r}(\mathcal{P}) &\leq \max\{\mathrm{d}(\theta), 1 + \mathrm{d}(\varphi_x(t))\} = \mathrm{d}(\theta).\end{aligned}$$

Důkaz $\mathcal{P}$ je tedy hledaným důkazem.

Zbývající případy, kdy formule θ je tvaru $\varphi\&\psi$, $\varphi\vee\psi$, $\neg\varphi$ nebo $\exists x\varphi$, jsou analogické probraným a ponecháváme je za cvičení. QED

Lemma 3.3.12 *Nechť $\mathcal{P}$ je regulární důkaz nenulové hodnosti. Pak existuje důkaz $\mathcal{P}'$ téhož sekventu, pro který platí $\mathrm{r}(\mathcal{P}') < \mathrm{r}(\mathcal{P})$ a $\mathrm{d}(\mathcal{P}') \leq 2^{\mathrm{d}(\mathcal{P})}$.*

Důkaz Postupujme indukcí podle hloubky důkazu $\mathcal{P}$. Maximální hloubka kterékoliv formule, na niž je v důkazu $\mathcal{P}$ užit řez, je $\mathrm{r}(\mathcal{P}) - 1$. Označme $\mathcal{S}$ finální sekvent důkazu $\mathcal{P}$. Sekvent $\mathcal{S}$ je krokem tvaru $\mathcal{S}_1 \,/\, \mathcal{S}$ odvozen ze sekventu $\mathcal{S}_1$, který je finálním sekventem důkazu $\mathcal{P}_1$, nebo je krokem tvaru $\mathcal{S}_1, \mathcal{S}_2 \,/\, \mathcal{S}$ odvozen ze sekventů $\mathcal{S}_1$ a $\mathcal{S}_2$, které jsou finálními sekventy důkazů $\mathcal{P}_1$ a $\mathcal{P}_2$. Bez újmy na obecnosti předpokládejme druhý případ. Každý z důkazů $\mathcal{P}_1$ a $\mathcal{P}_2$ má hloubku nejvýše $\mathrm{d}(\mathcal{P}) - 1$. Dle indukčního předpokladu existují důkazy $\mathcal{P}_1'$ a $\mathcal{P}_2'$ sekventů $\mathcal{S}_1$ a $\mathcal{S}_2$ splňující podmínky $\mathrm{r}(\mathcal{P}_1') < \mathrm{r}(\mathcal{P})$, $\mathrm{r}(\mathcal{P}_2') < \mathrm{r}(\mathcal{P})$, $\mathrm{d}(\mathcal{P}_1') \leq 2^{\mathrm{d}(\mathcal{P})-1}$, $\mathrm{d}(\mathcal{P}_2') \leq 2^{\mathrm{d}(\mathcal{P})-1}$. Označme $\mathcal{P}_0$ důkaz, který vznikne z důkazů $\mathcal{P}_1'$ a $\mathcal{P}_2'$ provedením téhož kroku, kterým končí důkaz $\mathcal{P}$, tj. kterým je v důkazu $\mathcal{P}$ odvozen sekvent $\mathcal{S}$. Je-li tímto posledním krokem důkazu $\mathcal{P}$ řez na formuli hloubky menší než $\mathrm{r}(\mathcal{P}) - 1$, nebo není-li to řez, je důkaz $\mathcal{P}_0$ hledaným důkazem $\mathcal{P}'$, neboť pro jeho hodnost a hloubku platí $\mathrm{r}(\mathcal{P}_0) < \mathrm{r}(\mathcal{P})$ a $\mathrm{d}(\mathcal{P}_0) = 1 + \max\{\mathrm{d}(\mathcal{P}_1'), \mathrm{d}(\mathcal{P}_2')\} \leq 1 + 2^{\mathrm{d}(\mathcal{P})-1} \leq 2^{\mathrm{d}(\mathcal{P})}$.

Předpokládejme tedy, že posledním krokem důkazu $\mathcal{P}$ (a tedy i důkazu $\mathcal{P}_0$) je řez na formuli θ, která má maximální možnou hloubku $\mathrm{r}(\mathcal{P}) - 1$. V tom případě platí

$\mathrm{r}(\mathcal{P}'_1) \leq \mathrm{d}(\theta)$ a $\mathrm{r}(\mathcal{P}'_2) \leq \mathrm{d}(\theta)$. Protože důkaz $\mathcal{P}$ je regulární, $\mathcal{S}$ je regulární sekvent. Díky lemmatu 3.3.7 tedy můžeme předpokládat, že důkaz $\mathcal{P}_0$ je regulární. Dle lemmatu 3.3.11 existuje důkaz $\mathcal{P}'$ sekventu $\mathcal{S}$, pro jehož hloubku a hodnost platí $\mathrm{r}(\mathcal{P}') \leq \mathrm{d}(\theta) = \mathrm{r}(\mathcal{P}) - 1$ a $\mathrm{d}(\mathcal{P}') \leq \mathrm{d}(\mathcal{P}'_1) + \mathrm{d}(\mathcal{P}'_2) \leq 2^{\mathrm{d}(\mathcal{P})-1} + 2^{\mathrm{d}(\mathcal{P})-1} = 2^{\mathrm{d}(\mathcal{P})}$. QED

Definujme *superexponenciální funkci* $[n, k] \mapsto 2^n_k$ rekurzí: $2^n_0 = n$, $2^n_{k+1} = 2^{2^n_k}$. Nyní jsme připraveni vyslovit větu o eliminovatelnosti řezů.

Věta 3.3.13 (o eliminovatelnosti řezů) *Má-li sekvent $\mathcal{S}$ regulární důkaz $\mathcal{P}$, pak týž sekvent má i bezřezový důkaz hloubky nejvýše $2^{\mathrm{d}(\mathcal{P})}_{\mathrm{r}(\mathcal{P})}$.*

Důkaz Indukcí dle hodnosti $\mathrm{r}(\mathcal{P})$ důkazu $\mathcal{P}$ a užitím lemmatu 3.3.12. QED

Důkaz věty o eliminovatelnosti řezů, který jsme uvedli, je s úpravami převzat z Kleeneho knihy [49], z Takeutiho knihy [91] a ze Schwichtenbergovy kapitoly [76]. V knize [49] se neuvažuje o hloubkách důkazů. Odhad $2^{\mathrm{d}(\mathcal{P})}_{\mathrm{r}(\mathcal{P})}$ pro hloubku důkazu $\mathcal{P}'$ vzniklého z důkazu $\mathcal{P}$ odstraněním řezů je stanoven v kapitole [76], tam se ale pracuje se zvlášť upraveným (zjednodušeným) kalkulem. Lze dokázat, že mez $2^{\mathrm{d}(\mathcal{P})}_{\mathrm{r}(\mathcal{P})}$ je optimální nebo blízká optimální. Přístupný důkaz, viz [69], nalezl P. Pudlák. Pudlákův důkaz je také vypracován v diplomové práci [53].

Věta o eliminovatelnosti řezů spolu s faktem, že odhad $2^{\mathrm{d}(\mathcal{P})}_{\mathrm{r}(\mathcal{P})}$ je blízký optimálnímu, dává odpověď na otázku položenou v úvodu tohoto oddílu, zda v definici důkazu je nutné připustit uvažování oklikou. Není to nutné, avšak správně zvolené okliky (tj. formule, na které jsou užity řezy) mohou některé důkazy velmi výrazně zkrátit.

Dále uvádíme několik často citovaných důsledků věty o eliminovatelnosti řezů.

Věta 3.3.14 (Hilbertova-Ackermannova) *Nechť θ je otevřená formule taková, že formule $\exists x\theta$ je logicky platná. Pak existují termy $t_1, \ldots, t_n$ takové, že disjunkce $\theta_x(t_1) \vee \ldots \vee \theta_x(t_n)$ je logicky platná.*

Důkaz Sekvent $\langle \Rightarrow \exists x\theta \rangle$ je regulární, logicky platný, a tedy dokazatelný. Nechť tedy $\mathcal{P}$ je jeho bezřezový důkaz. Z věty 3.3.4 víme, že každá formule v $\mathcal{P}$ je s-podformulí formule $\exists x\theta$. Z toho plyne, že v $\mathcal{P}$ se nevyskytuje žádná formule obsahující univerzální kvantifikátor, a že tedy v $\mathcal{P}$ není užito pravidlo $\forall$-l ani $\forall$-r. Dále je zřejmé, že formule $\exists x\theta$ není nikdy vstupní formulí jakéhokoliv pravidla, jinak by totiž vznikla formule, která obsahuje kvantifikátor $\exists x$ v rozsahu platnosti nějakého dalšího logického symbolu, čili formule, která není s-podformulí formule $\exists x\theta$. Jakákoliv formule vyskytující se v $\mathcal{P}$ v antecedentu může z antecedentu zmizet pouze (tak, že se stane s-podformulí nějaké formule, která z antecedentu zmizí) užitím některého z pravidel $\rightarrow$-r nebo $\neg$-r. Protože žádná s-podformule formule $\exists x\theta$ neobsahuje existenční kvantifikátor v rozsahu platnosti implikace ani negace (ani jiného logického symbolu), můžeme usoudit, že v $\mathcal{P}$ není užito pravidlo $\exists$-l a že formule $\exists x\theta$

není principální formulí žádného iniciálního sekventu (bez ohledu na to, zda připouštíme neatomické formule jako principální formule iniciálních sekventů). V $\mathcal{P}$ se mohou (a ovšem musí) vyskytovat užití pravidla $\exists$-r. Principální formulí každého takového kroku ale musí být formule $\exists x\theta$, a tedy každá vstupní formule takového kroku musí mít tvar $\theta_x(t)$ pro jistý term t.

Nechť Ω je množina všech vstupních formulí pravidla $\exists$-r, nechť $\theta_x(t_1), \ldots, \theta_x(t_n)$ jsou všechny její prvky. Pro libovolný sekvent $\mathcal{S}$ tvaru $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ označme $\mathcal{S}^\sharp$ sekvent $\langle\, \Gamma \Rightarrow \Omega, \Delta - \{\exists x\theta\} \,\rangle$. Když $\mathcal{S}$ je iniciální sekvent našeho důkazu $\mathcal{P}$, pak $\mathcal{S}^\sharp$ je opět iniciální sekvent. Když sekvent $\mathcal{S}$ je užitím výrokového kroku odvozen ze sekventu $\mathcal{S}_1$ nebo ze dvou sekventů $\mathcal{S}_1$ a $\mathcal{S}_2$, pak sekvent $\mathcal{S}^\sharp$ je tímtéž krokem odvoditelný ze sekventu $\mathcal{S}_1^\sharp$ resp. ze sekventů $\mathcal{S}_1^\sharp$ a $\mathcal{S}_2^\sharp$. Když sekvent $\mathcal{S}$ je jedním krokem odvozen ze sekventu $\mathcal{S}_1$ pomocí pravidla $\exists$-r nebo pravidla W, pak $\mathcal{S}^\sharp$ a $\mathcal{S}_1^\sharp$ jsou tytéž sekventy nebo je sekvent $\mathcal{S}^\sharp$ odvoditelný ze sekventu $\mathcal{S}_1^\sharp$ pomocí pravidla W. To znamená, že pro každý sekvent $\mathcal{S}$ důkazu $\mathcal{P}$ platí, že sekvent $\mathcal{S}^\sharp$ je dokazatelný (a logicky platný). Pro finální sekvent $\langle \Rightarrow \exists x\theta \rangle$ to znamená, že sekvent $\langle \Rightarrow \Omega \rangle$ je logicky platný, a že tedy disjunkce $\theta_x(t_1) \vee \ldots \vee \theta_x(t_n)$ je logicky platná. QED

K větě 3.3.14 ještě poznamenejme, že z cvičení 22 a 23 oddílu 3.1 plyne, že nelze požadovat, aby term t byl pouze jeden, a také že předpoklad, že formule θ je otevřená, je podstatný.

Následující lemma 3.3.15 a větu 3.3.16 by bylo možno formulovat a dokazovat pohodlněji, kdybychom mezi logickými symboly měli symbol $\bot$ pro nepravdu. Kvůli dvěma tvrzením ale seznam logických symbolů neměňme a místo toho se domluvme, že $\bot$ označuje pevně zvolenou vyvratitelnou sentenci (toho jazyka, se kterým pracujeme).

Lemma 3.3.15 *Nechť $\langle\, \Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2 \,\rangle$ je regulární a logicky platný sekvent. Pak existuje formule θ taková, že*

- *oba sekventy $\langle\, \Gamma_1 \Rightarrow \Delta_1, \theta \,\rangle$ a $\langle\, \Gamma_2, \theta \Rightarrow \Delta_2 \,\rangle$ jsou logicky platné,*
- *formule θ je jednou z formulí $\bot$, $\neg\bot$, nebo má vlastnost, že každý predikátový symbol, který se v ní vyskytuje, se současně vyskytuje v obou sekventech $\langle\, \Gamma_1 \Rightarrow \Delta_1 \,\rangle$ a $\langle\, \Gamma_2 \Rightarrow \Delta_2 \,\rangle$,*
- *každá volná proměnná formule θ se současně vyskytuje volně v obou sekventech $\langle\, \Gamma_1 \Rightarrow \Delta_1 \,\rangle$ a $\langle\, \Gamma_2 \Rightarrow \Delta_2 \,\rangle$.*

Důkaz Nechť je dán sekvent $\langle\, \Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2 \,\rangle$. Vezměme jeho bezřezový důkaz $\mathcal{P}$ a postupujme indukcí podle hloubky $\mathrm{d}(\mathcal{P})$ důkazu $\mathcal{P}$. Je-li $\mathrm{d}(\mathcal{P}) = 0$, pak $(\Gamma_1 \cup \Gamma_2) \cap (\Delta_1 \cup \Delta_2) \neq \emptyset$. Je-li množina $\Gamma_1 \cap \Delta_1$ neprázdná, volme $\theta := \bot$. Je-li množina $\Gamma_2 \cap \Delta_2$ neprázdná, volme $\theta := \neg\bot$. Je-li množina $\Gamma_1 \cap \Delta_2$ neprázdná, volme za formuli θ kterýkoliv její prvek, a je-li množina $\Gamma_2 \cap \Delta_1$ neprázdná, volme za formuli θ negaci kteréhokoliv jejího prvku. V obou případech je splněn požadavek na predikátové symboly a volné proměnné.

Nechť dále důkaz $\mathcal{P}$ má nenulovou hloubku. Předpokládejme, že jeho poslední krok má tvar $\langle\, \Gamma, \alpha \Rightarrow \Delta \,\rangle, \langle\, \Gamma, \beta \Rightarrow \Delta \,\rangle \,/\, \langle\, \Gamma, \alpha \vee \beta \Rightarrow \Delta \,\rangle$ a že jsou dány množiny Γ_1,

Γ_2, Δ_1 a Δ_2 takové, že $\Delta_1 \cup \Delta_2 = \Delta$ a $\Gamma_1 \cup \Gamma_2 = \Gamma \cup \{\alpha \vee \beta\}$. Označme $\Gamma_1' = \Gamma_1 \cap \Gamma$ a $\Gamma_2' = \Gamma_2 \cap \Gamma$. Platí $\Gamma_1' \cup \Gamma_2' = \Gamma$. Dále platí $\alpha \vee \beta \in \Gamma_1$ nebo $\alpha \vee \beta \in \Gamma_2$. Předpokládejme třeba druhý případ. Poslední krok důkazu $\mathcal{P}$ si tedy můžeme představit takto:

$$\frac{\langle\, \Gamma_1', \overbrace{\alpha, \Gamma_2'} \Rightarrow \Delta_1, \Delta_2 \,\rangle \qquad \langle\, \Gamma_1', \overbrace{\beta, \Gamma_2'} \Rightarrow \Delta_1, \Delta_2 \,\rangle}{\langle\, \Gamma_1', \underbrace{\alpha \vee \beta, \Gamma_2'} \Rightarrow \Delta_1, \Delta_2 \,\rangle.}$$

Přitom složená závorka dole naznačuje, že ve sjednocení, které je dáno, formule $\alpha \vee \beta$ patří k druhé množině Γ_2, kdežto složené závorky nahoře naznačují, že formuli α resp. formuli β jsme se tudíž rozhodli přiřadit rovněž k množině Γ_2. Dle indukčního předpokladu užitého na horní sekventy existují formule η a λ takové, že formule η je jednou z formulí $\bot$, $\neg\bot$, nebo obsahuje pouze takové predikátové symboly a volné proměnné, které se současně vyskytují (volně) v obou sekventech $\langle\, \Gamma_1' \Rightarrow \Delta_1 \,\rangle$ a $\langle\, \Gamma_2', \alpha \Rightarrow \Delta_2 \,\rangle$, formule λ je jednou z formulí $\bot$, $\neg\bot$, nebo obsahuje pouze takové predikátové symboly a volné proměnné, které se současně vyskytují (volně) v obou sekventech $\langle\, \Gamma_1' \Rightarrow \Delta_1 \,\rangle$ a $\langle\, \Gamma_2', \beta \Rightarrow \Delta_2 \,\rangle$, a sekventy

$$\langle\, \Gamma_1' \Rightarrow \Delta_1, \eta \rangle, \qquad \langle\, \Gamma_2', \alpha, \eta \Rightarrow \Delta_2 \,\rangle, \qquad \langle\, \Gamma_1' \Rightarrow \Delta_1, \lambda \rangle, \qquad \langle\, \Gamma_2', \beta, \lambda \Rightarrow \Delta_2 \,\rangle$$

jsou všechny logicky platné (dokazatelné). Z prvního a třetího lze odvodit sekvent $\langle\, \Gamma_1 \Rightarrow \Delta_1, \eta \,\&\, \lambda \,\rangle$, ze zbývajících lze odvodit sekvent $\langle\, \Gamma_2', \alpha \vee \beta, \eta \,\&\, \lambda \Rightarrow \Delta_2 \,\rangle$, tj. sekvent $\langle\, \Gamma_2, \eta \,\&\, \lambda \Rightarrow \Delta_2 \,\rangle$. Není-li žádná z formulí η a λ totožná s žádnou z formulí $\bot$ a $\neg\bot$, volme $\theta := \eta \,\&\, \lambda$. Je-li některá z formulí η a λ totožná s formulí $\bot$, volme za θ formuli $\bot$. Jsou-li obě z formulí η a λ totožné s formulí $\neg\bot$, volme $\theta := \neg\bot$. Formule θ je ve všech případech ekvivalentní s formulí $\eta \,\&\, \lambda$ a splňuje požadavky. V případě, kdy $\alpha \vee \beta \in \Gamma_1$, a také v případech, kdy je v posledním kroku důkazu $\mathcal{P}$ užito jiné výrokové pravidlo než $\vee$-l, se postupuje podobně.

Předpokládejme, že v posledním kroku důkazu $\mathcal{P}$ je užito pravidlo $\forall$-l, že máme dány množiny Γ_1, Γ_2, Δ_1 a Δ_2 podobně jako v předchozích případech a že pro principální formuli $\forall x \alpha$ posledního kroku opět platí $\forall x \alpha \in \Gamma_2$. Poslední krok důkazu $\mathcal{P}$ si tedy můžeme představit takto:

$$\frac{\langle\, \Gamma_1', \overbrace{\alpha_x(t), \Gamma_2'} \Rightarrow \Delta_1, \Delta_2 \,\rangle}{\langle\, \Gamma_1', \underbrace{\forall x \alpha, \Gamma_2'} \Rightarrow \Delta_1, \Delta_2 \,\rangle,}$$

kde množiny Γ_1' a Γ_2' se vztahují k daným množinám Γ_1 a Γ_2 analogicky jako ve výše probraném případě týkajícím se pravidla $\vee$-l. Dle indukčního předpokladu existuje formule λ, která je jednou z formulí $\bot$, $\neg\bot$, nebo obsahuje pouze predikátové symboly a volné proměnné, které se současně vyskytují (volně) v obou sekventech $\langle\, \Gamma_1' \Rightarrow \Delta_1 \,\rangle$ a $\langle\, \Gamma_2', \alpha_x(t) \Rightarrow \Delta_2 \,\rangle$, a přitom sekventy

$$\langle\, \Gamma_1' \Rightarrow \Delta_1, \lambda \,\rangle \quad \text{a} \quad \langle\, \Gamma_2', \alpha_x(t), \lambda \Rightarrow \Delta_2 \,\rangle$$

jsou oba logicky platné. Nechť $v_1, \ldots, v_k$ je seznam všech proměnných, které se vyskytují volně ve formuli $\alpha_x(t)$, ale nikoliv v sekventu $\langle\, \Gamma_2', \forall x\alpha \;\Rightarrow\; \Delta_2 \,\rangle$. Z levého sekventu lze odvodit sekvent $\langle\, \Gamma_1 \;\Rightarrow\; \Delta_1, \exists v_1 \,..\, \exists v_k \lambda \,\rangle$, z pravého lze odvodit sekvent $\langle\, \Gamma_2', \forall x\alpha, \exists v_1 \,..\, \exists v_k \lambda \;\Rightarrow\; \Delta_2 \,\rangle$, tj. sekvent $\langle\, \Gamma_2, \exists v_1 \,..\, \exists v_k \lambda \;\Rightarrow\; \Delta_2 \,\rangle$. Když λ je některá z formulí $\bot$, $\neg\bot$, pak $\exists v_1 \,..\, \exists v_k \lambda$ a λ jsou ekvivalentní formule a lze volit $\theta := \lambda$. Jinak volme $\theta := \exists v_1 \,..\, \exists v_k \lambda$.

Podívejme se ještě třeba na případ

$$\frac{\langle\, \overbrace{\Gamma_1', \alpha_x(y)}, \Gamma_2' \;\Rightarrow\; \Delta_1, \Delta_2 \,\rangle}{\langle\, \underbrace{\Gamma_1', \exists x\alpha}, \Gamma_2' \;\Rightarrow\; \Delta_1, \Delta_2 \,\rangle,}$$

kdy v posledním kroku důkazu $\mathcal{P}$ je užito pravidlo $\exists$-l a jeho principální formule je v rozkladu počítána k levé množině Γ_1. Indukční předpoklad dává formuli λ, která je jednou z formulí $\bot$, $\neg\bot$, nebo obsahuje pouze predikátové symboly a volné proměnné, které se současně vyskytují (volně) v sekventech $\langle\, \Gamma_1', \alpha_x(y) \;\Rightarrow\; \Delta_1 \,\rangle$ a $\langle\, \Gamma_2' \;\Rightarrow\; \Delta_2 \,\rangle$, a přitom sekventy

$$\langle\, \Gamma_1', \alpha_x(y) \;\Rightarrow\; \Delta_1, \lambda \,\rangle \quad \text{a} \quad \langle\, \Gamma_2', \lambda \;\Rightarrow\; \Delta_2 \,\rangle$$

jsou oba logicky platné. Protože proměnná y se nevyskytuje volně v λ (jinak by se musela vyskytovat volně v $\Gamma_2' \cup \Delta_2$ a v kroku $\exists$-l by nebyla splněna podmínka EVC), je sekvent $\langle\, \Gamma_1, \exists x\alpha \;\Rightarrow\; \Delta_1, \lambda \,\rangle$ logicky platný a formuli λ můžeme bez dalších úprav prohlásit za hledanou formuli θ. QED

Věta 3.3.16 *Nechť formule $\varphi \to \psi$ je regulární a logicky platná. Pak jedna z formulí $\neg\varphi$ a ψ je logicky platná, nebo existuje formule θ taková, že obě formule $\varphi \to \theta$ a $\theta \to \psi$ jsou logicky platné, a přitom formule θ obsahuje pouze takové predikátové symboly a volné proměnné, které se současně vyskytují (volně) ve φ i v ψ.*

Důkaz Zvolme $\Gamma_1 = \{\varphi\}$, $\Delta_2 = \{\psi\}$, $\Gamma_2 = \Delta_1 = \emptyset$. Vezměme formuli θ, jejíž existenci zaručuje lemma 3.3.15. Když θ je $\bot$ nebo $\neg\bot$, pak $\neg\varphi$ nebo ψ je logicky platnou formulí. QED

Platí i silnější tvrzení než věta 3.3.16, v němž stojí „mimologické symboly“ místo „predikátové symboly“. Tomuto silnějšímu tvrzení se říká *Craigova věta o interpolaci*. Větu 3.3.16 tedy můžeme označit jako slabou větu o interpolaci. Také lemma 3.3.15 lze považovat za variantu věty o interpolaci. Postup, kterým jsme dokázali větu 3.3.16, přes důkaz lemmatu 3.3.15, je v [91] označen jako Maeharova metoda.

Rozšiřme nyní kalkulus GK na kalkulus pro predikátovou logiku s rovností, a to podobným způsobem, jako když jsme v oddílu 3.2 rozšířili kalkulus HK na kalkulus HK_{e}. Kromě iniciálních sekventů tvaru A (tj. takových, jejichž antecedent a sukcedent mají neprázdný průnik) připusťme ještě následující iniciální sekventy týkající se rovnítka:

e1: $\langle \Rightarrow t = t \rangle$,

e2: $\langle t = s \Rightarrow s = t \rangle$,

e3: $\langle t = s, s = u \Rightarrow t = u \rangle$,

e4: $\langle t_1 = s_1, .., t_n = s_n \Rightarrow F(\underline{t}) = F(\underline{s}) \rangle$,

e5: $\langle t_1 = s_1, .., t_n = s_n, P(\underline{t}) \Rightarrow P(\underline{s}) \rangle$,

kde t, s, u, t_i, s_i jsou libovolné termy, F libovolný funkční symbol a P libovolný predikátový symbol (zvoleného jazyka). Výsledný *kalkulus* označme GK_e. Podobně jako v případě kalkulu $\mathrm{HK_e}$ lze ukázat, že iniciální sekventy tvaru e2 a e3 jsou zbytečné, pokud e5 chápeme tak, že predikát P může být i rovnítko. Dále libovolný sekvent $\langle \Gamma \Rightarrow \Delta \rangle$ je dokazatelný v kalkulu $\mathrm{GK_e}$ právě tehdy, když existuje konečná množina $F \subseteq E$ taková, že sekvent $\langle \Gamma, F \Rightarrow \Delta \rangle$ je dokazatelný v kalkulu GK, přičemž E je množina axiomů rovnosti definovaná v oddílu 3.2. Kalkulus $\mathrm{GK_e}$ je vzájemně polynomiálně simulovatelný s kalkulem $\mathrm{HK_e}$. Ověření všech těchto faktů ponecháváme za cvičení. Lze ověřit, že například sekvent $\langle x = y, x = z \Rightarrow y = z \rangle$ není iniciálním sekventem ani v případě, kdy predikát P v iniciálním sekventu e5 může být i rovnítko. Tento sekvent tedy v kalkulu $\mathrm{GK_e}$ nelze dokázat bez užití řezů. Znění věty o eliminovatelnosti řezů musíme pro kalkulus $\mathrm{GK_e}$ trochu upravit. Definujme, že řez v nějakém důkazu $\mathcal{P}$ je *nepodstatný* (tj. užití pravidla řezu v důkazu $\mathcal{P}$ je nepodstatné), jestliže jeho vstupní formule je rovnost, tj. formule tvaru $t = s$ pro jisté termy t a s. Ostatní řezy jsou *podstatné*.

Věta 3.3.17 *Každý regulární sekvent dokazatelný v kalkulu GK_e je v kalkulu GK_e dokazatelný i bez užití podstatných řezů.*

Důkaz Tentokrát pro jednoduchost neuvažujeme o hloubkách důkazů. Postup, který jsme ukázali pro kalkulus GK, lze následovně modifikovat pro kalkulus $\mathrm{GK_e}$. V tom místě důkazu lemmatu 3.3.11, kde jsme se starali o případ, kdy důkazy $\mathcal{P}_1$ a $\mathcal{P}_2$ mají oba nenulovou hloubku a formule θ je v obou z nich principální, uvažujme navíc případ, kdy formule θ není rovnost, a přitom je v obou důkazech principální formulí iniciálního sekventu tvaru e1–e5. Formule θ musí být tvaru $P(\underline{t})$, kde P není rovnítko, oba iniciální sekventy musí být tvaru e5, důkazy $\mathcal{P}_1$ a $\mathcal{P}_2$ mají hloubku nula a důkaz $\mathcal{P}_0$ má tvar

$$\frac{\langle s_1 = t_1, .., s_n = t_n, P(\underline{s}) \Rightarrow P(\underline{t}) \rangle \qquad \langle t_1 = u_1, .., t_n = u_n, P(\underline{t}) \Rightarrow P(\underline{u}) \rangle}{\langle s_1 = t_1, t_1 = u_1, .., s_n = t_n, t_n = u_n, P(\underline{s}) \Rightarrow P(\underline{u}) \rangle}.$$

Požadovaný důkaz neobsahující podstatné řezy získáme tak, že vezmeme iniciální sekvent $\langle s_1 = u_1, .., s_n = u_n, P(\underline{s}) \Rightarrow P(\underline{u}) \rangle$, dále vezmeme n iniciálních sekventů tvaru $\langle s_i = t_i, t_i = u_i \Rightarrow s_i = u_i \rangle$ a formule $s_1 = u_1$ až $s_n = u_n$ odstraníme pomocí n (nepodstatných) řezů. QED

Věta 3.3.18 *Nechť φ je sentence dokazatelná v teorii T. Pak φ má gentzenovský důkaz v T, tj. sekvent tvaru $\langle F \Rightarrow \varphi \rangle$, kde $F \subseteq T$ je konečná, má důkaz v kalkulu GK_e, v němž se nevyskytují jiné formule než rovnosti a s-podformule prvků množiny $T \cup \{\varphi\}$.*

Důkaz Máme sekvent $\langle F \Rightarrow \varphi \rangle$, který je dokazatelný v kalkulu $\mathrm{GK_e}$ a pro který platí $F \subseteq T$. Protože všechny jeho formule jsou sentence, tento sekvent je regulární. Existuje tedy důkaz $\mathcal{P}$ téhož sekventu, který neobsahuje podstatné řezy. Větu 3.3.4 lze snadno zobecnit do této podoby: každá formule v jakémkoliv důkazu $\mathcal{P}$ je s-podformulí některé formule ψ takové, že ψ je v $\mathcal{P}$ obsažena ve finálním sekventu nebo je na ni použit řez. QED

Cvičení

1. Nalezněte příklady na to, že všechny tři požadavky v podmínce EVC, totiž že y nemá volné výskyty v Γ, v Δ ani v $\exists x\varphi$, jsou podstatné. Vysvětlete, proč třetí požadavek nezní „y nemá volné výskyty ve φ“.

2. Sestrojte důkazy všech logických axiomů kalkulu HK, tj. všech formulí tvaru A1–A7 a B1 a B2, v kalkulu GK.

3. V důkazu věty 3.3.1 byla dokázána korektnost pravidla $\exists$-l. Dokončete důkaz věty, tj. dokažte korektnost všech ostatních pravidel kalkulu GK.

4. Zdůvodněte, že věta 3.3.2 platí i v případě, kdy délka $|\mathcal{P}|$ důkazu $\mathcal{P}$ je definována jako souhrnný počet výskytů všech symbolů (včetně číslic vyskytujících se v indexech proměnných) v důkazu $\mathcal{P}$.

5. Vypracujte všechny vynechané případy v důkazech lemmat 3.3.10 a 3.3.11.

6. Rozhodněte, zda platí: každá s-podformule regulární formule je regulární.

7. Každý regulární sekvent má důkaz, ve kterém není užito pravidlo W. Dokažte.

8. Zdůvodněte, že platí tato varianta věty 3.3.4: každá formule v libovolném důkazu $\mathcal{P}$ je s-podformulí nějaké formule, která je v důkazu $\mathcal{P}$ obsažena ve finálním sekventu nebo která je v důkazu $\mathcal{P}$ vstupní formulí některého užití pravidla řezu.

9. Dokažte větu o středním sekventu: každý regulární logicky platný sekvent, jehož všechny formule jsou prenexní, má bezřezový důkaz $\mathcal{P}$, v němž všechna užití výrokových pravidel předcházejí všechna užití kvantifikátorových pravidel. Středním sekventem je míněn poslední (nejnižší) sekvent $\mathcal{S}$ v důkazu $\mathcal{P}$, který neobsahuje kvantifikátory. Tento sekvent $\mathcal{S}$ je tautologický a přitom finální sekvent důkazu $\mathcal{P}$ lze ze sekventu $\mathcal{S}$ získat pouze užitím kvantifikátorových kroků.

Návod. Začněte s bezřezovým důkazem $\mathcal{P}$, v němž není užito pravidlo W. Definujte *řád* kvantifikátorového *kroku* jako počet všech výrokových kroků, které po něm (tj. na cestě k finálnímu sekventu důkazu $\mathcal{P}$) následují. Dále definujte *řád důkazu* jako součet řádů všech kvantifikátorových kroků. Má-li důkaz $\mathcal{P}$ nenulový řád, lze v něm nalézt nejnižší kvantifikátorový krok s nenulovým řádem. Bezprostředně následující krok musí být výrokový. Protože principální formule tohoto kvantifikátorového kroku není vstupní formulí onoho bezprostředně následujícího výrokového kroku, lze pořadí obou kroků zaměnit. Toto zdůvodněte podrobně, probráním všech možných případů. Důkaz vzniklý záměnou obou kroků má nižší řád.

10. Navrhněte alternativní důkaz věty 3.3.14 založený na předchozím cvičení.

11. Zdůvodněte, že předpoklad ve větě 3.3.16, že formule $\varphi \to \psi$ je regulární, není podstatný.

12. Zdůvodněte, že ve větě 3.3.16 a v lemmatu 3.3.15 lze psát „predikátové symboly a konstanty“ místo „predikátové symboly“.

13. Nechť L_1 a L_2 jsou jazyky bez funkčních symbolů, nechť T_1 je bezesporná teorie v jazyce L_1, nechť T_2 je bezesporná teorie v jazyce L_2 a nechť neexistuje sentence φ v jazyce $L_1 \cap L_2$, která je dokazatelná v T_1 a vyvratitelná v T_2. Pak $T_1 \cup T_2$ je bezesporná teorie. Toto tvrzení lze označit jako variantu Robinsonovy věty o bezespornosti. Dokažte je převedením na lemma 3.3.15.

    Návod. Když $T_1 \cup T_2$ je sporná, pak existují konečné množiny $F_1 \subseteq T_1$ a $F_2 \subseteq T_2$ takové, že sekvent $\langle F_1, F_2 \Rightarrow \rangle$ je logicky platný.

14. Dokažte, že věta 3.3.14 platí i pro predikátovou logiku s rovností.

15. Dokažte, že pro predikátovou logiku s rovností platí varianta věty 3.3.16 tohoto znění: když formule $\varphi \to \psi$ je logicky platná, pak existuje formule θ, jejíž všechny predikátové symboly s výjimkou rovnítka se současně vyskytují v obou formulích φ a ψ, jejíž všechny volné proměnné se současně vyskytují volně v obou formulích φ a ψ, a přitom formule $\varphi \to \theta$ a $\theta \to \psi$ jsou logicky platné.

    Návod. Za formuli $\bot$ vezměte třeba sentenci $\exists x(x \neq x)$. Formulujte a dokažte příslušnou variantu lemmatu 3.3.15.

3.4 Vlastnosti modelů a teorií

V tomto oddílu budeme klást důraz na užití *sémantických* metod. Jinými slovy, ukážeme, že některé vlastnosti axiomatických teorií lze zjistit úvahami o strukturách, modelech a vyplývání. Naším nejdůležitějším nástrojem bude věta o kompaktnosti (klasické) predikátové logiky s rovností.

Věta 3.4.1 (o kompaktnosti) *Nechť T je teorie. Pak*
(a) Když $T \models \varphi$, pak existuje konečná množina $F \subseteq T$ taková, že $F \models \varphi$.
(b) Když každá konečná množina $F \subseteq T$ má model, pak T má model.

Důkaz Nechť $T \models \varphi$. Podle věty o silné úplnosti platí $T \vdash \varphi$. Existuje tedy důkaz formule φ z předpokladů T. Důkaz je definován jako jistá *konečná* posloupnost formulí. Za množinu F tedy můžeme vzít množinu všech těch prvků množiny T, které se vyskytují v našem důkazu. Platí $F \vdash \varphi$, a tedy $F \models \varphi$.

Nechť T nemá žádný model. V tom případě lze o jakékoliv formuli φ říci, že platí v každém modelu teorie T, tj. že $T \models \varphi$. Zvolme za φ sentenci $\exists x(x \neq x)$. Podle tvrzení (a) existuje konečná $F \subseteq T$ taková, že $F \models \exists x(x \neq x)$. O sentenci $\exists x(x \neq x)$ je jasné, že neplatí v žádné struktuře. Dále o ní víme, že platí v každém modelu teorie F. Tedy F nemá žádný model. QED

Všimněme si, že věta o kompaktnosti je čistě sémantické tvrzení, kterému rozumí každý, kdo rozumí Tarského definici a definici vyplývání. Logický kalkulus není nutný k pochopení znění věty o kompaktnosti. Uplatnil se ale *v důkazu*.

Každé axiomatické teorii T s jazykem L odpovídá třída všech jejích modelů, tj. třída všech struktur pro jazyk L, ve kterých platí všechny axiomy teorie T. Představme si však, že úvahy začneme nikoliv od teorie, nýbrž od nějaké třídy $\mathcal{E}$ struktur pro daný jazyk, a položíme si otázku: je $\mathcal{E}$ třídou všech modelů nějaké teorie T? Existuje-li k třídě $\mathcal{E}$ teorie T taková, že $\mathcal{E}$ je třídou všech modelů teorie T, řekneme, že $\mathcal{E}$ je *axiomatizovatelná* nebo že $\mathcal{E}$ je *elementární třídou*. Ptáme se tedy:

- *Je každá třída $\mathcal{E}$ struktur pro nějaký jazyk L elementární třídou?*

Tato otázka má smysl jen v případě, kdy třída $\mathcal{E}$ s každým svým prvkem $\mathbf{D}$ obsahuje i všechny struktury izomorfní s $\mathbf{D}$. V opačném případě triviální odpověď zní ne.

S jedním netriviálním případem, tj. s případem, kdy $\mathcal{E}$ obsahuje s každou strukturou všechny s ní izomorfní struktury, a přesto není axiomatizovatelná, jsme se již setkali. Víme, viz 3.2.13, že je-li L nejvýše spočetný jazyk, pak každá bezesporná teorie v L má nejvýše spočetný model. To znamená, že libovolná elementární třída obsahující všechny nespočetné struktury obsahuje také nějaké nejvýše spočetné struktury. Třída všech nespočetných struktur pro jazyk L tedy není elementární třídou.

Fakt, že je-li jazyk L nejvýše spočetný, pak třída všech nespočetných struktur pro L není elementární třídou, lze také formulovat takto: vlastnost „býti nespočetnou strukturou“ nelze vyjádřit pomocí sentencí jazyka L. Z následující věty plyne, že ani vlastnost „býti konečnou strukturou“ nelze vyjádřit pomocí sentence ani pomocí množiny sentencí (v tomto případě bez ohledu na mohutnost jazyka).

Věta 3.4.2 *Nechť T je teorie a nechť pro každé přirozené číslo n existuje model teorie T, jehož nosná množina má více než n prvků. Pak T má i nekonečné modely.*

Důkaz Označme γ_n sentenci $\forall x_1 \,..\, \forall x_n \exists y(y \neq x_1 \,\&\, ..\, \&\, y \neq x_n)$ (stejně jako v příkladu 3.1.19(f)). I když nemáme žádný bližší údaj o jazyce teorie T, můžeme

tvrdit, že γ_n je sentence jazyka teorie T, protože γ_n neobsahuje žádné mimologické symboly. Sentence γ_n platí v libovolné struktuře $\mathbf{D}$ právě tehdy, když (nosná množina D struktury) $\mathbf{D}$ má více než n prvků. Označme $S = \{\, \gamma_n \,;\, n \geq 1 \,\}$.

Tvrdíme, že je-li $F \subseteq S$ a F je konečná, pak teorie $T \cup F$ má nějaký model. Nechť konečná $F \subseteq S$ je dána. Označme $\gamma_{n_1}, \ldots, \gamma_{n_r}$ prvky množiny F a označme $m = \max\{n_1, \ldots, n_r\}$. Podle předpokladu existuje nějaký model $\mathbf{M}$ teorie T, který má více než m prvků. V $\mathbf{M}$ platí γ_m, a tedy i všechny γ_{n_i}. Tedy $\mathbf{M} \models T \cup F$.

Je-li $F \subseteq T \cup S$ a F je konečná, pak $F = F_1 \cup F_2$, kde $F_1 \subseteq T$ a $F_2 \subseteq S$. Přitom F_1 a F_2 jsou konečné. Podle podmínky dokázané v předchozím odstavci existuje model $\mathbf{M}$ teorie $T \cup F_2$. Protože $F_1 \subseteq T$, platí také $\mathbf{M} \models F_1 \cup F_2$, tedy $\mathbf{M} \models F$. Tím jsme ověřili, že každá konečná $F \subseteq T \cup S$ má model. Podle věty o kompaktnosti teorie $T \cup S$ má nějaký model $\mathbf{K}$. Struktura $\mathbf{K}$ je model teorie T, ve kterém platí všechny sentence γ_n. Je jasné, že struktura, ve které platí všechny sentence γ_n, musí být nekonečná. $\mathbf{K}$ je tedy hledaný nekonečný model teorie T. QED

Množina sentencí S, která se vyskytla v předchozí větě, platí v libovolné struktuře $\mathbf{D}$ právě tehdy, když $\mathbf{D}$ je nekonečná. Vedlejším produktem předchozí věty je tedy pozorování, že vlastnost „býti nekonečnou strukturou“ je možné vyjádřit množinou sentencí (bez ohledu na jazyk). Tím jsme zároveň zjistili, že komplement nějaké elementární třídy $\mathcal{E}$, tj. třída všech struktur pro daný jazyk L, které nejsou v $\mathcal{E}$, nemusí být elementární třídou.

Ukažme si ještě další příklady toho, kdy o nějaké třídě struktur lze dokázat, že není elementární, neboli kdy o nějaké vlastnosti (struktur) lze dokázat, že není vyjádřitelná v příslušném jazyce. Uvažujme jazyk $\{<\}$ s jediným binárním predikátem a struktury tvaru $\langle D, R\rangle$, kde D je (neprázdná) množina a R je binární relace na D. Vlastnost, že $\langle D, R\rangle$ je lineárně uspořádanou množinou, vyjádřit lze. Teorie, jejímiž modely jsou právě ty struktury $\langle D, R\rangle$, které jsou lineárně uspořádanými množinami, je teorie LO, tj. teorie lineárního uspořádání definovaná v závěru oddílu 3.2. Uvažujme nyní vlastnost, že $\langle D, R\rangle$ je *dobře* uspořádanou množinou, tj. že $\langle D, R\rangle$ je lineárně uspořádanou množinou, jež navíc splňuje podmínku

$$\forall X \subseteq D(X \neq \emptyset \Rightarrow \exists a \in X \neg \exists b \in X(b\ R\ a)), \qquad (*)$$

která říká, že každá neprázdná podmnožina množiny D má R-minimální prvek. Struktura $\langle \mathrm{N}, <\rangle$ přirozených čísel s uspořádáním je příkladem dobře uspořádané množiny. Také libovolné ordinální číslo je dobře uspořádané relací $\in$ (tj. relací náležení). Každá konečná lineárně uspořádaná množina je dobře uspořádanou množinou. Z následující věty plyne, že podmínku $(*)$ nelze vyjádřit v jazyce $\{<\}$. Třída všech dobře uspořádaných množin není elementární třídou.

Věta 3.4.3 *Nechť T je teorie s jazykem L obsahujícím binární predikátový symbol $<$ a nechť T má nekonečný model $\mathbf{M}$ takový, že $\langle M, <^{\mathbf{M}}\rangle$ je dobře uspořádaná množina. Pak T má i model $\mathbf{K}$ takový, že $\langle K, <^{\mathbf{K}}\rangle$ není dobře uspořádaná množina. Je-li jazyk L nejvýše spočetný, pak T má i spočetný model $\mathbf{K}$ takový, že $\langle K, <^{\mathbf{K}}\rangle$ není dobře uspořádaná množina.*

Důkaz Zvolme pevně nekonečný model $\mathbf{M}$ teorie T. Označme symbolem L' jazyk $L \cup \{c_0, c_1, c_2, \dots\}$ vzniklý z jazyka L teorie T přidáním nekonečně mnoha nových (tj. nevyskytujících se v L) konstant c_0, c_1 atd. Označme S množinu všech sentencí v L' tvaru $c_i < c_j$, kde $j < i$. Tvrdíme, že teorie $T \cup S$ má nějaký model.

Podle věty o kompaktnosti stačí ověřit, že každá konečná $F \subseteq T \cup S$ má model. Postupujme podobně jako v důkazu věty 3.4.2: dokážeme, že je-li $F \subseteq S$ konečná, pak $T \cup F$ má model. Tím bude ověřena silnější, a tedy také dostatečná podmínka.

Nechť konečná $F \subseteq S$ je dána. Zvolme m takové, že pro každou sentenci $c_i < c_j$ v F platí $i, j \leq m$. Máme dobře uspořádaný nekonečný model $\mathbf{M}$ teorie T. Hledaný model $\mathbf{M}_F$ teorie $T \cup F$ sestrojíme tak, že v $\mathbf{M}$ zvolíme realizace konstant c_i (a realizace symbolů jazyka L ponecháme beze změny). Ať to uděláme jakkoliv, neporušíme platnost axiomů teorie T, protože ty neobsahují konstanty c_i.

Je-li $i > m$, pak se konstanta c_i nevyskytuje v $T \cup F$, a můžeme ji tedy realizovat libovolným prvkem nosné množiny M struktury $\mathbf{M}$. Zvolme prvky $a_0, \dots, a_m$ struktury $\mathbf{M}$ tak, aby platilo $a_0 <^{\mathbf{M}} a_1 <^{\mathbf{M}} \dots <^{\mathbf{M}} a_m$. To lze, neboť struktura $\mathbf{M}$ je nekonečná. Je-li $i \leq m$, realizujme konstantu c_i prvkem a_{m-i}. Tím jsme získali strukturu $\mathbf{M}_F$ pro jazyk L'. Je-li $j < i \leq m$, pak konstanta c_j je v $\mathbf{M}_F$ realizována větším prvkem než konstanta c_i. V $\mathbf{M}_F$ tedy platí všechny sentence z F.

Podle věty o kompaktnosti tedy existuje model $\mathbf{D}$ teorie $T \cup S$. Je-li jazyk L nejvýše spočetný, lze díky větě 3.2.13 předpokládat, že $\mathbf{D}$ je nejvýše spočetný. Prvky $c_0^{\mathbf{D}}, c_1^{\mathbf{D}}, \dots$ nosné množiny D modelu $\mathbf{D}$ tvoří klesající řetězec, tedy množinu, která nemá nejmenší prvek. Vraťme se k původnímu jazyku L, neboli utvořme ze struktury $\mathbf{D}$ novou strukturu $\mathbf{K}$ pro L, která má tutéž nosnou množinu D a v níž jsou všechny symboly jazyka L realizovány stejně jako v $\mathbf{D}$. Odstraněním konstant c_0, c_1, $\dots$ nezmizely z D jejich realizace. Zmizela pouze informace, že prvek $c_i^{\mathbf{D}}$ realizuje konstantu c_i. V K, což je táž množina jako D, tedy stále existuje neprázdná část, která vůči relaci $<^{\mathbf{K}}$ (která se shoduje s relací $<^{\mathbf{D}}$) nemá nejmenší prvek. $\mathbf{K}$ je tedy model teorie T takový, že $\langle K, <^{\mathbf{K}} \rangle$ není dobře uspořádaná množina. QED

Konstrukcím, které se vyskytly v důkazu předchozí věty, kdy k nějaké struktuře přidáme realizace dalších symbolů nebo naopak zrušíme realizace některých symbolů, říkáme expanze a redukce. Přesněji, je-li $\mathbf{D}_1$ struktura pro L_1 a $\mathbf{D}_2$ struktura pro L_2 a platí-li $L_1 \subseteq L_2$, řekneme, že $\mathbf{D}_1$ je *redukt* struktury $\mathbf{D}_2$ a $\mathbf{D}_2$ je *expanze* struktury $\mathbf{D}_1$, jestliže obě struktury mají tutéž nosnou množinu a jestliže libovolný symbol z L_1 má v $\mathbf{D}_1$ i v $\mathbf{D}_2$ tutéž realizaci.

Připomeňme opět, že *orientovaný graf* je libovolná struktura tvaru $\langle G, R \rangle$, kde R je binární relace na neprázdné množině G. Libovolný orientovaný graf $\langle G, R \rangle$ považujme za strukturu pro jazyk s jedním binárním predikátem, který zapisujeme opět jako „R“. Vrchol d grafu $\langle G, R \rangle$ je *dosažitelný* z vrcholu c, jestliže existuje sled (nebo cesta) z c do d.

Řekneme, že orientovaný graf $\langle G, R \rangle$ je *silně souvislý*, jestliže v $\langle G, R \rangle$ je každý vrchol z každého dosažitelný. Předpokládejme, že dovedeme napsat formuli $\varphi(x, y)$

v jazyce $\{R\}$, která vyjadřuje, že vrchol y je dosažitelný z vrcholu x. Formule $\varphi(x,y)$ je tedy v libovolném grafu $\langle G,R\rangle$ splněna dvojicí $[c,d]$ právě tehdy, když d je dosažitelný z c. V tom případě sentence $\forall x\forall y\varphi(x,y)$ vyjadřuje silnou souvislost grafu, neboli platí v libovolném grafu $\langle G,R\rangle$ právě tehdy, když $\langle G,R\rangle$ je silně souvislý. Rozmyslíme si, že to není možné. Třída všech silně souvislých grafů není axiomatizovatelná, a tedy neexistuje formule $\varphi(x,y)$ vyjadřující, že vrchol y je dosažitelný z vrcholu x. Než to uděláme, uvědomme si, že potíž je v tom, že definice dosažitelnosti vrcholu d z vrcholu c připouští libovolnou délku cesty z c do d, tj. libovolný (konečný) počet kroků, kterými lze z c dojít do d. Kdyby počet kroků byl omezený, snadno bychom příslušnou formuli napsali. Například d je z c dosažitelný nejvýše dvěma kroky, jestliže dvojice $[c,d]$ splňuje v $\langle G,R\rangle$ formuli

$$x=y \;\vee\; R(x,y) \;\vee\; \exists v(R(x,v) \;\&\; R(v,y)).$$

Následující příklad je převzat z knihy [62].

Příklad 3.4.4 Dokažme, že třída všech silně souvislých orientovaných grafů není elementární třídou. Postupujme sporem. Nechť T je teorie v jazyce $\{R\}$ taková, že libovolná struktura $\langle G,R\rangle$ je modelem teorie T, právě když $\langle G,R\rangle$ je silně souvislý orientovaný graf. Označme ψ sentenci

$$\forall x\forall y_1\forall y_2(R(x,y_1) \;\&\; R(x,y_2) \;\rightarrow\; y_1=y_2),$$

která vyjadřuje, že z každého vrcholu vede nejvýše jedna hrana. Je jasné, že teorie T,ψ má pro každé přirozené číslo $n\geq 1$ model mohutnosti n, totiž model tvaru

$$\langle\,\{0,\ldots,n-1\}\,,\,\{[0,1],[1,2],\ldots,[n-2,n-1],[n-1,0]\}\,\rangle$$

sestávající z jediného cyklu. Podle věty 3.4.2 teorie T,ψ má i nějaký nekonečný model $\langle G,R\rangle$. Struktura $\langle G,R\rangle$ je tedy nekonečný silně souvislý graf, ve kterém z každého vrcholu vede nejvýše jedna hrana. Zbývá zdůvodnit, že to není možné, nekonečné cykly neexistují. Zvolme pevně dva různé prvky c a d množiny G. Protože $\langle G,R\rangle$ je silně souvislý, d je dosažitelný z c a c je dosažitelný z d. V $\langle G,R\rangle$ tedy existují vrcholy $a_0,\ldots,a_n$ a $a_{n+1},\ldots,a_{n+m}$ takové, že $\forall i<n+m(a_i\ R\ a_{i+1})$, a přitom $a_0=c$, $a_n=d$ a $a_{n+m}=c$. Posloupnost $a_0,\ldots,a_{n+m}$ je tedy (konečnou) cestou z c do c délky alespoň 2. Protože graf $\langle G,R\rangle$ je nekonečný, lze zvolit vrchol $e\in G$ různý od všech vrcholů a_i. Také e je dosažitelný z c. Existuje tedy cesta $b_0,\ldots,b_k$, kde $b_0=c$ a $b_k=e$, z vrcholu c do vrcholu e. Cesty $a_0,\ldots,a_{n+m}$ a $b_0,\ldots,b_k$ mají společný začátek, ale různý konec. Existuje tedy poslední společný vrchol a_{i_0}, tj. existuje index $i_0<\min\{n+m,k\}$ takový, že $a_{i_0}=b_{i_0}$, $a_{i_0+1}\neq b_{i_0+1}$. Vrchol a_{i_0} porušuje axiom ψ, neboť z něj vycházejí dvě různé hrany.

Symbolický zápis na straně 207 označený hvězdičkou, který vyjadřuje, že nějaké uspořádání je dobrým uspořádáním, není formulí a ve větě 3.4.3 jsme dokázali, že vyjádřit jej pomocí formule nebo množiny formulí není možné. Lze si ale představit zobecnění definice formule a logické sémantiky, ve kterém by se zápis $(*)$ stal formulí. Stačilo by definici jazyka, struktury a realizace symbolů jazyka ponechat beze

změny, ale připustit proměnné dvojího druhu, jedny pro objekty a druhé pro podmnožiny struktury (a psát „$\forall X$“ místo „$\forall X \subseteq D$“). Podobně podmínka vyjadřující silnou souvislost grafu není formulí, ale stala by se formulí, kdybychom připustili delší než konečné formule: d je dosažitelný z c, jestliže je dosažitelný jedním, nebo dvěma, nebo třemi, nebo ... kroky.

Logika, ve které se připouští kvantifikace přes podmnožiny struktur, se nazývá *logika druhého řádu*. Logika, ve které se připouštějí i delší než konečné konjunkce, disjunkce nebo řetězce kvantifikátorů, se nazývá *nefinitní logikou*. Existuje více variant nefinitní logiky a existují také logiky ještě vyššího než druhého řádu. Fakt, že třída všech dobře uspořádaných struktur nebo třída všech silně souvislých grafů není axiomatizovatelná, se někdy vyjadřuje obratem, že dobré uspořádání nebo silná souvislost grafu není vlastností prvního řádu. Naše kniha je věnována výhradně logice prvního řádu. Pro stručnou úvodní informaci o logikách jiných než logika prvního řádu doporučujeme Barwisův Úvod [5] k příručce [4].

Užití různých zobecnění logiky prvního řádu může někdy zpřehlednit a zestručnit vyjadřování. Jejich společnou vlastností ale je, že pro ně neplatí některá z důležitých vět (o úplnosti, o kompaktnosti, nebo Löwenheimova-Skolemova už ve verzi 3.2.13). Zdá se tedy, že tato zobecnění neohrožují výsadní postavení logiky prvního řádu.

Věta 3.4.5 (Löwenheimova-Skolemova) *Nechť T je teorie s jazykem L, nechť κ je nekonečný kardinál takový, že $|L| \leq \kappa$, a nechť T má nekonečné modely. Pak T má i modely mohutnosti κ.*

Důkaz Vezměme nekonečný model $\mathbf{M}$ teorie T. Dále postupujeme podobně jako v důkazu věty 3.4.2. Vezměme množinu $\{\, c_\alpha \,;\, \alpha < \kappa \,\}$ nových (tj. navzájem různých a nevyskytujících se v L) konstant. Tato množina má mohutnost κ a také jazyk $L' = L \cup \{\, c_\alpha \,;\, \alpha < \kappa \,\}$ má mohutnost κ. Teorii T lze považovat i za teorii v jazyce L'. Označme S množinu všech sentencí tvaru $c_\alpha \neq c_\beta$, kde $\alpha \neq \beta$. Je-li $F \subseteq S$ libovolná konečná, pak $T \cup F$ má model: stačí model $\mathbf{M}$ expandovat na strukturu pro L' tak, že konstanty c_α vyskytující se v F (těch je jen konečně mnoho) jsou realizovány různými prvky modelu $\mathbf{M}$ a ostatní konstanty c_α jsou realizovány libovolnými prvky modelu $\mathbf{M}$. Podle věty o kompaktnosti má teorie $T \cup S$ nějaký model. Podle věty 3.2.13 má tato teorie i model $\mathbf{M}'$ mohutnosti nejvýše $\max\{|L'|, \kappa\}$, tj. mohutnosti nejvýše κ. Protože v $\mathbf{M}'$ platí všechny sentence z S, všechny nové konstanty jsou v $\mathbf{M}'$ realizovány navzájem různými prvky. Model $\mathbf{M}'$ nemůže mít mohutnost menší než κ. Tedy $|\mathbf{M}'| = \kappa$. QED

Z Löwenheimovy-Skolemovy věty plyne například to, že $\mathrm{Th}(\mathbf{N})$, teorie struktury přirozených čísel, má i nespočetné modely, a má dokonce modely libovolné nespočetné mohutnosti κ. Tento fakt se na první pohled může zdát paradoxní, podobně jako představa, že Zermelova-Fraenkelova teorie množin má spočetné modely. Uvažme ale toto. Kdybychom mohli zapsat aritmetickou sentencí, že každé číslo má ve smyslu uspořádání pouze konečně mnoho předchůdců, pak by tato sentence musela platit ve všech modelech teorie $\mathrm{Th}(\mathbf{N})$, a $\mathrm{Th}(\mathbf{N})$ by nemohla mít nespočetné

modely (viz cvičení 10). Fakt, že teorie Th(**N**) má i nespočetné modely, je tedy jeden z faktů, které vysvětlují, proč se nepodařilo to, co se nepodařilo (totiž zapsat v daném jazyce určitou vlastnost struktury), a domníváme se, že nic paradoxního na něm není.

Z Löwenheimovy-Skolemovy věty dále plyne, že třída všech struktur (pro libovolný nejvýše spočetný jazyk) mohutnosti menší než κ, kde κ je nespočetný kardinál, není elementární. V dalším výkladu nás ale více bude zajímat užití věty 3.4.5 v důkazech úplnosti teorií.

Řekneme, že struktury **A** a **B** pro týž jazyk L jsou *elementárně ekvivalentní*, jestliže pro každou sentenci φ v L platí $\mathbf{A} \models \varphi \Leftrightarrow \mathbf{B} \models \varphi$. Jinými slovy, **A** a **B** jsou elementárně ekvivalentní, jestliže se neliší platností žádné sentence. Dosud jsme zjistili, že struktury různé mohutnosti mohou být spolu elementárně ekvivalentní.

- *Existují struktury* **A** *a* **B** *téže mohutnosti, které jsou neizomorfní a přitom elementárně ekvivalentní?*

Dosavadní výsledky dovolují i na tuto otázku odpovědět kladně. Každý model teorie tvaru Th(**D**) je elementárně ekvivalentní s **D**. Z věty 3.4.3 plyne, že jak teorie Th($\langle \mathrm{N}, < \rangle$), tak teorie Th(**N**) mají spočetné modely, které nejsou dobře uspořádané. A dobře uspořádaná struktura samozřejmě nemůže být izomorfní se strukturou, která není dobře uspořádaná.

V dalším výkladu se budeme věnovat také otázce, zda daná teorie má neizomorfní modely dané nebo dokonce každé mohutnosti.

Definice 3.4.6 *Řekneme, že teorie T v jazyce L je* úplná*, jestliže T je bezesporná a neexistuje žádná sentence nezávislá na T, tj. jestliže T je bezesporná a pro každou sentenci φ jazyka L platí $T \vdash \varphi$ nebo $T \vdash \neg\varphi$.*

Příklad 3.4.7 Existují lineárně uspořádané množiny, které mají nejmenší prvek, a existují také lineárně uspořádané množiny, které nejmenší prvek nemají. To podle věty o korektnosti znamená, že sentence $\exists x \forall y \neg(y < x)$ je sentence nezávislá na teorii LO, a teorie LO tedy není úplná.

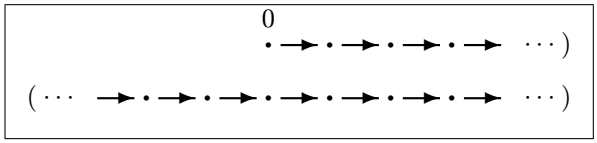
Příklad 3.4.8 Každá teorie tvaru Th(**D**), kde **D** je struktura pro libovolný jazyk, je úplná. Viz 3.1.17(b).

Je důležité, že v definici úplné teorie stojí slovo „sentence“. Nemělo by totiž dobrý smysl požadovat, aby pro každou *formuli* φ platilo $T \vdash \varphi$ nebo $T \vdash \neg\varphi$. Vezměme například za φ formuli $x = y$. Pokud platí $T \vdash \neg\varphi$, pak (vzhledem k pravidlu generalizace) platí i $T \vdash \forall x \forall y(x \neq y)$. To ale pro bezespornou teorii T není možné. Pokud platí $T \vdash \varphi$, pak (opět díky generalizaci) platí i $T \vdash \forall x \forall y(x = y)$, a tedy všechny modely teorie T jsou pouze jednoprvkové. Podmínka, že pro každou formuli φ platí $T \vdash \varphi$ nebo $T \vdash \neg\varphi$, je tedy splněna jen pro nezajímavé teorie T.

Poznamenejme ještě, že v definici 3.4.6 je slovo „úplnost“ užito v jiném smyslu, než ve větě o úplnosti. O pojmu „úplná teorie“ lze říci opak toho, co jsme řekli o

větě o kompaktnosti. „Úplná teorie“ je syntaktický pojem, kterému rozumí každý, kdo rozumí definici důkazu. Je to pojem nezávislý na logické sémantice a Tarského definici.

Chceme-li ukázat, že nějaká teorie T je neúplná, je nejpřirozenější postupovat tak, jak je naznačeno v příkladu 3.4.7: najít dva různé modely teorie T, a pak najít sentenci, která platí jen v jednom z nich. Z dosavadního textu je jasné, že úspěch v prvním kroku nezaručuje úspěch ve druhém kroku. Nalezneme-li neizomorfní modely $\mathbf{M}_1$ a $\mathbf{M}_2$, může se stát, že $\mathbf{M}_1$ a $\mathbf{M}_2$ jsou elementárně ekvivalentní, a neliší se tedy platností žádné sentence. Jinak řečeno, nedaří-li se nalézt sentenci nezávislou na teorii T, je naděje, že T je úplná, a to i v případě, kdy víme o existenci různých (sobě nepodobných) modelů teorie T.



Obrázek 3.4.1: Model $\langle \mathrm{N}, 0, \mathrm{s}\rangle + \langle \mathrm{Z}, \mathrm{s}\rangle$ teorie SUCC

V závěru oddílu 3.2 jsme definovali teorii SUCC, teorii následníka, formulovanou v jazyce $\{0, \mathrm{S}\}$. Její axiomy jsme vypozorovali ze struktury $\langle \mathrm{N}, 0, \mathrm{s}\rangle$ přirozených čísel s nulou a s následnickou funkcí. Snadno lze ověřit, že teorie SUCC má i jiné modely než $\langle \mathrm{N}, 0, \mathrm{s}\rangle$. Jeden z nich je na obrázku 3.4.1. Jeho nosná množina je disjunktním sjednocením množiny všech přirozených čísel a množiny všech celých čísel. Symbol S je realizován „normálně“, přičítáním jedničky v obou částech modelu, symbol 0 je realizován přirozenou (nikoliv celočíselnou) nulou. Mělo by být zřejmé, že tato struktura je opravdu modelem teorie SUCC a že není izomorfní se strukturou $\langle \mathrm{N}, 0, \mathrm{s}\rangle$. Žádný izomorfismus totiž nemůže zobrazit objekt, který je z nuly dosažitelný konečně mnoha skoky následnické funkce, na objekt, který tuto vlastnost nemá.

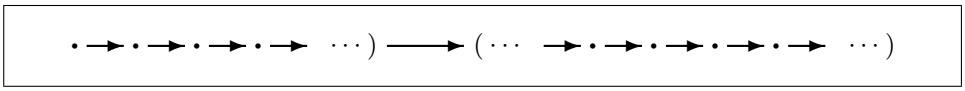
Do podobné situace lze dospět, budeme-li uvažovat o struktuře $\langle \mathrm{N}, <\rangle$ a domyslíme-li trochu dále to, co bylo řečeno v příkladu 3.4.7. Nejenže celá struktura má nejmenší prvek, ale také ke každému prvku x existuje nejmenší mezi většími. A dále, ke každému prvku x existuje největší mezi prvky menšími než x, pokud ovšem existují nějaké prvky menší než x. Definujme tedy teorii DO (discrete order) *diskrétního uspořádání* jako teorii s jazykem $\{<\}$, jejímiž axiomy jsou axiomy teorie LO a dále následující tři axiomy:

DO1: $\exists x \forall y \neg(y < x)$,

DO2: $\forall x \exists y (x < y \ \&\ \neg\exists v (x < v \ \&\ v < y))$,

DO3: $\forall x \forall y (y < x \rightarrow \exists z (z < x \ \&\ \neg\exists v (z < v \ \&\ v < x)))$.

Také teorie DO má i jiné modely, než je „preferovaný“ model $\langle \mathrm{N}, <\rangle$. Jeden z nich je na obrázku 3.4.2. Také tento model je disjunktním sjednocením dvou struktur.



Obrázek 3.4.2: Model $\langle \mathrm{N}, < \rangle + \langle \mathrm{Z}, < \rangle$ teorie DO

Šipky tentokrát neoznačují následnickou funkci, ale uspořádání. Neznázornili jsme spoustu „samozřejmých“ šipek, totiž ty, jejichž existence plyne z faktu, že uspořádání je tranzitivní. Delší šipkou mezi „oblastmi“ $\langle \mathrm{N}, < \rangle$ a $\langle \mathrm{Z}, < \rangle$ je znázorněno, že všechny objekty z oblasti $\langle \mathrm{N}, < \rangle$ jsou menší než všechny objekty z oblasti $\langle \mathrm{Z}, < \rangle$. Toto je důležitý rozdíl mezi modely teorií SUCC a DO. Na obrázku 3.4.2 jsou oblasti $\langle \mathrm{N}, < \rangle$ a $\langle \mathrm{Z}, < \rangle$ „za sebou“, na obrázku 3.4.1 jsou „vedle sebe“, neboť mezi oblastmi $\langle \mathrm{N}, 0, \mathrm{s} \rangle$ a $\langle \mathrm{Z}, \mathrm{s} \rangle$ není žádná „vazba“.

V závěru oddílu 3.2 jsme také definovali teorii DNO hustého lineárního uspořádání bez minima a maxima. O modelech teorie DNO se brzy zmíníme. Společnou vlastností všech tří teorií SUCC, DO a DNO je to, že pro žádnou z nich nejsme schopni podat příklad nezávislé sentence. Všechny tři tedy pokládejme za kandidáty na úplnou teorii.

Definice 3.4.9 *Nechť κ je nekonečný kardinál. Řekneme, že teorie T je κ-kategorická, jestliže každé dva modely teorie T mohutnosti κ jsou spolu izomorfní.*

Příklad 3.4.10 Každá ze struktur $\langle \mathrm{R} - \{0\}, < \rangle$ (všech nenulových reálných čísel s uspořádáním) a $\langle \mathrm{R}, < \rangle$ (všech reálných čísel s uspořádáním) je modelem teorie DNO. V první z nich neplatí a v druhé naopak platí věta o supremu. Tyto struktury tedy nejsou spolu izomorfní. Obě ale mají stejnou mohutnost $2^{\aleph_0}$. Teorie DNO tedy není $2^{\aleph_0}$-kategorická. Fakt, že struktury $\langle \mathrm{R} - \{0\}, < \rangle$ a $\langle \mathrm{R}, < \rangle$ nejsou izomorfní, zdůvodníme pro jistotu podrobněji. Postupujme sporem. Nechť $f : (\mathrm{R} - \{0\}) \to \mathrm{R}$ je izomorfismus obou struktur, tedy vzájemně jednoznačná funkce, která zachovává uspořádání. Vezměme množiny $A = \{\, f(x) \,;\, x < 0 \,\}$ a $B = \{\, f(x) \,;\, x > 0 \,\}$. Je-li $y_1 \in A$ a $y_2 \in B$, pak $y_1 = f(x_1)$ pro jisté $x_1 < 0$ a $y_2 = f(x_2)$ pro jisté $x_2 > 0$. Protože f zachovává uspořádání, platí $y_1 < y_2$. Tím jsme ověřili, že libovolný prvek množiny A je menší než libovolný prvek množiny B. Množina A nemá maximum, protože když $y \in A$, $y = f(x)$ a $x < 0$, pak $x < \frac{x}{2} < 0$, a tedy $f(\frac{x}{2})$ je prvek množiny A větší než y. Z analogického důvodu B nemá minimum. Tím jsme dospěli ke sporu: z věty o supremu plyne, že jsou-li A a B neprázdné navzájem komplementární množiny reálných čísel takové, že všechny prvky množiny A jsou menší než všechny prvky množiny B, pak A má maximum nebo B má minimum.

Příklad 3.4.11 Nechť L je prázdný jazyk (tedy všechny formule jazyka L jsou sestaveny z atomických formulí tvaru $x = y$). Pak struktura pro L je plně určena svou nosnou množinou. Je-li f libovolná vzájemně jednoznačná funkce z množiny D_1 na množinu D_2, pak f je automaticky izomorfismus, protože f zachovává realizace všech symbolů jazyka L. Pokud D_1 a D_2 mají stejnou mohutnost, pak vzájemně

jednoznačná funkce z D_1 na D_2 existuje. Tím je ověřeno, že libovolná teorie T s prázdným jazykem je κ-kategorická pro každý nekonečný kardinál κ.

Příklad 3.4.12 Rozmysleme si, že teorie DNO je $\aleph_0$-kategorická. Nechť $\langle A, <_1\rangle$ a $\langle B, <_2\rangle$ jsou libovolné dva její spočetné modely. Očíslujme jejich nosné množiny: $A = \{a_0, a_1, a_2, \dots\}$, $B = \{b_0, b_1, b_2, \dots\}$. Izomorfismus $f : A \to B$ obou struktur sestrojíme jako sjednocení spočetně mnoha konečných funkcí $f_0 \subseteq f_1 \subseteq \dots$ Posloupnost $\{\, f_n \,;\, n \in \mathrm{N} \,\}$ konstruujme rekurzí. Položme $f_0 = \emptyset$. V kroku $2n$ máme konečné množiny $C \subseteq A$ a $D \subseteq B$ a prostou funkci f_{2n} z C na D. Přitom platí $\{a_0, \dots, a_{n-1}\} \subseteq C$, $\{b_0, \dots, b_{n-1}\} \subseteq D$ a pro libovolná $c_1, c_2 \in C$ platí $f_{2n}(c_1) <_2 f_{2n}(c_2)$, právě když $c_1 <_1 c_2$. Uvažujme o a_n. Pokud $a_n \in C$, neděláme nic a položíme $f_{2n+1} = f_{2n}$. Pokud $a_n \notin C$, určíme polohu prvku a_n vůči prvkům množiny C. Když a_n je větší než všechny, zvolíme za jeho obraz libovolný prvek b množiny B větší než všechny prvky množiny D. To lze, žádný prvek množiny D není maximální v B, protože struktura $\langle B, <_2\rangle$ žádné maximum nemá. Podobně postupujeme, když a_n je menší než všechny prvky množiny C. Zbývá případ, kdy některé prvky množiny C jsou menší a některé větší než a_n. Tehdy označme c_1 největší z oněch menších a c_2 nejmenší z oněch větších. Platí tedy $c_1 <_1 a_n <_1 c_2$. Zvolme b libovolně tak, aby platilo $f_{2n}(c_1) <_2 b <_2 f_{2n}(c_2)$. To lze, interval $(\!(f_{2n}(c_1), f_{2n}(c_2))\!)$ je neprázdný, protože $\langle B, <_2\rangle$ je hustě uspořádaná množina. Nakonec položme $f_{2n+1} = f_{2n} \cup \{[a_n, b]\}$. Zcela analogicky postupujme v kroku $2n+1$: není-li b_n v D, zvolíme $a \in A$ tak, aby funkce $f_{2n+2} = f_{2n+1} \cup \{[a, b_n]\}$ neporušovala uspořádání.

Příklad 3.4.13 Z komentáře k obrázku 3.4.1 je jasné, že teorie SUCC není $\aleph_0$-kategorická. Udělejme si lepší představu, jak vypadají její modely. Nechť $\mathbf{D} = \langle D, e, f\rangle$ je libovolný model teorie SUCC. Tedy $e \in D$ a $f : D \to D$. Z platnosti axiomů plyne, že f je prostá funkce a pro její obor hodnot platí $\mathrm{Rng}(f) = D - \{e\}$. Definujme na D relaci $\sim$ takto: $a \sim b$, jestliže některý prvek dvojice $\{a, b\}$ je z druhého dosažitelný konečně mnoha skoky funkce f. Relace $\sim$ je ekvivalence (cvičení: jak toto plyne z platnosti axiomů teorie SUCC v $\mathbf{D}$?) a každá třída rozkladu je nekonečná (cvičení: jak toto plyne ...). Třída rozkladu obsahující e je izomorfní se strukturou $\langle \mathrm{N}, 0, \mathrm{s}\rangle$, každá jiná třída rozkladu je izomorfní se strukturou $\langle \mathrm{Z}, \mathrm{s}\rangle$. Jiné třídy ovšem nemusí existovat. Pokud ale celá množina D má nespočetnou mohutnost κ, třídy izomorfní se $\langle \mathrm{Z}, \mathrm{s}\rangle$ existovat musí a musí jich být κ. Sjednocení méně než κ spočetných množin má totiž mohutnost menší než κ a sjednocení více než κ disjunktních neprázdných množin má naopak mohutnost větší než κ. Model $\mathbf{D}$ mohutnosti κ má tedy jedinou možnou podobu: κ kopií struktury $\langle \mathrm{Z}, \mathrm{s}\rangle$ plus jedna kopie struktury $\langle \mathrm{N}, 0, \mathrm{s}\rangle$. Tím jsme dokázali, že teorie SUCC je κ-kategorická pro každý nespočetný kardinál κ.

Příklad 3.4.14 Rozmysleme si, že podobně lze charakterizovat také modely teorie DO. Nechť $\mathbf{D} = \langle D, <\rangle$ je libovolný model teorie DO. Definujme na množině D relaci podobnou jako v příkladu 3.4.13: $a \sim b$, jestliže mezi a a b je v $\mathbf{D}$ jen konečně mnoho prvků. Opět platí, že relace $\sim$ je ekvivalence a že každá třída

rozkladu je nekonečná. Podobně jako v příkladu 3.4.13 je jedna z tříd rozkladu izomorfní se strukturou $\langle \mathrm{N}, < \rangle$ a všechny ostatní jsou izomorfní se strukturou $\langle \mathrm{Z}, < \rangle$. Na rozdíl od příkladu 3.4.13 nyní ale nemůžeme tvrdit, že různé modely se liší pouze počtem tříd izomorfních se $\langle \mathrm{Z}, < \rangle$. Záleží totiž také na tom, jaké podmínky tvaru $a < b$ platí pro a a b z různých tříd rozkladu. Označme $[a]$ třídu rozkladu obsahující prvek a a definujme relaci R na faktorové množině $D/\!\sim$ předpisem $[a]\ R\ [b] \Leftrightarrow a < b\ \&\ \neg(a \sim b)$. Struktura $\langle D/\!\sim, R \rangle$ je lineárně uspořádaná množina, která má nejmenší prvek. Model **D** tedy vypadá takto: na začátku je oblast izomorfní se strukturou $\langle \mathrm{N}, < \rangle$, pak následuje blíže neurčený počet oblastí izomorfních se strukturou $\langle \mathrm{Z}, < \rangle$, které jsou *nějak* lineárně uspořádány. Jinými slovy, každý model teorie DO vznikl z nějaké lineárně uspořádané struktury $\langle M, R \rangle$ s nejmenším prvkem tak, že nejmenší prvek byl nahrazen oblastí izomorfní s $\langle \mathrm{N}, < \rangle$, každý z ostatních prvků byl nahrazen oblastí izomorfní se $\langle \mathrm{Z}, < \rangle$, přičemž uspořádání uvnitř oblastí zůstalo zachováno, a uspořádání mezi prvky různých oblastí určila relace R. Domluvme se, že bude-li se to hodit, uspořádané struktury budeme značit malými řeckými písmeny. Jsou-li γ a λ uspořádané množiny, pak $\gamma + \lambda$ je jejich disjunktní sjednocení (tj. struktura sestávající ze dvou oblastí, z nichž jedna je izomorfní s γ a všechny její prvky jsou menší než všechny prvky druhé oblasti, která je izomorfní s λ). Součinem $\gamma \cdot \lambda$ značíme strukturu vzniklou nahrazením každého prvku struktury λ kopií struktury γ. Označme ještě λ^* strukturu vzniklou z λ obrácením všech šipek a označme ω strukturu $\langle \mathrm{N}, < \rangle$. Na obrázku 3.4.2 je tedy struktura $\omega + \omega^* + \omega$. V tomto příkladu jsme si rozmysleli, že každý model teorie DO je ω, nebo je tvaru $\omega + (\omega^* + \omega) \cdot \lambda$, kde λ je nějaká lineárně uspořádaná množina. Na druhé straně každá struktura tvaru $\omega + (\omega^* + \omega) \cdot \lambda$ je modelem teorie DO. Uvážíme-li ještě, že modely tvaru $\omega + (\omega^* + \omega) \cdot \lambda_1$ a $\omega + (\omega^* + \omega) \cdot \lambda_2$ jsou izomorfní pouze v případě, kdy λ_1 a λ_2 jsou izomorfní (cvičení), a že pro každý nekonečný kardinál κ existují neizomorfní lineárně uspořádané množiny mohutnosti κ (cvičení), dokázali jsme, že teorie DO není κ-kategorická pro žádný nekonečný kardinál κ.

To, že v žádném z našich příkladů není uvedena teorie, která by byla κ-kategorická jen pro některý nespočetný kardinál κ, není náhoda. M. Morley dokázal, že je-li T teorie s nejvýše spočetným jazykem, která je κ-kategorická pro některý nespočetný kardinál κ, pak T je κ-kategorická pro každý nespočetný kardinál κ. Morleyova věta tedy pro teorii T se spočetným jazykem připouští pouze čtyři možnosti: (i) T není κ-kategorická pro žádný nekonečný kardinál κ, (ii) T je $\aleph_0$-kategorická, ale není κ-kategorická pro žádný nespočetný kardinál κ, (iii) T není $\aleph_0$-kategorická, je ale κ-kategorická pro každý nespočetný kardinál κ, (iv) T je κ-kategorická pro každý nekonečný kardinál κ. Důkaz Morleyovy věty je (prý) dost obtížný. V dalším výkladu ji ale nebudeme potřebovat.

Věta 3.4.15 (Vaughtova) *Nechť T je bezesporná teorie v jazyce L, která nemá žádné konečné modely, nechť κ je nekonečný kardinál takový, že $|L| \leq \kappa$ a T je κ-kategorická. Pak T je úplná.*

Důkaz Nechť T není úplná. Existuje tedy sentence φ taková, že $T \nvdash \varphi$ a $T \nvdash \neg\varphi$. Podle lemmatu 3.2.7(d) jsou obě teorie T, φ a $T, \neg\varphi$ bezesporné. Každá z nich má tedy nějaký model, a to nekonečný model, protože T nemá konečné modely. Díky Löwenheimově-Skolemově větě 3.4.5 má každá z nich i model mohutnosti κ. Nechť tedy $\mathbf{M}_1$ a $\mathbf{M}_2$ jsou struktury pro L mohutnosti κ takové, že $\mathbf{M}_1 \models T, \varphi$ a $\mathbf{M}_2 \models T, \neg\varphi$. Je jasné, a také to plyne z lemmatu 3.2.11(b), že struktury $\mathbf{M}_1$ a $\mathbf{M}_2$ nejsou izomorfní, neboť se liší platností sentence φ. Struktury $\mathbf{M}_1$ a $\mathbf{M}_2$ jsou tedy dvěma neizomorfními modely teorie T mohutnosti κ. To je spor s předpokladem, že T je κ-kategorická. QED

Dříve jsme zjistili, že teorie DNO je $\aleph_0$-kategorická a že teorie SUCC je κ-kategorická pro každý nespočetný kardinál κ. Podle Vaughtovy věty jsou tedy obě teorie úplné. To má zajímavé důsledky i pro toho, kdo uvažuje raději o strukturách než o teoriích. Například struktury $\langle \mathrm{R}, < \rangle$, $\langle \mathrm{R} - \{0\}, < \rangle$ a $\langle \mathrm{R} - \mathrm{Q}, < \rangle$ jsou modely téže úplné teorie, totiž DNO, a neliší se tedy platností žádné sentence. Jinak řečeno, jsou elementárně ekvivalentní. Také struktura z obrázku 3.4.1 je elementárně ekvivalentní se strukturou $\langle \mathrm{N}, 0, \mathrm{s} \rangle$. Model $\langle \mathrm{N}, 0, \mathrm{s} \rangle + \langle \mathrm{Z}, \mathrm{s} \rangle$ tedy nelze zakázat přidáním dalších axiomů k teorii SUCC. Každá teorie tvaru $\mathsf{SUCC} \cup \{\varphi\}$, kde φ je sentence v jazyce $\{0, \mathrm{S}\}$, má totiž buď tytéž modely jako teorie SUCC, nebo nemá žádné modely (podle toho, platí-li $\mathsf{SUCC} \vdash \varphi$ nebo $\mathsf{SUCC} \vdash \neg\varphi$).

Tím se nám podařilo odpovědět na zbývající otázky 3 a 4 ze závěru oddílu 3.1. Ne, neizomorfní a sobě nepodobné struktury $\mathbf{D}_1$ a $\mathbf{D}_2$ se nemusí lišit platností žádné sentence, a ano, může se stát, že všechny sentence platné v nějaké struktuře vyplývají z nějaké přehledné množiny předpokladů.

Nyní je také lépe vidět, proč jsme věty o úplnosti a kompaktnosti (v této kapitole a již dříve v kapitole 1) formulovali pro libovolné jazyky. Nebylo to ani tak ve snaze o co nejobecnější výsledky, ale proto, že úvahy o nespočetných modelech a nekonečných nebo (v důkazu věty 3.4.5) dokonce nespočetných jazycích mají důsledky i pro teorie „ze života“, které většinou mají konečný jazyk a konečně mnoho axiomů nebo axiomatických schémat. Teorie s nespočetnými jazyky tedy nepokládáme za důležitý předmět zkoumání, ale spíš za důležitý nástroj, který může pomoci zjistit něco i o těch teoriích, které nás zajímají především. Za obzvláště zajímavé pokládáme ty situace, kdy ověření nějaké abstraktní podmínky (například že formule φ platí ve všech modelech teorie T, nebo že každé dva modely téže mohutnosti κ jsou spolu izomorfní) má za následek existenci nějakého konkrétního objektu, který lze zapsat pomocí konečně mnoha symbolů (například určitého důkazu).

Ve zbytku tohoto oddílu ukážeme ještě další sémantické metody a konstrukce. Na začátku oddílu jsme uvažovali otázku, zda daná třída struktur je axiomatizovatelná. V dalším budeme řešit podrobnější otázku: je daná třída axiomatizovatelná pomocí nějaké množiny sentencí, které jsou syntakticky jednoduché v tom smyslu, že se v nich nestřídá příliš mnoho kvantifikátorů? Také otázka, zda teorie DO je úplná, zůstává zatím nezodpovězená. Nejprve ale ukážeme, že Hilbertova-Ackermannova věta, kterou jsme již dokázali důkazově teoreticky v oddílu 3.3, má i celkem snadný sémantický důkaz.

V oddílu 3.2 jsme definovali homomorfismus struktur **A** a **B** jako funkci f z **A** do **B**, která zachovává všechny funkční i predikátové symboly. Podmínku, že f zachovává rovnítko, lze zapsat ekvivalencí

$$\forall a \forall b(\mathbf{A} \models (x = y)[a, b] \Leftrightarrow \mathbf{B} \models (x = y)[f(a), f(b)]).$$

Protože v predikátové logice s rovností je rovnítko realizováno rovností (v **A** i v **B**), lze tuto podmínku přepsat na

$$\forall a \forall b(a = b \Leftrightarrow f(a) = f(b)).$$

Funkce f tedy zachovává symbol „=“, právě když je prostá. V predikátové logice s rovností (ve které se rovnítko považuje za logický symbol) tedy definujeme *homomorfismus* struktur **A** a **B** pro jazyk L jako prostou funkci z A do B, která zachovává všechny (mimologické) symboly jazyka L. Lemma 3.2.11(a) se vztahuje i na predikátovou logiku s rovností: každý homomorfismus automaticky zachovává všechny otevřené formule. Místo homomorfismus struktur **A** a **B** budeme nadále říkat *vnoření* struktury **A** do struktury **B**.

Jsou-li **A** a **B** struktury pro týž jazyk L a je-li f vnoření struktury **A** do struktury **B**, pak f je zároveň izomorfismus struktury **A** a jisté podstruktury struktury **B**, neboli struktura **B** je rozšířením jisté struktury izomorfní se strukturou **A**. Naopak, je-li **A** podstruktura struktury **B**, pak identická funkce (z A do B) je vnoření struktury **A** do struktury **B**. Z toho je vidět, že pojem vnoření je vzájemně zaměnitelný s dvojicí pojmů podstruktura (případně rozšíření struktury) a izomorfismus. Pokud **A** je podstruktura struktury **B** a identická funkce z A do B zachovává formuli φ, řekneme, že φ je *absolutní* (pro podstrukturu **A** struktury **B**). Otevřené formule jsou vždy absolutní. Tím jsme znovu vyřešili cvičení 20(a) oddílu 3.1.

Věta 3.4.16 (Hilbertova-Ackermannova) *Nechť $\varphi(v, x_1, \ldots, x_k)$ je otevřená formule v jazyce L taková, že formule $\exists v \varphi(v, \underline{x})$ je logicky platná. Pak existují termy $t_1(\underline{x}), \ldots, t_n(\underline{x})$ v jazyce L takové, že disjunkce $\varphi(t_1(\underline{x}), \underline{x}) \vee \ldots \vee \varphi(t_n(\underline{x}), \underline{x})$ je logicky platná.*

Důkaz Předpokládejme, že formule $\bigvee_{i=1}^{n} \varphi(t_i(\underline{x}), \underline{x})$ není pro žádnou n-tici termů $t_1(\underline{x}), \ldots, t_n(\underline{x})$ logicky platná, tj. že pro každou n-tici $t_1(\underline{x}), \ldots, t_n(\underline{x})$ existuje struktura **D** a ohodnocení e, které formuli $\neg\varphi(t_1(\underline{x}), \underline{x}) \,\&\, \ldots \,\&\, \neg\varphi(t_n(\underline{x}), \underline{x})$ splňuje ve struktuře **D**. Přidejme k jazyku L nové konstanty $c_1, \ldots, c_k$ a definujme teorii T jako množinu všech sentencí v $L \cup \{c_1, \ldots, c_k\}$ tvaru $\neg\varphi(t(c_1, \ldots, c_k), c_1, \ldots, c_k)$, kde t je term v L neobsahující jiné volné proměnné než $x_1, \ldots, x_k$. Je jasné, že každá konečná množina $F \subseteq T$ má model. Podle věty o kompaktnosti existuje tedy struktura **B** pro jazyk $L \cup \{c_1, \ldots, c_k\}$, která je modelem teorie T. Vezměme za **A** podstrukturu struktury **B** generovanou prvky $c_1^{\mathbf{B}}, \ldots, c_k^{\mathbf{B}}$, tj. podstrukturu sestávající ze všech prvků množiny B tvaru $(t(c_1, \ldots, c_k))^{\mathbf{B}}$. Protože formule $\exists v \varphi(v, \underline{x})$ je logicky platná, ke každé k-tici prvků libovolné struktury **D** existuje prvek $b \in \mathbf{D}$ takový,

že $\mathbf{D} \models \varphi[b, \underline{a}]$. Zvolme za $\mathbf{D}$ strukturu $\mathbf{A}$ a za $a_1, \ldots, a_k$ její prvky $c_1^{\mathbf{B}}, \ldots, c_k^{\mathbf{B}}$. Pro některý z prvků $(t(\underline{c}))^{\mathbf{B}}$ struktury $\mathbf{A}$ tedy platí $\mathbf{A} \models \varphi[(t(\underline{c}))^{\mathbf{B}}, c_1^{\mathbf{B}}, \ldots, c_k^{\mathbf{B}}]$. Protože otevřené formule jsou absolutní, platí i $\mathbf{B} \models \varphi[(t(\underline{c}))^{\mathbf{B}}, c_1^{\mathbf{B}}, \ldots, c_k^{\mathbf{B}}]$. Užít hodnotu uzavřeného termu jako ohodnocení nějaké proměnné je podle lemmatu 3.1.14(b) totéž, jako substituovat onen term za onu proměnnou. Tedy $\mathbf{B} \models \varphi(t(\underline{c}), \underline{c})$. To je spor, protože $\mathbf{B} \models T$, a přitom sentence $\neg\varphi(t(\underline{c}), \underline{c})$ je jeden z axiomů teorie T. QED

Zvolme pevně jazyk L a definujme množiny formulí U_n a E_n jazyka L. Množina U_n je množina všech formulí tvaru

$$\forall v_{1,1} \ldots \forall v_{1,r_1} \exists v_{2,1} \ldots \exists v_{2,r_2} \forall v_{3,1} \ldots \quad \ldots v_{n,r_n} \varphi,$$

kde φ je otevřená formule. Kvantifikátory u proměnných $v_{n,1}$ až v_{n,r_n} jsou všechny existenční nebo všechny univerzální podle toho, zda n je sudé nebo liché. Každá formule v U_n je tedy formule v prenexním tvaru, jejíž kvantifikátory lze rozdělit do nejvýše n souvislých bloků obsahujících kvantifikátory stejného druhu. Velikost bloků určují čísla $r_1, \ldots, r_n$. Každé z nich může být rovno nule. U_0 je množina všech otevřených formulí. Množina U_{n+1} sestává ze všech otevřených formulí a dále ze všech prenexních formulí, v jejichž kvantifikátorovém prefixu je nejvýše n „střídání“ kvantifikátorů, a je-li jich přesně n, pak první kvantifikátor musí být univerzální (je-li jich méně, můžeme si myslet, že na začátku je několik bloků nulové délky). Množinu formulí E_n definujme duálně jako množinu všech formulí tvaru

$$\exists v_{1,1} \ldots \exists v_{1,r_1} \forall v_{2,1} \ldots \forall v_{2,r_2} \exists v_{3,1} \ldots \quad \ldots v_{n,r_n} \varphi,$$

kde φ je otevřená formule. Formule v U_1 a E_1 jsou tedy tytéž, kterým se v oddílu 3.2 říkalo *univerzální* resp. *existenční* formule. Platí $\mathrm{U}_n \cup \mathrm{E}_n \subseteq \mathrm{U}_{n+1} \cap \mathrm{E}_{n+1}$ pro každé n. Formulím v U_2 se někdy říká *induktivní* formule.

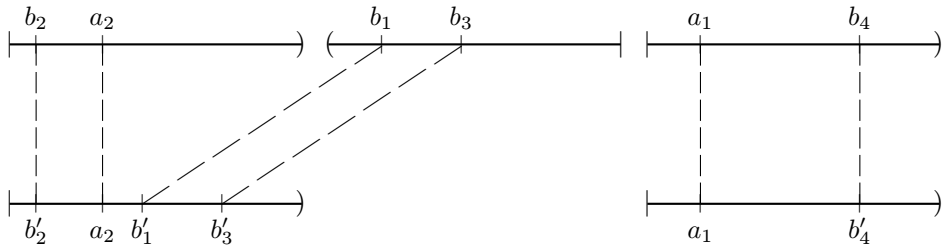
Řekneme, že vnoření f struktury $\mathbf{A}$ do struktury $\mathbf{B}$ je *n-elementární*, jestliže f zachovává všechny U_n-formule. Vnoření f je *elementární*, jestliže f zachovává všechny formule. Podstruktura $\mathbf{A}$ struktury $\mathbf{B}$ je *n-elementární* nebo *elementární*, jestliže identická funkce z A do B je n-elementární resp. elementární vnoření, tj. jestliže všechny formule v U_n resp. vůbec všechny formule jsou absolutní pro $\mathbf{A}$ a $\mathbf{B}$. Pišme $f : \mathbf{A} \to_n \mathbf{B}$ nebo $f : \mathbf{A} \to_{\mathrm{e}} \mathbf{B}$, jestliže f je n-elementární resp. elementární vnoření $\mathbf{A}$ do $\mathbf{B}$, a pišme $\mathbf{A} \prec_n \mathbf{B}$ nebo $\mathbf{A} \prec \mathbf{B}$, jestliže $\mathbf{A}$ je n-elementární resp. elementární podstruktura struktury $\mathbf{B}$.

Lemma 3.4.17 *(a) Každé vnoření je 0-elementární.*
(b) Vnoření f struktury $\mathbf{A}$ do struktury $\mathbf{B}$ je n-elementární, právě když f zachovává všechny E_n-formule.
(c) Platí-li $f : \mathbf{A} \to_n \mathbf{B}$, pak pro každou formuli $\varphi(x_1, \ldots, x_k)$ v U_{n+1}, každou formuli $\psi(x_1, \ldots, x_k)$ v E_{n+1} a každou k-tici $a_1, \ldots, a_k$ prvků z A platí implikace $\mathbf{A} \models \psi[\underline{a}] \Rightarrow \mathbf{B} \models \psi[f(a_1), \ldots, f(a_k)]$ a $\mathbf{B} \models \varphi[f(a_1), \ldots, f(a_k)] \Rightarrow \mathbf{A} \models \varphi[\underline{a}]$.
(d) Když vnoření f struktury $\mathbf{A}$ do struktury $\mathbf{B}$ je n-elementární pro každé n, pak $f : \mathbf{A} \to_{\mathrm{e}} \mathbf{B}$.

(e) Když existuje f takové, že $f : \mathbf{A} \to_{\mathrm{e}} \mathbf{B}$, pak $\mathbf{A}$ a $\mathbf{B}$ jsou elementárně ekvivalentní.
(f) Když $f : \mathbf{A} \to_n \mathbf{B}$ a $g : \mathbf{B} \to_n \mathbf{C}$, pak $g \circ f : \mathbf{A} \to_n \mathbf{C}$.

Důkaz Když vnoření f zachovává formuli $\varphi(x_1, .., x_k)$, pak f zachovává i její negaci $\neg\varphi(x_1, .., x_k)$. Když φ je v U_n nebo v E_n, pak $\neg\varphi$ je ekvivalentní s formulí v E_n resp. v U_n. Tím je zdůvodněno (b). Tvrzení (d) plyne z toho, že každá formule je ekvivalentní s prenexní formulí a každá prenexní formule je v některé z množin U_n. V definici toho, že f zachovává formuli $\varphi(x_1, .., x_k)$, má smysl i případ $k = 0$. Když f zachovává všechny formule, pak f zachovává i všechny sentence. Odtud plyne (e). QED

Příklad 3.4.18 Struktura $\mathbf{Q}$ racionálních čísel není 1-elementární podstrukturou struktury $\mathbf{R}$ reálných čísel, protože číslo 2 ve struktuře $\mathbf{Q}$ splňuje a ve struktuře $\mathbf{R}$ nesplňuje formuli $\forall v(v^2 \neq x)$.



Obrázek 3.4.3: 1-elementární podstruktura

Příklad 3.4.19 Vezměme jazyk $\{<\}$ a za $\mathbf{B}$ vezměme strukturu $\omega + \omega^* + \omega$. Struktura $\mathbf{B}$ je disjunktním sjednocením tří struktur. Říkejme jim levá, prostřední a pravá část struktury $\mathbf{B}$. Vezměme za $\mathbf{A}$ strukturu $\omega + \omega$ vzniklou z $\mathbf{B}$ vynecháním prostřední části. Pak $\mathbf{A}$ není 2-elementární podstrukturou struktury $\mathbf{B}$, protože nejmenší prvek pravé části splňuje v $\mathbf{A}$ formuli $\forall u(u < x \to \exists v(u < v \ \& \ v < x))$ (která je ekvivalentní s U_2-formulí), ale v $\mathbf{B}$ ji nesplňuje. Rozmyslíme si, že $\mathbf{A}$ je 1-elementární podstruktura struktury $\mathbf{B}$. Podle lemmatu 3.4.17(b) stačí ověřit, že každá E_1-formule je absolutní. Nechť je tedy dána E_1-formule $\varphi(\underline{x})$ tvaru $\exists v_1 \, . \, \exists v_r \psi(v_1, .., v_r, x_1, .., x_k)$, kde ψ je otevřená. Máme ověřit, že pro libovolnou k-tici $a_1, .., a_k$ prvků z A platí ekvivalence $\mathbf{A} \models \varphi[\underline{a}] \Leftrightarrow \mathbf{B} \models \varphi[\underline{a}]$. Implikace $\Rightarrow$ je jasná z 3.4.17(c). Nechť $\mathbf{B} \models (\exists \underline{v} \psi)[\underline{a}]$ a nechť $b_1, .., b_r$ jsou prvky z B, pro které platí $\mathbf{B} \models \psi[\underline{b}, \underline{a}]$. Další postup je pro $k = 2$ a $r = 4$ znázorněn na obrázku 3.4.3. Ke každému b_i lze zvolit $b'_i \in A$ tak, aby nedošlo ke křížení přerušovaných čar. Je-li $b_i \in A$, stačí volit $b'_i = b_i$, ostatní b'_i zvolíme jako dost velké prvky levé části struktury $\mathbf{B}$. Nekřížení čar znamená, že $(r + k)$-tice $[b'_1, .., b'_r, a_1, .., a_k]$ a $[b_1, .., b_r, a_1, .., a_k]$ splňují stejné atomické formule, a tedy také stejné otevřené formule. Tedy $\mathbf{A} \models \psi[\underline{b'}, \underline{a}]$ a $\mathbf{A} \models \varphi[\underline{a}]$.

Příklad 3.4.20 Nechť $\mathbf{M}$ je libovolná struktura pro aritmetický jazyk, která je modelem teorie $\mathrm{Th}(\mathbf{N})$. Tedy $\mathbf{M}$ a $\mathbf{N}$ jsou elementárně ekvivalentní. Definujme funkci f předpisem $n \mapsto \overline{n}^{\mathbf{M}}$. Je zřejmé, že f je prostá funkce z množiny N všech přirozených čísel do nosné množiny M struktury $\mathbf{M}$. Nechť $\varphi(x_1, \ldots, x_k)$ je libovolná aritmetická formule. Pak $\mathbf{N} \models \varphi[n_1, \ldots, n_k]$ je ekvivalentní s $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_k})$ (protože hodnotou numerálu $\overline{n_i}$ ve struktuře $\mathbf{N}$ je číslo n_i), a $\mathbf{M} \models \varphi[\overline{n_1}^{\mathbf{M}}, \ldots, \overline{n_k}^{\mathbf{M}}]$ je ekvivalentní s $\mathbf{M} \models \varphi(\overline{n_1}, \ldots, \overline{n_k})$. Sentence $\varphi(\overline{n_1}, \ldots, \overline{n_k})$ nemůže platit jen v jedné ze struktur $\mathbf{N}$ a $\mathbf{M}$. Tím je zdůvodněno, že strukturu $\mathbf{N}$ lze elementárně vnořit do každého modelu $\mathbf{M}$ teorie $\mathrm{Th}(\mathbf{N})$.

Úvahu v předchozím příkladu lze zobecnit. Je-li ve struktuře $\mathbf{A}$ každý prvek hodnotou nějakého uzavřeného termu, pak strukturu $\mathbf{A}$ lze elementárně vnořit do jakékoliv struktury $\mathbf{B}$ pro týž jazyk, pokud platí $\mathbf{B} \models \mathrm{Th}(\mathbf{A})$. A spokojíme-li se s vnořením, které není elementární, pak stačí, aby v $\mathbf{B}$ platily všechny otevřené (nebo, což je totéž, všechny atomické) sentence platné v $\mathbf{A}$. Není-li splněna podmínka, že každý prvek struktury $\mathbf{A}$ je hodnotou uzavřeného termu, můžeme ji splnit postupem, který jsme v tomto oddílu užili již několikrát: dočasně rozšíříme jazyk přidáním nových konstant.

Nechť $\mathbf{A}$ je struktura pro jazyk L. Přiřaďme každému prvku $a \in A$ konstantu $\widehat{a}$ tak, aby všechny takto přiřazené konstanty byly navzájem různé a různé od všech konstant jazyka L. Označme L_A rozšíření jazyka L o všechny konstanty $\widehat{a}$, kde $a \in A$. Označme $\mathbf{A}'$ „přirozenou“ expanzi struktury $\mathbf{A}$ pro jazyk L_A, která vznikne z $\mathbf{A}$ tak, že každý prvek a prohlásíme za realizaci konstanty $\widehat{a}$. Definujme $\mathrm{Diag}_n(\mathbf{A})$ a $\mathrm{Diag}_{\mathrm{e}}(\mathbf{A})$ jako množinu všech U_n-sentencí resp. množinu všech sentencí jazyka L_A, které platí ve struktuře $\mathbf{A}'$. Množinám $\mathrm{Diag}_n(\mathbf{A})$ a $\mathrm{Diag}_{\mathrm{e}}(\mathbf{A})$ říkáme *n-elementární diagram* resp. *elementární diagram* struktury $\mathbf{A}$. 0-elementárnímu diagramu se říká prostě *diagram* a místo $\mathrm{Diag}_0(\mathbf{A})$ se píše jen $\mathrm{Diag}(\mathbf{A})$. Označme ještě $\mathrm{Thm}_n(T)$ množinu všech U_n-sentencí dokazatelných v T.

Věta 3.4.21 *Nechť L je jazyk, $\mathbf{A}$ je struktura pro L a T je teorie v jazyce L. Pak $\mathbf{A} \models \mathrm{Thm}_{n+1}(T)$, právě když existuje model $\mathbf{B}$ teorie T a funkce g taková, že $g : \mathbf{A} \to_n \mathbf{B}$.*

Důkaz Nechť $g : \mathbf{A} \to_n \mathbf{B}$ a $\mathbf{B} \models T$. Platí $\mathbf{B} \models \mathrm{Thm}_{n+1}(T)$. Pokud g zachovává všechny U_n- a E_n-formule, pak platnost U_{n+1}-formulí se dle lemmatu 3.4.17(c) přenáší směrem „dolů“. Tedy $\mathbf{A} \models \mathrm{Thm}_{n+1}(T)$. Tím je zdůvodněna implikace $\Leftarrow$.

Nechť $\mathbf{B}'$ je libovolný model teorie $T \cup \mathrm{Diag}_n(\mathbf{A})$ (v jazyce L_A). Označme g funkci $a \mapsto \widehat{a}^{\mathbf{B}'}$ a označme $\mathbf{B}$ redukt struktury $\mathbf{B}'$ pro jazyk L. Podobně jako v příkladu 3.4.20, je-li $\varphi(x_1, \ldots, x_k)$ libovolná formule v U_n a jsou-li $a_1, \ldots, a_k$ prvky množiny A, pak podmínky $\mathbf{A} \models \varphi[\underline{a}]$, $\mathbf{A}' \models \varphi(\widehat{a_1}, \ldots, \widehat{a_k})$, $\mathbf{B}' \models \varphi(\widehat{a_1}, \ldots, \widehat{a_k})$ a $\mathbf{B} \models \varphi[g(a_1), \ldots, g(a_k)]$ jsou ekvivalentní. $\mathbf{B}$ je tedy model teorie T a g je n-elementární vnoření.

Zbývá tedy zdůvodnit, že platí-li $\mathbf{A} \models \mathrm{Thm}_{n+1}(T)$, pak teorie $T \cup \mathrm{Diag}_n(\mathbf{A})$ má nějaký model. Nechť jej nemá. Pak podle věty o silné úplnosti existují sentence $\varphi_1, \ldots, \varphi_m$ v L_A takové, že $\{\varphi_1, \ldots, \varphi_m\} \subseteq \mathrm{Diag}_n(\mathbf{A})$ a $T \vdash \neg(\varphi_1 \,\&\, \ldots \,\&\, \varphi_m)$.

Vezměme důkaz $\mathcal{P}$ sentence $\neg \bigwedge \varphi_i$, utvořme seznam $\widehat{a}_1, \ldots, \widehat{a}_k$ konstant z $L_A - L$, které se v něm vyskytují, a nahraďme v důkazu $\mathcal{P}$ konstanty $\widehat{a}_1, \ldots, \widehat{a}_k$ navzájem různými proměnnými $x_1, \ldots, x_k$ nevyskytujícími se v $\mathcal{P}$. Výsledek $\mathcal{P}'$ této záměny je opět důkazem, a to důkazem z množiny předpokladů T, protože v axiomech teorie T se konstanty $\widehat{a}_i$ nevyskytují. Každou sentenci φ_i můžeme psát ve tvaru $\alpha_i(\widehat{a}_1, \ldots, \widehat{a}_k)$, kde α_i je U_n-formule v jazyce L. Důkaz $\mathcal{P}'$ je tedy důkazem formule $\neg \bigwedge \alpha_i(\underline{x})$. Platí také (díky generalizaci) $T \vdash \forall \underline{x} \neg \bigwedge \alpha_i(\underline{x})$ a $T \vdash \neg \exists \underline{x} \bigwedge \alpha_i(\underline{x})$. Sentence $\neg \exists \underline{x} \bigwedge \alpha_i(\underline{x})$ je ekvivalentní s U_{n+1}-sentencí dokazatelnou v T. Protože $\mathbf{A} \models \mathrm{Thm}_{n+1}(T)$, máme $\mathbf{A} \models \neg \exists \underline{x} \bigwedge \alpha_i(\underline{x})$. Avšak protože prvky $a_1, \ldots, a_k$ realizují konstanty $\widehat{a}_1, \ldots, \widehat{a}_k$ a každá sentence $\alpha_i(\widehat{a}_1, \ldots, \widehat{a}_k)$ (tj. sentence φ_i) je v $\mathrm{Diag}_n(\mathbf{A})$, k-tice $[a_1, \ldots, a_k]$ splňuje v $\mathbf{A}$ formuli $\bigwedge \alpha_i(\underline{x})$. Tedy $\mathbf{A} \models \exists \underline{x} \bigwedge \alpha_i(\underline{x})$, spor. QED

Věta 3.4.22 (Łošova-Tarského) *Teorie T je ekvivalentní s teorií, jejíž všechny axiomy jsou univerzální sentence, právě když každá podstruktura libovolného modelu teorie T je opět modelem teorie T.*

Důkaz Nechť T je ekvivalentní s T', všechny axiomy teorie T' jsou v množině U_1 a přitom $\mathbf{A} \prec_0 \mathbf{B} \models T$. Pak $\mathbf{A} \models T$ vzhledem k tvrzení 3.4.17(c). Nechť naopak T je teorie taková, že kdykoliv $\mathbf{A} \prec_0 \mathbf{B} \models T$, pak $\mathbf{A} \models T$. Vezměme za T' množinu $\mathrm{Thm}_1(T)$. K ověření, že T a T' jsou ekvivalentní, stačí zdůvodnit, že každý model teorie T' je zároveň modelem teorie T. Nechť tedy $\mathbf{A} \models T'$, tj. $\mathbf{A} \models \mathrm{Thm}_1(T)$. Dle věty 3.4.21 lze strukturu $\mathbf{A}$ vnořit do jistého modelu teorie T. Lze také říci, že strukturu $\mathbf{A}$ lze ztotožnit s podstrukturou jistého modelu $\mathbf{B} \models T$. Takže $\mathbf{A} \prec_0 \mathbf{B} \models T$. Dle předpokladu platí $\mathbf{A} \models T$. QED

Lemma 3.4.23 *Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou struktury pro jazyk L a nechť $f : \mathbf{A} \to_1 \mathbf{B}$. Pak existuje struktura $\mathbf{C}$ pro L a vnoření $g : \mathbf{B} \to_0 \mathbf{C}$ takové, že $g \circ f$ je elementární vnoření struktury $\mathbf{A}$ do struktury $\mathbf{C}$.*

Důkaz Vezměme opět rozšíření jazyka L o konstanty $\widehat{a}$ příslušné prvkům $a \in A$. Ve struktuře $\mathbf{A}$ realizujme každou konstantu $\widehat{a}$ „přirozeně“, tj. prvkem a, a ve struktuře $\mathbf{B}$ realizujme každou $\widehat{a}$ prvkem $f(a)$. Tím jsme získali expanze $\mathbf{A}'$ a $\mathbf{B}'$ struktur $\mathbf{A}$ a $\mathbf{B}$ pro jazyk L_A. Funkce f je 1-elementární vnoření struktury $\mathbf{A}'$ do struktury $\mathbf{B}'$. Tedy $\mathbf{B}' \models \mathrm{Diag}_1(\mathbf{A})$. Platí $\mathrm{Thm}_1(\mathrm{Diag}_{\mathrm{e}}(\mathbf{A})) = \mathrm{Diag}_1(\mathbf{A})$. Podle věty 3.4.21 existuje struktura $\mathbf{C}'$ pro jazyk L_A taková, že $\mathbf{C}' \models \mathrm{Diag}_{\mathrm{e}}(\mathbf{A})$, a vnoření $g : \mathbf{B}' \to_0 \mathbf{C}'$. Označme $\mathbf{C}$ redukt struktury $\mathbf{C}'$ pro jazyk L. Je-li $\psi(x_1, \ldots, x_k)$ libovolná formule v L a $a_1, \ldots, a_k$ libovolná k-tice prvků z A, pak podmínky $\mathbf{A} \models \psi[\underline{a}]$, $\mathbf{A}' \models \psi(\widehat{a}_1, \ldots, \widehat{a}_k)$ a (protože $\mathbf{C}' \models \mathrm{Diag}_{\mathrm{e}}(\mathbf{A})$) $\mathbf{C}' \models \psi(\widehat{a}_1, \ldots, \widehat{a}_k)$ jsou ekvivalentní. Protože funkce g je vnořením, musí realizaci libovolné konstanty v $\mathbf{B}'$ zobrazit na realizaci téže konstanty v $\mathbf{C}'$. Tedy $g(f(a_i))$ je realizace konstanty $\widehat{a}_i$ v $\mathbf{C}'$, takže $\mathbf{C}' \models \psi(\widehat{a}_1, \ldots, \widehat{a}_k)$ a $\mathbf{C} \models \psi[g(f(a_1)), \ldots, g(f(a_k))]$ jsou ekvivalentní podmínky. Tedy $g \circ f$ je elementární vnoření. QED

Posloupnost $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2, \ldots$ struktur pro jazyk L je *řetěz*, jestliže pro každé i platí $\mathbf{A}_i \prec_0 \mathbf{A}_{i+1}$, tj. jestliže každá struktura $\mathbf{A}_i$ je podstrukturou struktury $\mathbf{A}_{i+1}$.

Řetěz $\{ \mathbf{A}_i ; i \in \mathrm{N} \}$ je *elementární*, jestliže pro každé i platí $\mathbf{A}_i \prec \mathbf{A}_{i+1}$. *Limitu řetězu* $\{ \mathbf{A}_i ; i \in \mathrm{N} \}$ definujeme jako strukturu $\mathbf{D}$, jejíž nosná množina je $\bigcup_{i\in\mathrm{N}} A_i$ a ve které realizace $I^{\mathbf{D}}$ každého symbolu $I \in L$ je sjednocení jeho realizací $I^{\mathbf{A}_i}$ ve strukturách $\mathbf{A}_i$.

Lemma 3.4.24 *Když* $\{ \mathbf{A}_i ; i \in \mathrm{N} \}$ *je elementární řetěz a* $\mathbf{D}$ *je jeho limita, pak pro každé* i *platí* $\mathbf{A}_i \prec \mathbf{D}$.

Důkaz Nechť i je dáno. Indukcí podle složitosti formule $\varphi(x_1, .., x_k)$ lze dokázat, že každá formule φ je absolutní pro podstrukturu $\mathbf{A}_i$ struktury $\mathbf{D}$. Ukažme si krok pro existenční kvantifikátor. Nechť φ je tvaru $\exists v\psi(v, \underline{x})$, nechť $a_1, .., a_k$ jsou prvky množiny A_i a nechť $\mathbf{D} \models (\exists v\psi)[\underline{a}]$. Existuje tedy prvek $b \in D$ takový, že $\mathbf{D} \models \psi[b, \underline{a}]$. Protože $D = \bigcup_{i\in\mathrm{N}} A_i$, platí $b \in A_j$ pro jisté j. Lze předpokládat $i \leq j$. Indukční předpoklad říká, že ψ je absolutní pro podstrukturu $\mathbf{A}_j$. Tedy $\mathbf{A}_j \models \psi[b, \underline{a}]$ a $\mathbf{A}_j \models (\exists v\psi)[\underline{a}]$. Z $\mathbf{A}_i \prec \mathbf{A}_{i+1} \prec .. \prec \mathbf{A}_j$ plyne $\mathbf{A}_i \prec \mathbf{A}_j$, viz 3.4.17(f). Tedy $\mathbf{A}_i \models (\exists v\psi)[\underline{a}]$. Ostatní úvahy ponecháváme za cvičení. QED

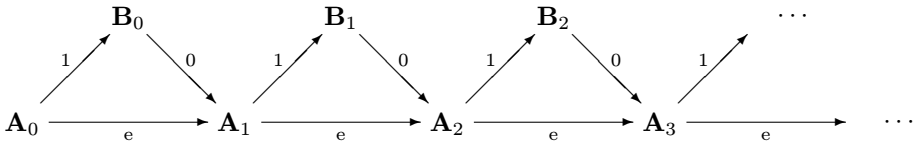
Pojem řetězu a limity řetězu bychom mohli (nepodstatně) zobecnit pro případ, kdy $\{ \mathbf{A}_i ; i \in \mathrm{N} \}$ je posloupnost struktur a $\{ g_i ; i \in \mathrm{N} \}$ je posloupnost funkcí taková, že $g_i : \mathbf{A}_i \to_{\mathrm{e}} \mathbf{A}_{i+1}$. Pro úspornost jsme ale dali přednost jazyku podmodelů a izomorfismů před jazykem vnoření. Takto postupujeme i nadále, ve formulaci a důkazu věty 3.4.25. Lemma 3.4.23 v jazyce podmodelů říká, že když $\mathbf{A} \prec_1 \mathbf{B}$, pak $\mathbf{B}$ je podmodelem jisté struktury $\mathbf{C}$, která je elementárním rozšířením struktury $\mathbf{A}$. A z věty 3.4.21 plyne tento důsledek formulovaný v řeči podmodelů: platí-li $\mathbf{A} \models \mathrm{Thm}_2(T)$, pak $\mathbf{A}$ je 1-elementárním podmodelem jistého modelu teorie T.

Věta 3.4.25 *Teorie* T *je ekvivalentní s teorií, jejíž všechny axiomy jsou sentence v* U_2*, právě když limita libovolného řetězu modelů teorie* T *je opět modelem teorie* T.

Důkaz Nechť $T' \subseteq \mathrm{U}_2$ a T' je ekvivalentní s T, nechť $\mathbf{A}_0 \prec_0 \mathbf{A}_1 \prec_0 \mathbf{A}_2 \prec_0 \ldots$ je řetěz modelů teorie T a nechť $\mathbf{D}$ je jeho limita. Pro každé i platí $\mathbf{A}_i \prec_0 \mathbf{D}$. Nechť $\varphi = \forall x_1 .. \forall x_k \exists y_1 .. \exists y_r \psi(\underline{x}, \underline{y})$ je libovolný prvek množiny T'. Zdůvodníme, že $\mathbf{D} \models \varphi$. Nechť $a_1, .., a_k$ jsou libovolné prvky množiny D. Protože $D = \bigcup A_i$, existuje index j takový, že všechny $a_1, .., a_k$ jsou v A_j. Protože $\mathbf{A}_j \models \varphi$, v $\mathbf{A}_j$ existují $b_1, .., b_r$ takové, že $\mathbf{A}_j \models \psi[\underline{a}, \underline{b}]$. Protože $\mathbf{A}_j \prec_0 \mathbf{D}$, máme $\mathbf{D} \models \psi[\underline{a}, \underline{b}]$ a $\mathbf{D} \models (\exists y_1 .. \exists y_r \psi(\underline{x}, \underline{y}))[\underline{a}]$. Tím je ověřena implikace $\Rightarrow$.

Nechť naopak T splňuje podmínku, že limita libovolného řetězu modelů teorie T je opět modelem teorie T. Vezměme za T' množinu $\mathrm{Thm}_2(T)$. Máme dokázat, že je-li $\mathbf{A}$ libovolný model teorie T', pak $\mathbf{A} \models T$. Definujme rekurzí posloupnosti $\mathbf{A}_i$ a $\mathbf{B}_i$ struktur jako na obrázku 3.4.4. $\mathbf{A}_0$ je struktura $\mathbf{A}$. Nechť již jsou sestrojeny struktury $\mathbf{A}_0 \subseteq \mathbf{B}_0 \subseteq \mathbf{A}_1 \subseteq .. \subseteq \mathbf{B}_{i-1} \subseteq \mathbf{A}_i$, všechny $\mathbf{B}_0, .., \mathbf{B}_{i-1}$ jsou modely teorie T, všechny $\mathbf{A}_0, .., \mathbf{A}_i$ jsou modely teorie T', a přitom pro každé $j < i$ platí

$\mathbf{A}_j \prec_1 \mathbf{B}_j$, $\mathbf{B}_j \prec_0 \mathbf{A}_{j+1}$ a $\mathbf{A}_j \prec \mathbf{A}_{j+1}$. Podle věty 3.4.21 můžeme zvolit 1-elementární rozšíření $\mathbf{B}_i$ struktury $\mathbf{A}_i$ takové, že $\mathbf{B}_i \models T$. A podle lemmatu 3.4.23 lze zvolit strukturu $\mathbf{A}_{i+1}$ takovou, že $\mathbf{B}_i \prec_0 \mathbf{A}_{i+1}$ a $\mathbf{A}_i \prec \mathbf{A}_{i+1}$. Dle lemmatu 3.4.17(e) jsou struktury $\mathbf{A}_i$ a $\mathbf{A}_{i+1}$ elementárně ekvivalentní. Tedy $\mathbf{A}_{i+1} \models T'$. Označme nyní $\mathbf{D}$ limitu řetězu $\mathbf{A}_0$, $\mathbf{B}_0$, $\mathbf{A}_1$, $\mathbf{B}_1$ atd. Struktura $\mathbf{D}$ je současně také limitou obou řetězů $\{\, \mathbf{A}_i \,;\, i \in \mathrm{N} \,\}$ a $\{\, \mathbf{B}_i \,;\, i \in \mathrm{N} \,\}$. Podle předpokladu platí $\mathbf{D} \models T$. Podle lemmatu 3.4.24 je struktura $\mathbf{D}$ elementárním rozšířením všech struktur $\mathbf{A}_i$. Tedy, opět dle 3.4.17(e), platí $\mathbf{A}_0 \models T$. QED



Obrázek 3.4.4: Metoda alternujících řetězů

Konstrukce uvedená v důkazu předchozí věty, založená na faktu, že limita řetězu je zároveň také limitou kteréhokoliv nekonečného podřetězu, je ukázkou užití metody, které se říká *metoda alternujících řetězů*.

Příklad 3.4.26 Uvažujme strukturu celých čísel $\langle \mathrm{Z}, < \rangle$ a její podstruktury $\mathbf{A}_i$, kde A_i je vpravo neomezený interval $[\![-i, +\infty)$. Struktura $\langle \mathrm{Z}, < \rangle$ celých čísel s uspořádáním je limitou řetězu struktur $\mathbf{A}_i$. To znamená, že vlastnost uspořádané množiny, že v ní existuje nejmenší prvek, nelze vyjádřit pomocí U_2-sentencí.

V tomto oddílu jsme naznačili některé z úvah běžných v *teorii modelů*. O většině důležitých metod a konstrukcí jsme se ale nezmínili. Jedna z metod, které jsme pominuli, je například ultraprodukt, pomocí něhož lze jednoduše formulovat nutnou a postačující podmínku pro to, aby nějaká třída struktur byla axiomatizovatelná. Zájemce o další informace odkazujeme na zdroje, ze kterých jsme čerpali: úvodní kapitoly knihy [40] a příručky [4], případně kapitolu [70] příručky [4] a knihu [51]. Cvičení 29–32 jsou založena na Ehrenfeuchtově metodě, která je podrobněji vyložena a rozpracována v knize [21].

Cvičení

1. Řekneme, že třída $\mathcal{E}$ struktur pro jazyk L je *konečně axiomatizovatelná*, jestliže existuje konečná množina T sentencí v L taková, že $\mathcal{E}$ je třída všech modelů teorie T. Dokažte, že komplement libovolné konečně axiomatizovatelné třídy je opět konečně axiomatizovatelná třída.

2. Dokažte, že třída všech nekonečných struktur (pro libovolný jazyk L) je axiomatizovatelná, není ale konečně axiomatizovatelná.

3. Teorie AG, *teorie abelovských grup*, má jazyk $\{+, 0\}$ s binární operací a s konstantou a axiomy R1–R4 teorie komutativních těles. Modely teorie AG jsou *abelovské grupy* neboli komutativní grupy. Domluvme se, že místo výrazu $a + a + \ldots + a$ s n sčítanci píšeme na. Řekneme, že abelovská grupa $\langle G, +, 0\rangle$ je *cyklická*, jestliže existuje prvek $a \in G$ a přirozené číslo $n \geq 1$ takové, že $G = \{0a, 1a, 2a, \ldots, (n-1)a\}$. Platí ovšem $0a = 0$ a $1a = a$. Řekneme, že abelovská grupa $\langle G, +, 0\rangle$ je *torzní*, jestliže pro každé $a \in G$ existuje přirozené číslo $n \geq 1$ takové, že $na = 0$. Dokažte, že každá cyklická grupa je torzní. Nalezněte příklad torzní grupy, která není cyklická.

4. Dokažte, že třída všech cyklických grup ani třída všech torzních grup není axiomatizovatelná.

   Návod. Přidejte k jazyku $\{+, 0\}$ teorie grup dočasně novou konstantu c. Zvolte za S množinu všech sentencí tvaru $nc \neq 0$ pro $n \geq 1$, zvolte za T množinu všech sentencí v jazyce $\{+, 0\}$, které platí ve všech cyklických grupách. Zdůvodněte, že teorie $T \cup S$ má model.

5. Když $\mathcal{E}$ je třída struktur pro jazyk L, která je axiomatizovatelná, a když navíc komplement třídy $\mathcal{E}$ (tj. třída všech struktur pro L, které nejsou v $\mathcal{E}$) je axiomatizovatelná třída, pak $\mathcal{E}$ i její komplement jsou konečně axiomatizovatelné.

   Návod. Nechť teorie T axiomatizuje $\mathcal{E}$ a nechť S axiomatizuje komplement třídy $\mathcal{E}$. Pak $T \cup S$ nemá žádný model. Dle věty o kompaktnosti existují množiny $F_1 \subseteq T$ a $F_2 \subseteq S$ konečné takové, že $F_1 \cup F_2$ nemá žádný model. Zdůvodněte, že F_1 a F_2 jsou hledané teorie.

6. Teorie T je *konečně axiomatizovatelná*, jestliže třída všech jejích modelů je konečně axiomatizovatelná, neboli jestliže T je ekvivalentní s nějakou konečnou množinou sentencí (svého jazyka). Dokažte sémantickými prostředky (tj. užitím věty o kompaktnosti), že je-li T konečně axiomatizovatelná, pak T je ekvivalentní s jistou konečnou množinou F sentencí takovou, že $F \subseteq T$.

7. Abelovská grupa $\langle G, +, 0\rangle$ je *grupa s dělením*, jestliže pro každé $a \in G$ a pro každé přirozené číslo $n \geq 1$ existuje prvek $b \in G$ takový, že $nb = a$. Dokažte, že třída všech abelovských grup s dělením je axiomatizovatelná, ale není konečně axiomatizovatelná.

8. Dokažte, že teorie SUCC definovaná v závěru oddílu 3.2 není konečně axiomatizovatelná.

9. Neorientovaný graf je *souvislý*, jestliže každý jeho vrchol je z každého dosažitelný, tj. jestliže z každého jeho vrcholu c vede (neorientovaná) cesta do každého jeho vrcholu d. Dokažte, že souvislost neorientovaného grafu není vlastností prvního řádu.

   Návod. Místo podmínky, že z a vede nejvýše jedna hrana, uvažujte tuto podmínku: každý vrchol má nejvýše dva sousedy a přitom existují nejméně dva vrcholy, z nichž každý má nejvýše jednoho souseda.

10. Dokažte, že je-li $\langle D, <\rangle$ lineárně uspořádaná množina, v níž každý prvek má jen konečně mnoho předchůdců, pak D je nejvýše spočetná.

11. Nechť $\langle D, <\rangle$ je (ne nutně lineárně) uspořádaná množina. Pišme $a \leq b$ místo $a < b \vee a = b$. Nechť $A \subseteq D$. Řekneme, že $d \in D$ je *supremum* množiny A, jestliže d splňuje podmínky $\forall a \in A(a \leq d)$ a $\forall d'(\forall a \in A(a \leq d') \Rightarrow d \leq d')$. Dokažte, že každá $A \subseteq D$ má nejvýše jedno supremum. Nemá-li $\langle D, <\rangle$ největší prvek, pak existují množiny $A \subseteq D$, například sama D, které nemají supremum. Ukažte na příkladech, že supremum množiny A může, ale nemusí být v A a že A nemusí mít supremum, přestože $\langle D, <\rangle$ má největší prvek, a to vše i v případě, kdy $\langle D, <\rangle$ je lineárně uspořádaná.

12. Nechť $\langle D, <\rangle$ je uspořádaná množina a nechť $A \subseteq D$. Řekneme, že $d \in D$ je *horní závora* množiny A, jestliže $\forall a \in A(a \leq d)$. Řekneme, že v $\langle D, <\rangle$ platí *věta o supremu*, jestliže každá neprázdná $A \subseteq D$, která má nějakou horní závoru, má i supremum. Supremum bylo tedy v předchozím cvičení definováno jako nejmenší horní závora. Definujte analogicky *infimum* množiny jako největší dolní závoru a formulujte *větu o infimu*. Dokažte, že v $\langle D, <\rangle$ platí věta o supremu, právě když tam platí věta o infimu.

13. Nechť $\langle D, <\rangle$ je lineárně uspořádaná množina. Řekneme, že množina $A \subseteq D$ je *hustá* v $\langle D, <\rangle$, jestliže každý otevřený interval (včetně „nevlastních“ intervalů, tj. včetně množin tvaru $\{x; x < a\}$ a $\{x; x > a\}$) má neprázdný průnik s množinou A. Když A je hustá v $\langle D, <\rangle$, pak $\langle D, <\rangle$ i $\langle A, <\rangle$ jsou modely teorie DNO. Dokažte, že když $\langle D_1, <_1\rangle$ a $\langle D_2, <_2\rangle$ jsou lineárně uspořádané množiny, ve kterých platí věta o supremu, a existuje množina A_1 hustá v $\langle D_1, <_1\rangle$ a A_2 hustá v $\langle D_2, <_2\rangle$ takové, že $\langle A_1, <_1\rangle$ a $\langle A_2, <_2\rangle$ jsou spolu izomorfní, pak i celé struktury $\langle D_1, <_1\rangle$ a $\langle D_2, <_2\rangle$ jsou spolu izomorfní.

14. Nechť $\langle A, <_A\rangle$ je model teorie DNO. Pak existuje lineárně uspořádaná množina $\langle D, <_D\rangle$, ve které platí věta o supremu, a taková, že $\langle A, <_A\rangle$ je izomorfní s jistou podmnožinou množiny D, která je hustá v $\langle D, <_D\rangle$. Dokažte.

    Návod. Definujte *řez* v $\langle A, <_A\rangle$ jako množinu $X \subseteq A$ různou od $\emptyset$ a A, která nemá maximum a která splňuje podmínku $\forall a \forall b(a < b \ \& \ b \in X \Rightarrow a \in X)$. Definujte D jako množinu všech řezů v $\langle A, <_A\rangle$. Definujte $<_D$ jako inkluzi.

15. Teorie DNO má jediný (až na izomorfismus) model, ve kterém platí věta o supremu a který obsahuje spočetnou hustou podmnožinu. Dokažte. Jaká je jeho mohutnost?

    Návod. Použijte cvičení 13, příklad 3.4.12 a vědomost, že ve struktuře $\langle \mathrm{R}, <\rangle$ reálných čísel s uspořádáním platí věta o supremu.

16. Uvažujte teorii T, která má spočetný jazyk $L = \{c_0, c_1, c_2, \dots\}$ obsahující pouze konstanty a jejíž axiomy jsou všechny sentence tvaru $c_i \neq c_j$ pro $i \neq j$. Rozhodněte, pro která κ platí, že T je κ-kategorická.

17. Uvažujte třídu všech struktur $\langle D, P\rangle$ pro jazyk s jedním unárním predikátem takových, že P i $D - P$ jsou nekonečné množiny. Dokažte, že tato třída je axiomatizovatelná. Je konečně axiomatizovatelná? Rozhodněte, pro která κ je příslušná teorie κ-kategorická.

18. Každá spočetná lineárně uspořádaná množina je izomorfní s jistou podmnožinou množiny Q všech racionálních čísel (s obvyklým uspořádáním). Dokažte.

19. Když pro vnoření $f : \mathbf{A} \to_0 \mathbf{B}$ a $g : \mathbf{B} \to_\mathrm{e} \mathbf{C}$ platí, že $g \circ f$ je elementární, pak $f : \mathbf{A} \to_\mathrm{e} \mathbf{B}$. Dokažte.

20. Dokažte, že tvrzení lemmatu 3.4.23 lze obrátit: když $f : \mathbf{A} \to_0 \mathbf{B}$, $g : \mathbf{B} \to_0 \mathbf{C}$ a $g \circ f$ je elementární vnoření struktury $\mathbf{A}$ do struktury $\mathbf{C}$, pak $f : \mathbf{A} \to_1 \mathbf{B}$.

21. Rozhodněte, zda platí: když $\mathbf{A} \prec_0 \mathbf{B}$ a $\mathbf{A}$ a $\mathbf{B}$ jsou izomorfní, pak $\mathbf{A} \prec \mathbf{B}$.

    Návod. Uvažujte třeba struktury $\langle \mathrm{N}, <\rangle$ a $\langle \mathrm{N} - \{0\}, <\rangle$.

22. Jsou-li $\mathbf{A}$ a $\mathbf{B}$ elementárně ekvivalentní struktury pro týž jazyk L, pak existuje struktura $\mathbf{C}$ pro jazyk L a elementární vnoření $g_1 : \mathbf{A} \to_\mathrm{e} \mathbf{C}$ a $g_2 : \mathbf{B} \to_\mathrm{e} \mathbf{C}$. Dokažte.

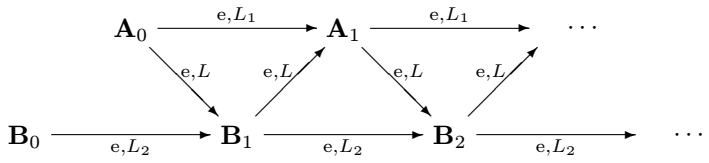
    Návod. Nemá-li $\mathrm{Diag}_\mathrm{e}(\mathbf{A}) \cup \mathrm{Diag}_\mathrm{e}(\mathbf{B})$ model, existuje logicky platná formule tvaru $\bigwedge \alpha_i(\widehat{\underline{a}}) \to \neg \bigwedge \beta_j(\widehat{\underline{b}})$, kde $\alpha_i(\widehat{\underline{a}}) \in \mathrm{Diag}_\mathrm{e}(\mathbf{A})$ a $\beta_j(\widehat{\underline{b}}) \in \mathrm{Diag}_\mathrm{e}(\mathbf{B})$. Pak také sentence $\exists \underline{x} \bigwedge \alpha_i(\underline{x}) \to \neg \exists \underline{y} \bigwedge \beta_j(\underline{y})$ je logicky platná atd.

23. Dokažte tuto modifikaci věty 3.4.21: nechť T je teorie v jazyce L', nechť $L \subseteq L'$ a nechť $\mathbf{A}$ je struktura pro jazyk L, ve které platí všechny L-sentence dokazatelné v T. Pak existuje model $\mathbf{B}$ teorie T a funkce g z $\mathbf{A}$ do $\mathbf{B}$ taková, že $g : \mathbf{A} \to_{\mathrm{e},L} \mathbf{B}$, tj. taková, která je vnořením struktury $\mathbf{A}$ do reduktu struktury $\mathbf{B}$ pro jazyk L.

24. Dokažte následující modifikaci lemmatu 3.4.23: je-li $L \subseteq L'$, je-li $\mathbf{A}$ struktura pro L', je-li $\mathbf{B}$ struktura pro L a platí-li $f : \mathbf{A} \to_{\mathrm{e},L} \mathbf{B}$, pak existuje struktura $\mathbf{C}$ pro jazyk L' a vnoření $g : \mathbf{B} \to_{\mathrm{e},L} \mathbf{C}$ takové, že $g \circ f : \mathbf{A} \to_{\mathrm{e},L'} \mathbf{C}$.

25. Dokažte *Robinsonovu větu* o bezespornosti: nechť L_1 a L_2 jsou jazyky, nechť T je úplná teorie v $L = L_1 \cap L_2$, nechť T_1 a T_2 jsou bezesporné teorie v L_1 resp. L_2 takové, že $\mathrm{Thm}(T) \subseteq \mathrm{Thm}(T_1)$ a $\mathrm{Thm}(T) \subseteq \mathrm{Thm}(T_2)$. Pak $T_1 \cup T_2$ je bezesporná teorie.

    Návod. Vezměte model $\mathbf{A}_0$ teorie T_1 a model $\mathbf{B}_0$ teorie T_2 a zdůvodněte existenci takovýchto struktur a vnoření:



Strukturu $\mathbf{A}_i$ pro $i \geq 1$, vnoření struktury $\mathbf{B}_i$ do $\mathbf{A}_i$ zachovávající všechny L-formule a vnoření struktury $\mathbf{A}_{i-1}$ do $\mathbf{A}_i$ zachovávající všechny L_1-formule lze získat volbou $L' := L_1$ v tvrzení z předchozího cvičení. Strukturu $\mathbf{B}_i$ pro $i \geq 2$ a příslušná vnoření lze naopak získat volbou $L' := L_2$. Existenci struktury $\mathbf{B}_1$ zdůvodněte zvlášť. Limitu $\mathbf{C}$ elementárního řetězu $\mathbf{A}_0, \mathbf{B}_1, \mathbf{A}_1, \ldots$ struktur pro jazyk L lze expandovat do struktury pro jazyk L_1, která je limitou řetězu $\{\ \mathbf{A}_i\ ;\ i \in \mathrm{N}\ \}$, a také do struktury pro jazyk L_2, která je limitou řetězu $\{\ \mathbf{B}_i\ ;\ i \in \mathrm{N}\ \}$. Provedeme-li obě expanze najednou, získáme model teorie $T_1 \cup T_2$.

26. Nechť T_1 je teorie v jazyce L_1 a T_2 je teorie v jazyce L_2. Je-li teorie $T_1 \cup T_2$ sporná, pak existuje sentence θ v jazyce $L_1 \cap L_2$ taková, že $T_1 \vdash \theta$ a $T_2 \vdash \neg\theta$. Dokažte toto tvrzení převedením na Robinsonovu větu.

    Návod. Nechť taková sentence neexistuje. Označte T_0 množinu všech L-sentencí dokazatelných v teorii T_1 a zdůvodněte, že $T_0 \cup T_2$ má model. Vezměte libovolný model $\mathbf{M}$ teorie $T_0 \cup T_2$, vezměte jeho redukt $\mathbf{M}_0$ pro jazyk L a aplikujte Robinsonovu větu na úplnou teorii $T := \mathrm{Th}(\mathbf{M}_0)$ a na teorie $\mathrm{Th}(\mathbf{M}_0) \cup T_1$ a $\mathrm{Th}(\mathbf{M}_0) \cup T_2$.

27. Vyvoďte z předchozího cvičení *Craigovu větu* o interpolaci: je-li φ sentence v L_1 a ψ sentence v L_2 a je-li implikace $\varphi \to \psi$ logicky platná, pak existuje sentence θ v jazyce $L_1 \cap L_2$ taková, že obě implikace $\varphi \to \theta$ a $\theta \to \psi$ jsou logicky platné.

28. Vyvoďte Robinsonovu větu o bezespornosti z Craigovy věty o interpolaci. Nalezněte příklady na to, že předpoklady v Robinsonově větě, že teorie T je úplná a že její jazyk je průnikem jazyků teorií T_1 a T_2, jsou podstatné.

29. Nechť relace R_n jsou na množině $\mathrm{N} \cup \{\infty\}$ (přirozených čísel s jedním dodatečným prvkem) definovány předpisem $a\ R_n\ b \Leftrightarrow a = b \vee (2^n \leq a\ \&\ 2^n \leq b)$, přičemž ∞ se považuje za větší než všechna čísla $m \in \mathrm{N}$. Zdůvodněte, že všechny relace R_n jsou ekvivalence. Nechť $\infty - m$ je pro $m \in \mathrm{N}$ definováno jako ∞. Dokažte, že když $a\ R_{n+1}\ b$, pak pro každé $c \leq a$ existuje $d \leq b$ takové, že $c\ R_n\ d$ a $(a - c)\ R_n\ (b - d)$.

30. Nechť $\mathbf{D} = \langle D, < \rangle$ je libovolný model teorie DO. Definujme *vzdálenost* $|a - b|$ libovolných prvků a, b jako počet prvků $d \in D$ splňujících v $\mathbf{D}$ podmínku $a \leq d < b$. Vzdálenost $|a - b|$ je prvek množiny $\mathrm{N} \cup \{\infty\}$ z předchozího cvičení. Vzdálenost dvou sousedních prvků je 1 a vzdálenost libovolného prvku od sebe samého je 0. Definujme systém relací $E_{n,k}$ na množině D^k. Mějme dvě k-tice $a_1, \ldots, a_k$ a $b_1, \ldots, b_k$ prvků z D. Zvolme permutaci π indexů $\{1, \ldots, k\}$, která uspořádá k-tici $a_1, \ldots, a_k$, tj. pro kterou (v $\mathbf{D}$) platí $a_{\pi(1)} \leq \ldots \leq a_{\pi(k)}$. Pak $[\underline{a}]\ E_{n,k}\ [\underline{b}]$, jsou-li splněny podmínky

    - $\forall i (1 \leq i < k \Rightarrow b_{\pi(i)} \leq b_{\pi(i+1)}\ \&\ (b_{\pi(i)} = b_{\pi(i+1)} \Leftrightarrow a_{\pi(i)} = a_{\pi(i+1)}))$,
    - $|0 - a_{\pi(1)}|\ R_n\ |0 - b_{\pi(1)}|$,

- $\forall i(1 \leq i < k \Rightarrow |a_{\pi(i)} - a_{\pi(i+1)}| \; R_n \; |b_{\pi(i)} - b_{\pi(i+1)}|)$.

Dokažte, že když $[\underline{a}] \; E_{n+1,k} \; [\underline{b}]$, pak pro každé $c \in D$ existuje $d \in D$ takové, že $[\underline{a}, c] \; E_{n,k} \; [\underline{b}, d]$.

31. Nechť $\varphi(x_1, \ldots, x_k)$ je prenexní formule v jazyce $\{<\}$ obsahující nejvýše n kvantifikátorů, nechť $a_1, \ldots, a_k$ a $b_1, \ldots, b_k$ jsou dvě k-tice prvků z $\mathbf{D}$ takové, že $[\underline{a}] \; E_{n,k} \; [\underline{b}]$. Pak $\mathbf{D} \models \varphi[\underline{a}] \Leftrightarrow \mathbf{D} \models \varphi[\underline{b}]$. Dokažte.

32. Dokažte na základě předchozího cvičení, že počáteční úsek modelu $\mathbf{D}$ izomorfní se strukturou ω, tj. podstruktura sestávající ze všech prvků, jejichž vzdálenost od nuly je konečná, je elementární podstrukturou struktury $\mathbf{D}$. Vyvoďte z toho (a z 3.4.17(e)), že DO je úplná teorie.

3.5 Eliminace kvantifikátorů

Je-li zvolena teorie T s jazykem L, můžeme se ptát, zda každá formule jazyka L je v T ekvivalentní s nějakou formulí neobsahující kvantifikátory. Snadno lze zdůvodnit (například na základě cvičení 1), že alespoň pro některé teorie odpověď zní ne, kvantifikátory obecně nelze pominout. V tomto oddílu uvidíme, že pro některé teorie naopak platí ano. Platí-li o teorii T, že každá formule φ je v T ekvivalentní s otevřenou formulí ψ, jejíž všechny volné proměnné jsou zároveň volné ve φ, říkáme, že T *připouští eliminaci kvantifikátorů*.

Je-li každá formule φ v T ekvivalentní s formulí ψ, která oproti φ nemá žádné volné proměnné navíc, znamená to, že každá sentence φ je v T ekvivalentní s otevřenou sentencí ψ. Máme-li pak dokázat, že teorie T je úplná, stačí ověřit, že podmínka $T \vdash \varphi$ nebo $T \vdash \neg\varphi$ platí pro každou *otevřenou sentenci*. Eliminace kvantifikátorů nám tedy kromě metod, které jsme poznali dosud (jedna byla založena na větě 3.4.15 a druhá byla naznačena ve cvičeních 29–32 oddílu 3.4), poskytuje další, poměrně široce aplikovatelnou metodu pro důkaz úplnosti axiomatické teorie.

Pomocí eliminace kvantifikátorů dokážeme úplnost teorie DO z oddílu 3.4 a dále úplnost teorie celočíselného sčítání a teorie reálně uzavřených těles.

Neplatí-li, že každá formule teorie T je v T ekvivalentní s otevřenou formulí, může to platit pro jisté rozšíření T' teorie T formulované v jazyce $L' \supseteq L$. Pokud navíc T' rozšiřuje T „nepodstatně“, z úplnosti teorie T' lze usoudit na úplnost teorie T. Nalezení vhodného nepodstatného (budeme říkat konzervativního) rozšíření T' teorie T tedy bude důležitou a někdy jedinou netriviální částí důkazu, že T je úplná.

Definice 3.5.1 *Nechť T_1 a T_2 jsou teorie s jazyky L_1 resp. L_2. Řekneme, že teorie T_1 je* podteorie *teorie T_2 a že teorie T_2 je* rozšíření *teorie T_1, jestliže $L_1 \subseteq L_2$ a $\mathrm{Thm}(T_1) \subseteq \mathrm{Thm}(T_2)$. Řekneme, že teorie T_2 je* konzervativní rozšíření *teorie T_1, jestliže T_2 je rozšíření teorie T_1 a navíc každá sentence jazyka L_1 dokazatelná v T_2 je dokazatelná i v T_1.*

Připomeňme, že jsou-li $\mathbf{D}_1$ a $\mathbf{D}_2$ struktury pro jazyky L_1 a L_2, kde $L_1 \subseteq L_2$, pak $\mathbf{D}_2$ je expanze struktury $\mathbf{D}_1$, jestliže $\mathbf{D}_1$ a $\mathbf{D}_2$ mají tutéž nosnou množinu D a jestliže navíc každý symbol z L_1 má v $\mathbf{D}_1$ i v $\mathbf{D}_2$ tutéž realizaci.

Věta 3.5.2 *Když T_2 je rozšíření teorie T_1 a každý model teorie T_1 má expanzi, která je modelem teorie T_2, pak T_2 je konzervativním rozšířením teorie T_1.*

Důkaz Nechť φ je sentence jazyka L_1 taková, že $T_2 \vdash \varphi$. Chceme ověřit, že $T_1 \vdash \varphi$. Stačí zdůvodnit, že φ platí ve všech modelech teorie T_1. Nechť tedy $\mathbf{D}_1 \models T_1$. Dle podmínky věty existuje expanze $\mathbf{D}_2$ modelu $\mathbf{D}_1$ taková, že $\mathbf{D}_2 \models T_2$. Protože $T_2 \vdash \varphi$, máme $\mathbf{D}_2 \models \varphi$. Platnost formule φ závisí jen na realizaci symbolů z L_1 (viz cvičení 18 z oddílu 3.1), které ale jsou v $\mathbf{D}_1$ i v $\mathbf{D}_2$ realizovány shodně. Tedy $\mathbf{D}_1 \models \varphi$. QED

Důležitý zvláštní případ konzervativního rozšíření teorie popisuje následující věta. V jejím znění je užit definovaný kvantifikátor $\exists!$, který budeme používat i ve zbývajícím textu. Zápis $\exists! y \varphi(\underline{x}, y)$ znamená $\exists y(\varphi(\underline{x}, y) \ \& \ \forall v(\varphi(\underline{x}, v) \rightarrow v = y))$ a čteme jej „existuje právě jedno y takové, že $\varphi(\underline{x}, y)$“.

Věta 3.5.3 *(a) Nechť T je teorie s jazykem L, nechť $P \notin L$ je n-ární predikátový symbol, nechť $\varepsilon(x_1, \ldots, x_n)$ je formule v jazyce L, jejíž všechny volné proměnné jsou mezi $x_1, \ldots, x_n$. Nechť dále T' je teorie, která má jazyk $L \cup \{P\}$ a která má tytéž axiomy jako teorie T a navíc axiom*

$$\forall x_1 \ldots \forall x_n (P(x_1, \ldots, x_n) \equiv \varepsilon(x_1, \ldots, x_n)). \tag{d1}$$

Pak T' je konzervativním rozšířením teorie T.
(b) Nechť T je teorie s jazykem L, nechť $F \notin L$ je n-ární funkční symbol, nechť $\eta(x_1, \ldots, x_n, y)$ je formule v L, jejíž všechny volné proměnné jsou mezi $x_1, \ldots, x_n, y$, a nechť $T \vdash \forall \underline{x} \exists! y \eta(\underline{x}, y)$. Nechť dále T' je teorie, která má jazyk $L \cup \{F\}$ a která má tytéž axiomy jako teorie T a navíc axiom

$$\forall x_1 \ldots \forall x_n \forall y (F(x_1, \ldots, x_n) = y \equiv \eta(x_1, \ldots, x_n, y)). \tag{d2}$$

Pak T' je konzervativním rozšířením teorie T.

Důkaz Ověříme podmínku z věty 3.5.2. Nechť $\mathbf{M}$ je libovolný model teorie T. Realizujeme-li symbol P množinou $\{ [a_1, \ldots, a_n] \in M^n \ ; \ \mathbf{M} \models \varepsilon[\underline{a}] \}$, dostaneme (jedinou) expanzi $\mathbf{M}'$ struktury $\mathbf{M}$ pro jazyk $L \cup \{P\}$, která splňuje axiom (d1). Tím je ověřena podmínka z věty 3.5.2, a tedy dokázáno tvrzení (a). Důkaz tvrzení (b) je obdobný, symbol F realizujeme množinou $\{ [\underline{a}, b] \in M^{n+1} \ ; \ \mathbf{M} \models \eta[\underline{a}, b] \}$. Navíc je třeba dodat, že tato množina je vzhledem k podmínce $T \vdash \forall \underline{x} \exists! y \eta(\underline{x}, y)$ funkcí z M^n do M, a tedy může být zvolena za realizaci n-árního funkčního symbolu. QED

Řekneme, že teorie S je *rozšířením* teorie T *o definice*, jestliže existuje (konečná nebo nekonečná spočetná) posloupnost teorií $T_0, T_1, \ldots$ taková, že T_0 je T, každá T_{i+1} je rozšířením teorie T_i o definici jednoho symbolu tak, jak je popsáno ve větě 3.5.3 (a) nebo (b), a dále jazyk teorie S je sjednocením jazyků všech T_i a množina axiomů teorie S je sjednocením množin axiomů všech T_i. Je-li posloupnost $\{T_i\}$ konečná, pak S je totožná s jejím posledním členem. Každá teorie je považována za své vlastní rozšíření o definice.

Je-li teorie T' konzervativním rozšířením teorie T, znamená to, že v ní nelze navíc oproti teorii T dokázat žádné z těch tvrzení, která lze formulovat v jazyce teorie T. Je-li T' rozšířením teorie T o definice, znamená to, že v ní dokonce nelze formulovat žádná nová tvrzení, tj. tvrzení, která by nešlo formulovat už v jazyce teorie T.

Nyní jsme připraveni dokázat úplnost teorie DO pomocí eliminace kvantifikátorů. Postup, který ukážeme, je až na drobnosti převzat z Rabinovy kapitoly [70] příručky [4].

Protože teorie DO eliminaci kvantifikátorů nepřipouští (viz cvičení 1), abychom mohli dokázat její úplnost pomocí eliminace kvantifikátorů, musíme nejprve nalézt její vhodné konzervativní rozšíření. Připomeňme, že axiomy teorie DO jsou sentence LO1–LO3 uvedené na str. 172 a dále sentence DO1–DO3 uvedené na str. 212. Označme DOS teorii, jejíž jazyk je $\{0, \mathrm{S}, <\}$ a jejíž axiomy jsou axiomy teorie DO a navíc axiomy

$$\forall x(x = 0 \equiv \neg\exists y(y < x)),$$

$$\forall x \forall y(y = \mathrm{S}(x) \equiv x < y \ \&\ \neg\exists v(x < v \ \&\ v < y)).$$

Těmto dvěma axiomům říkejme definice nuly a definice následnické funkce. Axiom DO1 teorie DO postuluje, že existuje objekt, před kterým není žádný menší, a užitím axiomu LO3 lze snadno usoudit, že takový objekt je jen jeden. Definice nuly tedy splňuje podmínku jednoznačnosti z věty 3.5.3(b). Podobně lze zdůvodnit, že také definice následnické funkce ji splňuje. Podle věty 3.5.3 je tedy teorie DOS konzervativním rozšířením teorie DO. Je zřejmé, že struktura $\langle \mathrm{N}, 0, \mathrm{S}, < \rangle$ je jedním z modelů teorie DOS.

V teorii DOS můžeme užívat všechna tvrzení, která jsme dokázali v teorii DO nebo v teorii LO. Bude se nám například hodit schéma, které pro každé $n \geq 1$ tvrdí, že každá n-tice objektů má maximální prvek. Dále budeme kromě symbolů $<$, 0 a S užívat také symbol $\leq$ pro neostré uspořádání. Přitom je jedno, zda jej považujeme za zkratku a za každou formulí $t \leq s$ si představujeme formuli $t < s \vee t = s$ (tak jsme se na symbol $\leq$ dívali v oddílu 3.2), nebo zda jej považujeme za čtvrtý symbol jazyka teorie DOS definovaný formulí $\forall x \forall y(x \leq y \equiv x < y \vee x = y)$ (na základě věty 3.5.3).

Úvahy směřující k eliminaci kvantifikátorů pro teorii DOS budou zjednodušeny faktem, že lze snadno charakterizovat všechny termy teorie DOS. Každý term sestavený z proměnných a symbolů 0 a S má totiž tvar $\mathrm{S}^{(m)}(z)$, kde z je nějaká proměnná, nebo tvar $\mathrm{S}^{(m)}(0)$. Žádný term tedy nemůže obsahovat více než jednu

proměnnou. Připomeňme ještě, že místo $\mathrm{S}^{(m)}(0)$ píšeme $\overline{m}$ a že termům tvaru $\overline{m}$ říkáme numerály.

Lemma 3.5.4 *V teorii* DOS *lze dokázat následující sentence:*

(a) $\forall x(x < \mathrm{S}(x))$,
(b) $\forall x \forall y(x < \mathrm{S}(y) \equiv x < y \vee x = y)$,
(c) $\forall x \forall y(\mathrm{S}(x) < \mathrm{S}(y) \equiv x < y)$,
(d) $\forall x \forall y(\mathrm{S}(x) = \mathrm{S}(y) \equiv x = y)$,
(e) $\forall x(\mathrm{S}^{(m)}(x) < \mathrm{S}^{(n)}(x))$, *je-li* $m < n$,
(f) $\forall x(\mathrm{S}^{(m)}(x) \neq \mathrm{S}^{(n)}(x))$, *je-li* $m \neq n$,
(g) $\forall x(\overline{m} \leq x \equiv \exists v(x = \mathrm{S}^{(m)}(v)))$.

Důkaz Implikace $\rightarrow$ v (b) se dokáže takto:

> Neplatí-li $x < y$ ani $x = y$, dle axiomu LO3 platí $y < x$. V tom případě x je některý z objektů větších než y. Protože $\mathrm{S}(y)$ je definován jako nejmenší z objektů větších než y, platí $\mathrm{S}(y) \leq x$. To je spor s předpokladem $x < \mathrm{S}(y)$.

Implikace $\rightarrow$ v (c) se snadno dokáže dosazením termu $\mathrm{S}(x)$ za x v (b). Zbývající kroky v důkazech sentencí (a)–(c) ponecháváme na čtenáři. Sentenci (d) lze dokázat z (c) užitím axiomu LO3. V (e) si stačí uvědomit, že $\mathrm{S}^{(m)}(x)$ a $\mathrm{S}^{(n-m)}(\mathrm{S}^{(m)}(x))$ jsou tytéž termy, a $(n-m)$-krát užít (a). Sentence (f) plyne z (e) a v důkazu se uplatní axiom LO2. Existence důkazu implikace $\rightarrow$ sentence (g) se dokáže indukcí podle m. Ukažme si indukční krok. Je-li důkaz pro m již sestrojen, důkaz pro $m+1$ může vypadat takto:

> Nechť x je dáno a nechť $\overline{m+1} \leq x$. Tedy $\mathrm{S}(\overline{m}) \leq x$. Podle již dokázané sentence (a) to znamená $\overline{m} < x$. Podle axiomu DO3 existuje z takové, že $z < x$ a mezi z a x není nic. Podle definice následnické funkce to znamená, že $x = \mathrm{S}(z)$. Dále určitě platí $\overline{m} \leq z$, jinak by objekt $\overline{m}$ byl mezi z a x. Dle již dokázaného tvrzení pro $\overline{m}$ k objektu z existuje v takové, že $z = \mathrm{S}^{(m)}(v)$. Platí tedy $x = \mathrm{S}^{(m+1)}(v)$.

Důkaz pro $m = 0$ a důkaz implikace $\leftarrow$ opět ponecháváme na čtenáři. QED

Nyní můžeme postupně dokázat, že teorie DOS připouští eliminaci kvantifikátorů, tj. že každá formule jejího jazyka je ekvivalentní s otevřenou formulí. K pojmu „ekvivalentní formule“ pro jistotu zdůrazněme, že jsou-li formule $\varphi(\underline{x})$ a $\psi(\underline{x})$ ekvivalentní v teorii DOS, znamená to, že podmínky $\mathbf{M} \models \varphi[e]$ a $\mathbf{M} \models \psi[e]$ jsou ekvivalentní pro *každý model* teorie DOS (a ne například jen pro „preferovaný“ model $\langle \mathrm{N}, 0, \mathrm{S}, < \rangle$) a pro *každé ohodnocení* proměnných e. K prokazování ekvivalence samozřejmě užíváme neformální důkazy. Nejprve se budeme zabývat formulemi, jako je například $\exists x(y_1 < \mathrm{S}^{(7)}(x) \ \& \ \mathrm{S}^{(7)}(x) = y_2)$, které neobsahují jiné logické spojky než konjunkci, obsahují právě jeden kvantifikátor, který je existenční a je umístěn hned na začátku, a které navíc splňují podmínku, že ta proměnná, kterou určuje onen jediný kvantifikátor, se v každé atomické podformuli vyskytuje pouze v určitém kontextu a vždy nejvýše na jedné straně (rovnosti nebo nerovnosti).

Lemma 3.5.5 *Nechť m je přirozené číslo a nechť $A(x, y_1, .., y_q)$ je konjunkce (libovolného počtu) atomických formulí v jazyce teorie* DOS *taková, že každá atomická podformule formule A obsahující proměnnou x má jeden z tvarů $\mathrm{S}^{(m)}(x) < t$, nebo $\mathrm{S}^{(m)}(x) = t$, nebo $t < \mathrm{S}^{(m)}(x)$, kde t je term neobsahující x. Pak formule $\exists x A$ je v teorii* DOS *ekvivalentní s otevřenou formulí, jejíž všechny volné proměnné jsou mezi $y_1, .., y_q$.*

Důkaz Je-li mezi atomickými podformulemi formule A alespoň jedna rovnost, můžeme si jednu vybrat a psát formuli A ve tvaru $\mathrm{S}^{(m)}(x) = t(\underline{y}) \ \& \ B(\mathrm{S}^{(m)}(x), \underline{y})$. Víme ovšem, že term $t(\underline{y})$ může z proměnných $y_1, .., y_q$ obsahovat nejvýše jednu. Pro následující úvahu to ale nemá žádný význam. Tvrdíme, že formule $\exists x A$ je v teorii DOS ekvivalentní s otevřenou formulí $\overline{m} \leq t(\underline{y}) \ \& \ B(t(\underline{y}), \underline{y})$. Zde je důkaz jejich ekvivalence:

> Nechť x je takové, že $\mathrm{S}^{(m)}(x) = t(\underline{y})$ a $B(\mathrm{S}^{(m)}(x), \underline{y})$. Podle implikace $\leftarrow$ v 3.5.4(g) platí $\overline{m} \leq t(\underline{y})$. Z $\mathrm{S}^{(m)}(x) = t(\underline{y})$ a z $B(\mathrm{S}^{(m)}(x), \underline{y})$ ovšem plyne také $B(t(\underline{y}), \underline{y})$.
>
> Když naopak $\overline{m} \leq t(\underline{y})$, pak dle implikace $\rightarrow$ v 3.5.4(g) k $t(\underline{y})$ existuje x takové, že $\mathrm{S}^{(m)}(x) = t(\underline{y})$. Když navíc $B(t(\underline{y}), \underline{y})$, pak ovšem i $B(\mathrm{S}^{(m)}(x), \underline{y})$. Tedy existuje x takové, že $A(x, \underline{y})$.

Zbývá případ, kdy žádná atomická podformule formule $A(x, \underline{y})$ není rovnost, tj. kdy A má tvar

$$t_1(\underline{y}) < \mathrm{S}^{(m)}(x) \ \& \ .. \ \& \ t_n(\underline{y}) < \mathrm{S}^{(m)}(x) \ \& \\ \& \ \mathrm{S}^{(m)}(x) < u_1(\underline{y}) \ \& \ .. \ \& \ \mathrm{S}^{(m)}(x) < u_k(\underline{y}) \ \& \ D(\underline{y}),$$

kde termy $t_i(\underline{y})$ a $u_j(\underline{y})$ a formule $D(\underline{y})$ neobsahují x. Tvrdíme, že formule $\exists x A$ je v teorii DOS ekvivalentní s formulí

$$\bigwedge_{i,j}(\mathrm{S}(t_i(\underline{y})) < u_j(\underline{y})) \ \& \ \bigwedge_{j}(\overline{m} < u_j(\underline{y})) \ \& \ D(\underline{y}), \qquad (*)$$

neboť jejich ekvivalenci lze v teorii DOS dokázat takto:

> Nechť x je takové, že $A(x, \underline{y})$. Z $t_i(\underline{y}) < \mathrm{S}^{(m)}(x)$ a $\mathrm{S}^{(m)}(x) < u_j(\underline{y})$ jistě plyne $\mathrm{S}(t_i(\underline{y})) < u_j(\underline{y})$. Dále z $\mathrm{S}^{(m)}(x) < u_j(\underline{y})$ jistě plyne $\overline{m} < u_j(\underline{y})$ dle $\leftarrow$ v 3.5.4(g). Tedy $(*)$.
>
> Nechť naopak $(*)$. Vezměme za z maximální z $n+1$ objektů $\overline{m}$ a $\mathrm{S}(t_1(\underline{y}))$ až $\mathrm{S}(t_n(\underline{y}))$. Tento objekt z splňuje všechny podmínky $t_i(\underline{y}) < z$ i $z < u_j(\underline{y})$. Dle implikace $\rightarrow$ v 3.5.4(g) k z existuje x splňující podmínku $\mathrm{S}^{(m)}(x) = z$. Pro x platí $A(x, \underline{y})$. Tedy $\exists x A(x, \underline{y})$.

Platí-li $k = 0$, formule $\exists x A(x, \underline{y})$ je ekvivalentní s formulí D, neboť v teorii DOS lze dokázat sentenci $\forall \underline{y} \exists x \bigwedge_i (t_i(\underline{y}) < \mathrm{S}^{(m)}(x))$. Pokud navíc formule D chybí, $\exists x A$ má tvar $\exists x \bigwedge_i (t_i(\underline{y}) < \mathrm{S}^{(m)}(x))$ a je ekvivalentní s (otevřenou) formulí $0 = 0$. Můžeme ale tvrdit, že konjunkce nulového počtu formulí je formule $0 = 0$ a že všechny krajní případy (kdy některé z čísel n nebo k je nula nebo kdy D chybí) jsou zahrnuty ve výše zmíněném zdůvodnění, že $\exists x A$ a $(*)$ jsou ekvivalentní formule. QED

Čtenáři, který pochybuje o dokazatelnosti sentence $\forall \underline{y} \exists x \bigwedge_i (t_i(\underline{y}) < \mathrm{S}^{(m)}(x))$, připomeňme, že podobnou sentencí jsme se dost podrobně zabývali v oddílu 3.2 v souvislosti s teorií SUCC.

Lemma 3.5.6 *Nechť $A(x, y_1, \ldots, y_q)$ je konjunkce atomických formulí v jazyce teorie* DOS. *Pak formule $\exists x A(x, \underline{y})$ je v teorii* DOS *ekvivalentní s jistou otevřenou formulí, jejíž všechny volné proměnné jsou mezi $y_1, \ldots, y_q$.*

Důkaz Je-li mezi atomickými podformulemi dané formule A nějaká formule tvaru $\mathrm{S}^{(m)}(x) < \mathrm{S}^{(n)}(x)$, kde $n \leq m$, nebo formule tvaru $\mathrm{S}^{(m)}(x) = \mathrm{S}^{(n)}(x)$, kde $m \neq n$, jsme hotovi. Každou ze sentencí $\neg\exists x(\mathrm{S}^{(m)}(x) < \mathrm{S}^{(n)}(x))$ a $\neg\exists x(\mathrm{S}^{(m)}(x) = \mathrm{S}^{(n)}(x))$ lze totiž pro $n \leq m$ resp. pro $m \neq n$ v teorii DOS dokázat užitím tvrzení 3.5.4 (e) a (f).

Jinak, tj. pokud A nemá žádnou podformuli uvedeného tvaru, vyhledejme všechny atomické podformule formule A, ve kterých se x vyskytuje na obou stranách rovnosti nebo nerovnosti. Všechny musí mít tvar buď $\mathrm{S}^{(m)}(x) = \mathrm{S}^{(m)}(x)$, nebo tvar $\mathrm{S}^{(m)}(x) < \mathrm{S}^{(n)}(x)$, kde $m < n$. Tyto formule můžeme prostě škrtnout, neboť uvnitř teorie DOS je jasné, že jsou splněny každým x. Pokud po tomto škrtání nezbude nic, tj. pokud A byla například $\mathrm{S}^{(2)}(x) < \mathrm{S}^{(5)}(x)\ \&\ \mathrm{S}^{(4)}(x) < \mathrm{S}^{(11)}(x)$, formule $\exists x A(x, \underline{y})$ je ekvivalentní s formulí $0 = 0$ a jsme hotovi.

Zbývá případ, kdy A je konjunkce atomických formulí neobsahujících x a formulí tvaru $\mathrm{S}^{(m)}(x) < t$, nebo $\mathrm{S}^{(m)}(x) = t$, nebo $t < \mathrm{S}^{(m)}(x)$, kde t je term neobsahující x a m je nějaké (v každé atomické formuli případně jiné) přirozené číslo. Opakovaným užitím tvrzení 3.5.4 (c) a (d) ve směru zprava doleva lze dosáhnout toho, že m bude vždy totéž. Například formule

$$\exists x(\mathrm{S}^{(4)}(x) = \mathrm{S}^{(3)}(y_1)\ \&\ y_2 < \mathrm{S}^{(11)}(x)\ \&\ \mathrm{S}(y_1) = y_3)$$

je ekvivalentní s formulí

$$\exists x(\mathrm{S}^{(11)}(x) = \mathrm{S}^{(10)}(y_1)\ \&\ y_2 < \mathrm{S}^{(11)}(x)\ \&\ \mathrm{S}(y_1) = y_3).$$

Tímto postupem je tvrzení lemmatu převedeno na tvrzení lemmatu 3.5.5. QED

Lemma 3.5.7 *Nechť φ je otevřená formule. Pak formule $\exists x \varphi$ je v teorii* DOS *ekvivalentní s jistou otevřenou formulí, která nemá jiné volné proměnné než ty, které jsou volné také ve formuli $\exists x \varphi$.*

Důkaz Ponechme nejprve kvantifikátor $\exists x$ stranou a pracujme pouze s formulí φ. Pomocí výrokově logicky ekvivalentních záměn převeďme formuli φ na formuli φ', která neobsahuje implikaci a v níž se negace nevyskytuje nikde jinde než případně u atomických podformulí. To se udělá stejně jako v důkazu věty 1.1.10 a nejsou k tomu potřeba axiomy teorie DOS ani znalosti o predikátové logice, vystačí se s výrokovou logikou.

Dále nahraďme každou podformuli formule φ' tvaru $\neg(t = u)$ nebo $\neg(t < u)$ formulí $t < u \vee u < t$ resp. formulí $t = u \vee u < t$. Tyto záměny jsou v teorii DOS (přesněji

řečeno už v teorii LO) ekvivalentní a jejich výsledkem je formule φ'' neobsahující jiné logické spojky než & a $\vee$.

Nakonec postupujme opět stejně jako v důkazu věty 1.1.10 a převeďme formuli φ'' na ekvivalentní formuli, která je disjunkcí konjunkcí, tj. která je tvaru $A_1 \vee .. \vee A_k$, kde každá A_i je konjunkce atomických formulí. Formule $\exists x\varphi$ je ekvivalentní s formulí $\exists x(A_1 \vee .. \vee A_k)$ a také s disjunkcí $\exists xA_1 \vee .. \vee \exists xA_k$. Každá z formulí $\exists xA_i$ je dle lemmatu 3.5.6 ekvivalentní s otevřenou formulí. Tedy $\exists x\varphi$ je ekvivalentní s otevřenou formulí. Navíc je zřejmé, že v žádném z kroků, které jsme provedli, nepřibyly volné proměnné. QED

Lemma 3.5.8 *Každá otevřená sentence v jazyce* $\{0, \mathrm{S}, <\}$ *je v teorii* DOS *dokazatelná nebo vyvratitelná.*

Důkaz Dosazením nuly do sentence 3.5.4(e) dostaneme $\mathsf{DOS} \vdash \overline{m} < \overline{n}$ pro $m < n$. Uvažme zbývající případy, tj. případy, kdy $m = n$ nebo $n < m$. Když $m = n$, pak $\mathsf{DOS} \vdash \overline{m} = \overline{n}$. Když $n < m$, pak dle předchozího $\mathsf{DOS} \vdash \overline{n} < \overline{m}$. V obou případech axiom LO2 dává $\mathsf{DOS} \vdash \neg(\overline{m} < \overline{n})$. Každá sentence tvaru $\overline{m} < \overline{n}$ je tedy v teorii DOS dokazatelná nebo vyvratitelná. Podobnými úvahami lze zjistit, že totéž platí i pro každou sentenci tvaru $\overline{m} = \overline{n}$. To dohromady znamená, že každá atomická sentence je v teorii DOS dokazatelná nebo vyvratitelná. Zbytek je indukce podle počtu logických spojek ve formuli φ. Je-li například φ tvaru $\varphi_1 \to \varphi_2$ a φ_2 je dokazatelná nebo φ_1 vyvratitelná, pak $\mathsf{DOS} \vdash \varphi$. Je-li naopak φ_1 dokazatelná a φ_2 vyvratitelná, pak $\mathsf{DOS} \vdash \neg\varphi$. Podobně lze uvažovat i v případě ostatních logických spojek. QED

Věta 3.5.9 *Teorie* DOS *připouští eliminaci kvantifikátorů. Obě teorie* DOS *a* DO *jsou úplné.*

Důkaz Nechť je dána libovolná formule ψ v jazyce teorie DOS. Nahraďme nejprve každou její podformuli tvaru $\forall x\varphi$ ekvivalentní formulí $\neg\exists x\neg\varphi$. Výslednou formuli označme ψ_0. Formule ψ_0 neobsahuje univerzální kvantifikátor. Neobsahuje-li ψ_0 ani existenční kvantifikátor, jsme hotovi. Jinak ψ_0 má podformuli $\exists x\varphi$ takovou, že φ je otevřená. Označme ψ_1 formuli, která vznikne z ψ_0 aplikací lemmatu 3.5.7 na formuli $\exists x\varphi$. Je-li třeba, opakujme tento postup, kterým jsme získali ψ_1 z ψ_0, ještě vícekrát. Výsledkem je otevřená formule, která je ekvivalentní s původní formulí ψ a která vůči ψ nemá žádné volné proměnné navíc. Tím je zdůvodněno, že teorie DOS připouští eliminaci kvantifikátorů.

Je-li ψ sentence, pak existuje otevřená sentence χ ekvivalentní s ψ. Dle lemmatu 3.5.8 je sentence χ dokazatelná nebo vyvratitelná. Platí-li $\mathsf{DOS} \vdash \chi$, pak z $\mathsf{DOS} \vdash \psi \equiv \chi$ plyne $\mathsf{DOS} \vdash \psi$. Platí-li $\mathsf{DOS} \vdash \neg\chi$, pak z $\mathsf{DOS} \vdash \psi \equiv \chi$ plyne $\mathsf{DOS} \vdash \neg\psi$. Teorie DOS je tedy úplná. Z toho a z faktu, že teorie DOS je konzervativním rozšířením teorie DO, plyne i úplnost teorie DO. QED

K důkazu věty 3.5.9 poznamenejme, že přestože definice úplné teorie mluví pouze o sentencích, opravdu jsme se museli zabývat všemi formulemi. Lemma 3.5.7

umožňuje odstranit kvantifikátor z otevřené formule, a máme-li je použít k nalezení otevřené formule ekvivalentní s danou formulí ψ, musíme postupovat od vnitřních kvantifikátorů směrem k vnějším. To znamená, že i když ψ je sentence, musíme se zabývat jejími podformulemi, které sentencemi být nemusí.

Druhý příklad na eliminaci kvantifikátorů, kterým se chceme zabývat, je *teorie celočíselného sčítání*. Tato teorie má jazyk $\{+, 0, 1\}$, čtyři jednotlivé axiomy a tři axiomatická schémata. Čtyři jednotlivé axiomy jsou:

Ad1: $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$,

Ad2: $\forall x (x + 0 = x)$,

Ad3: $\forall x \exists y (x + y = 0)$,

Ad4: $\forall x \forall y (x + y = y + x)$.

Tyto axiomy postulují, že operace sčítání je asociativní a komutativní, nula je neutrální a že ke každému objektu existuje objekt k němu opačný. Objektům teorie celočíselného sčítání říkejme *čísla*. Snadno se dokáže, že nula je jediné neutrální číslo a že ke každému číslu existuje právě jedno číslo k němu opačné. Poznamenejme, že teorii s jazykem $\{+, 0\}$ a s axiomy Ad1–Ad4 jsme ve cvičeních oddílu 3.2 říkali *teorie abelovských grup*.

Numerály užíváme v teorii celočíselného sčítání ve stejném smyslu jako v teorii komutativních těles z oddílu 3.2: $\overline{0}$ je term 0, $\overline{m+1}$ je term $(\overline{m}+1)$. Odhlédneme-li od závorek, $\overline{m}$ je součtem m jedniček.

Je-li $t(y_1, .., y_q)$ libovolný term v jazyce $\{+, 0, 1\}$, můžeme opět odhlédnout od závorek (tj. několikrát užít axiom Ad1), „sestěhovat“ k sobě všechny výskyty téže proměnné a všechny výskyty konstanty 1 (tj. užít případně opakovaně axiom Ad4) a upravit počet výskytů konstanty 0 na jeden (užitím Ad2). Domluvíme-li se, že my znamená $y + .. + y$ (m sčítanců), a přesuneme-li ještě konstanty na vhodné místo, dostaneme term tvaru $m_1 y_1 + .. + m_q y_q + \overline{r}$. Tím jsme zdůvodnili, že ke každému termu $t(\underline{y})$ v jazyce $\{+, 0, 1\}$ existuje term $u(\underline{y})$ tvaru $m_1 y_1 + .. + m_q y_q + \overline{r}$ takový, že sentence $\forall \underline{y}(t(\underline{y}) = u(\underline{y}))$ je dokazatelná v teorii celočíselného sčítání.

Pomocí numerálů a termů tvaru my můžeme formulovat zbývající axiomy (schémata) teorie celočíselného sčítání:

Ad5: $\forall x (mx = my \rightarrow x = y)$, je-li $m \geq 1$,

Ad6: $\forall x (mx \neq \overline{k})$, je-li $0 < k < m$,

Ad7: $\forall x \exists y (x = my \vee x = my + \overline{1} \vee .. \vee x = my + \overline{m-1})$, je-li $m \geq 1$.

Výslednou teorii s axiomy Ad1–Ad7 označme IAdd (integer addition). Schéma Ad7 lze chápat jako axiom o dělení se zbytkem: každé číslo x lze dělit číslem $m \geq 1$, výsledkem je podíl y a zbytek, který je menší než dělitel m. Protože mezi symboly jazyka není symbol pro uspořádání, nelze napsat přímo, že zbytek je menší než m. Místo toho jsou všechny zbytky menší než m vyjmenovány. Zdůrazněme pro jistotu,

že my i $\overline{m}$ jsou zkratky, které neznamenají rozšíření jazyka. V jazyce teorie IAdd nemáme násobení a nemůžeme v něm vyjádřit fakt, že každé číslo x lze dělit každým nenulovým číslem z. Pro každé (metamatematické) číslo $m \geq 1$ ale můžeme (vždy jinou sentencí) vyjádřit, že každé číslo x lze dělit se zbytkem číslem m. Je zřejmé, že všechny axiomy Ad1–Ad7 platí ve struktuře $\langle \mathrm{Z}, +, 0, 1 \rangle$ celých čísel se sčítáním, nulou a jedničkou.

Konzervativní rozšíření teorie IAdd, o kterém postupně dokážeme, že připouští eliminaci kvantifikátorů, získáme přidáním nekonečně mnoha binárních predikátových symbolů $=_n$, kde $n \geq 1$ je přirozené číslo. Predikát $=_n$ je definován axiomem

$$\forall x \forall y (x =_n y \equiv \exists v (x + nv = y)).$$

Zápis $x =_n y$ čteme číslo x je n-kongruentní s číslem y. Nechť dále L^+_{IAdd} označuje jazyk $\{+, 0, 1, =_1, =_2, \dots\}$ vzniklý přidáním právě definovaných binárních symbolů k jazyku $L_{\mathsf{IAdd}} = \{+, 0, 1\}$ teorie IAdd.

Lemma 3.5.10 *Následující sentence jsou v teorii* IAdd *dokazatelné pro libovolná čísla $n \geq 1$ a $k \geq 1$.*

(a) $\forall x \forall y \forall z (y + x = z + x \equiv y = z)$,
(b) $\forall x (x =_n x)$,
(c) $\forall x \forall y (x =_n y \to y =_n x)$,
(d) $\forall x \forall y \forall z (x =_n y \;\&\; y =_n z \to x =_n z)$,
(e) $\forall x \forall y \forall z (y + x =_n z + x \equiv y =_n z)$,
(f) $\forall x \forall y (kx = ky \equiv x = y)$,
(g) $\forall x \forall y (kx =_{kn} ky \equiv x =_n y)$,
(h) $\forall x \forall y (x =_{kn} y \to x =_n y)$.

Důkaz Sentenci (c) lze dokázat takto:

> Nechť $x =_n y$. Dle definice symbolu $=_n$ existuje v takové, že $x + nv = y$. Vezměme z opačné k v a přičtěme je n-krát na obě strany rovnosti. Dostaneme $x + nv + nz = y + nz$ a $x = y + nz$. Tedy $y =_n x$.

Zbývající úvahy jsou podobné a ponecháváme je na čtenáři. QED

Lemma 3.5.11 *Následující sentence jsou v teorii* IAdd *dokazatelné pro libovolné číslo $n \geq 1$ a pro libovolná m a r.*

(a) $\forall x \forall y (m(x + y) = mx + my)$,
(b) $\overline{m} + \overline{r} = \overline{m + r}$,
(c) $m\overline{r} = \overline{mr}$,
(d) $\forall x (m(rx) = (mr)x)$,
(e) $\overline{m} \neq \overline{r}$, *když* $m \neq r$,
(f) $\overline{m} =_n \overline{r}$, *když n dělí $m - r$*,
(g) $\neg(\overline{m} =_n \overline{r})$, *když n nedělí $m - r$.*

Důkaz Důkazy sentencí (a)–(d) jsou jasné, termy na obou stranách rovnosti se liší nanejvýš pořadím členů a umístěním závorek. Malý trik je v důkazu sentence (e). Předpokládejme například $r < m$ a uvažujme v teorii IAdd:

> Nechť $\overline{m} = \overline{r}$, tj. $\overline{m - r} + \overline{r} = \overline{r}$. Dle (a) lemmatu 3.5.10 platí $\overline{m - r} = 0$. Dále platí $\overline{m - r + 1} = 1$ a $(m - r + 1)1 = 1$. To je spor s axiomem Ad6.

Důkaz sentence (f) ponecháváme na čtenáři, použije se již dokázaná sentence (c). Dokažme ještě (g). Předpokládejme $r \leq m$ a dělme rozdíl $m-r$ se zbytkem číslem n: $m-r = nq+k$, $k < n$. Protože n nedělí $m-r$, máme $k \neq 0$. Uvažujme v teorii IAdd:

> Nechť $\overline{m} =_n \overline{r}$. Pak $\overline{m-r} + \overline{r} =_n \overline{r}$, dále $\overline{m-r} =_n 0$, a také $n\overline{q} + \overline{k} =_n 0$. Dle (f) platí $n\overline{q} =_n 0$. Z (c) a (d) lemmatu 3.5.10 plyne $n\overline{q} =_n n\overline{q} + \overline{k}$. Z toho dále plyne $0 =_n \overline{k}$. Tedy existuje v takové, že $nv = \overline{k}$. To je spor s axiomem Ad6.

QED

Eliminace kvantifikátorů pro teorii IAdd (přesněji řečeno pro její rozšíření o definice symbolů $=_n$) se nyní dokáže podobně jako pro teorii DOS. Domluvme se, že formulím tvaru $t = u$, $t \neq u$, $t =_n u$ a $\neg(t =_n u)$ říkáme *literály*. To je ve shodě s terminologií, kterou jsme v kapitole 2 užívali v souvislosti s výrokovou logikou.

Lemma 3.5.12 *Nechť $A(x, y_1, \ldots, y_q)$ je konjunkce literálů v jazyce teorie* IAdd *taková, že každý literál v A obsahující proměnnou x má jeden z tvarů $x = t(\underline{y})$, nebo $x \neq t(\underline{y})$, nebo $x =_n t(\underline{y})$, kde t je term neobsahující x. Pak formule $\exists x A$ je v teorii* IAdd *ekvivalentní s otevřenou formulí, jejíž všechny volné proměnné jsou mezi $y_1, \ldots, y_q$.*

Důkaz Je-li mezi literály formule A obsahujícími x alespoň jedna rovnost, pak A má tvar $x = t(\underline{y}) \ \& \ B(x, \underline{y})$ a formule $\exists x A$ je ekvivalentní s formulí $B(t(\underline{y}), \underline{y})$. V opačném případě má formule A tvar

$$x =_{n_1} t_1(\underline{y}) \ \& \ \ldots \ \& \ x =_{n_k} t_k(\underline{y}) \ \& \ x \neq u_1(\underline{y}) \ \& \ \ldots \ \& \ x \neq u_r(\underline{y}) \ \& \ D(\underline{y}),$$

kde termy $t_i(\underline{y})$ a $u_j(\underline{y})$ a formule $D(\underline{y})$ neobsahují x. Zvolme číslo m, které je společným násobkem čísel $n_1 \ldots, n_k$. Tvrdíme, že $\exists x A$ je ekvivalentní s formulí

$$D(\underline{y}) \ \& \bigvee_{j<m} (\overline{j} =_{n_1} t_1(\underline{y}) \ \& \ \ldots \ \& \ \overline{j} =_{n_k} t_k(\underline{y})). \qquad (*)$$

Toto je důkaz jejich ekvivalence:

> Nechť pro x a $y_1, \ldots, y_q$ platí $A(x, \underline{y})$. Dle axiomu Ad7 k x existuje y takové, že x je rovno některému z čísel my, $my+\overline{1}$ až $my+\overline{m-1}$. Tedy x je m-kongruentní s některým z čísel $\overline{0}, \ldots, \overline{m-1}$.
> Z $x =_m \overline{0}$ a $\bigwedge_{i=1}^{k}(x =_{n_i} t_i(\underline{y}))$ plyne $\bigwedge_{i=1}^{k}(\overline{0} =_{n_i} t_i(\underline{y}))$.
> Z $x =_m \overline{1}$ a $\bigwedge_{i=1}^{k}(x =_{n_i} t_i(\underline{y}))$ plyne $\bigwedge_{i=1}^{k}(\overline{1} =_{n_i} t_i(\underline{y}))$.
> $\vdots$
> Z $x =_m \overline{m-1}$ a $\bigwedge_{i=1}^{k}(x =_{n_i} t_i(\underline{y}))$ plyne $\bigwedge_{i=1}^{k}(\overline{m-1} =_{n_i} t_i(\underline{y}))$.
> Přitom se uplatnila tvrzení (h), (c) a (d) lemmatu 3.5.10. Zjistili jsme, že platí některá z podmínek $\bigwedge_{i=1}^{k}(\overline{j} =_{n_i} t_i(\underline{y}))$, kde $j < m$, tedy platí $(*)$.
> Nechť naopak pro $y_1, \ldots, y_q$ platí podmínka $(*)$. Nechť $\overline{j}$ je ono z čísel $\overline{0}$ až $\overline{m-1}$, pro které platí $\bigwedge_{i=1}^{k}(\overline{j} =_{n_i} t_i(\underline{y}))$. Platí také $\bigwedge_{i=1}^{k}(\overline{j} + \overline{m} =_{n_i} t_i(\underline{y}))$,

$\bigwedge_{i=1}^{k}(\overline{j} + \overline{2m} =_{n_i} t_i(\underline{y}))$ až $\bigwedge_{i=1}^{k}(\overline{j} + \overline{rm} =_{n_i} t_i(\underline{y}))$. Alespoň jedno z $r+1$ různých čísel $\overline{j}, \overline{j}+\overline{m}, \ldots, \overline{j}+\overline{rm}$ se liší od všech $u_1(\underline{y}), \ldots, u_r(\underline{y})$, a to lze zvolit za x splňující podmínku $A(x, \underline{y})$.

Druhou část důkazu, zdůvodnění implikace $(*) \to \exists x A$, se nám podařilo zpřehlednit díky malé nekorektnosti, která se skrývá v obratu nechť $\overline{j}$ je ono z čísel atd. Za tímto obratem je třeba si představit m kroků tvaru když $\bigwedge_{i=1}^{k}(\overline{0} =_{n_i} t_i(\underline{y}))$, pak $\exists x A(x, \underline{y})$; když $\bigwedge_{i=1}^{k}(\overline{1} =_{n_i} t_i(\underline{y}))$, pak $\exists x A(x, \underline{y})$ atd. Bez takovéhoto mírně nekorektního zkracování, zato méně přehledně, jsme napsali zdůvodnění implikace $\exists x A \to (*)$. QED

Příklad 3.5.13 Aplikujeme-li postup popsaný v důkazu předchozího lemmatu na formuli

$$\exists x(x =_{30} y_1 \ \&\ x =_{14} y_2 \ \&\ x =_{35} y_3),$$

dostaneme s ní ekvivalentní otevřenou formuli

$$\bigvee_{j<210} (\overline{j} =_{30} y_1 \ \&\ \overline{j} =_{14} y_2 \ \&\ \overline{j} =_{35} y_3).$$

Nezabýváme se faktem, že tato formule je zbytečně dlouhá. Použijí-li se podrobnější úvahy o dělitelnosti celých čísel, lze nalézt formuli, která je dokonce *kratší* než kterýkoliv z dvou set deseti členů naší disjunkce, viz cvičení 14.

Lemma 3.5.14 *Nechť $A(x, y_1, \ldots, y_q)$ je formule v jazyce L^{+}_{lAdd}, která je konjunkcí literálů tvaru $t = s$, nebo $t \neq s$, nebo $t =_n s$. Pak formule $\exists x A$ je v teorii* lAdd *ekvivalentní s jistou otevřenou formulí, jejíž všechny volné proměnné jsou mezi $y_1, \ldots, y_q$.*

Důkaz Nechť formule $A(x, \underline{y})$ je dána. Nejprve užitím tvrzení 3.5.10 (a) a (c) převeďme formuli A na ekvivalentní formuli $A_1(x, \underline{y})$, ve které se proměnná x nikdy nevyskytuje na pravé straně rovnosti, nerovnosti nebo kongruence. Když například A je formule

$$x + y_1 = 3x + \overline{5} \ \&\ 4x \neq y_2 \ \&\ 15x =_7 9x + y_2 + 2y_3,$$

pak A_1 je

$$2x + \overline{5} = y_1 \ \&\ 4x \neq y_2 \ \&\ 6x =_7 y_2 + 2y_3.$$

Dále užijme tvrzení 3.5.10 (f) a (g) a nalezněme formuli A_2 ekvivalentní s A_1, ve které se x vyskytuje vždy pouze v kontextu „mx“, kde $m \geq 1$ je stejné pro všechny výskyty x. V našem příkladu to znamená první, druhý a třetí literál formule A_1 „násobit“ šesti, třemi a dvěma. Výslednou formulí A_2 je formule

$$12x + \overline{30} = 6y_1 \ \&\ 12x \neq 3y_2 \ \&\ 12x =_{14} 2y_2 + 4y_3.$$

Nyní užijme vhodným způsobem tvrzení 3.5.10 (a) a (e) a nalezněme formuli A_3 ekvivalentní s A_2 takovou, že x se v A_3 vyskytuje pouze v kontextu „$mx+s(\underline{y})$“, kde číslo m a term $s(\underline{y})$ neobsahující x jsou společné pro všechny výskyty proměnné x.

V našem příkladu lze vystačit s termem $s(\underline{y})$ neobsahujícím proměnné $y_1, .., y_q$ a za A_3 vzít například formuli

$$12x + \overline{30} = 6y_1 \ \& \ 12x + \overline{30} \neq 3y_2 + \overline{30} \ \& \ 12x + \overline{30} =_{14} 2y_2 + 4y_3 + \overline{30}.$$

Formule A_3 je formule tvaru $B(mx + s(\underline{y}), \underline{y})$. Zvolme proměnnou z různou od x i od všech $y_1, .., y_q$. Formule $\exists x A(x, \underline{y})$ je ekvivalentní s $\exists z(z =_m s(\underline{y}) \ \& \ B(z, \underline{y}))$ (cvičení), což je formule, která díky lemmatu 3.5.12 je ekvivalentní s otevřenou formulí. QED

Lemma 3.5.15 *Nechť φ je otevřená formule v jazyce L^+_{IAdd}. Pak formule $\exists x\varphi$ je v teorii* IAdd *ekvivalentní s jistou otevřenou formulí, která nemá jiné volné proměnné než ty, které jsou volné také ve formuli $\exists x\varphi$.*

Důkaz Důkaz lemmatu 3.5.7 spočíval v tom, že mezi kroky převádějící formuli φ na formuli v disjunktivním normálním tvaru jsme vložili krok, který odstranil všechny literály s negací. Nyní postupujme obdobně až na to, že literály tvaru $t \neq s$ zůstanou beze změny, odstraníme pouze literály tvaru $\neg(t =_n s)$, a to využitím ekvivalence

$$\neg(t =_n s \equiv t =_n s + \overline{1} \vee \ .. \ \vee t =_n s + \overline{n-1}).$$

Domníváme se, že důkaz této ekvivalence lze ponechat za cvičení. Výsledkem je formule tvaru $A_1 \vee .. \vee A_k$, která je ekvivalentní s φ a v níž každá A_i je konjunkcí literálů tvaru $t = s$, $t \neq s$ a $t =_n s$. Pak, stejně jako v důkazu lemmatu 3.5.7, $\exists x\varphi$ je ekvivalentní s $\exists x(A_1 \vee .. \vee A_k)$ a také s $\exists x A_1 \vee .. \vee \exists x A_k$. Každá $\exists x A_i$ je dle lemmatu 3.5.14 ekvivalentní s otevřenou formulí. Tedy $\exists x\varphi$ je ekvivalentní s otevřenou formulí a opět nepřibyly volné proměnné. QED

Lemma 3.5.16 *Každá otevřená sentence v jazyce L^+_{IAdd} je v teorii* IAdd *dokazatelná nebo vyvratitelná.*

Důkaz Ke každému uzavřenému termu t existuje (jediné) přirozené číslo m takové, že rovnost $t = \overline{m}$ je dokazatelná v teorii IAdd. Každá atomická sentence je tedy ekvivalentní se sentencí tvaru $\overline{m} = \overline{r}$ nebo $\overline{m} =_n \overline{r}$. Každá taková sentence je dokazatelná nebo vyvratitelná díky tvrzením (e)–(g) lemmatu 3.5.11. Zbytek je indukce dle počtu logických spojek, stejně jako v důkazu lemmatu 3.5.8. QED

Věta 3.5.17 *Rozšíření teorie* IAdd *o definice symbolů $=_n$ připouští eliminaci kvantifikátorů. Teorie* IAdd *je úplná.*

Důkaz je úplně stejný jako důkaz věty 3.5.9.

Náš poslední a nejsložitější příklad na eliminaci kvantifikátorů se týká struktury $\mathbf{R} = \langle \mathrm{R}, +, \cdot, 0, 1, < \rangle$ *reálných čísel*. Stejně jako pro strukturu $\langle \mathrm{N}, 0, \mathrm{s}, < \rangle$ a pro strukturu $\langle \mathrm{Z}, +, 0, 1 \rangle$ lze i pro strukturu $\mathbf{R}$ stanovit přehlednou množinu axiomů, které v $\mathbf{R}$ platí a které dohromady tvoří teorii, jejíž úplnost lze dokázat eliminací kvantifikátorů. Tento fakt dokázal A. Tarski a je to jeden z nejvýznamnějších

výsledků moderní logiky. Postup, který si ukážeme, je založen na návodu v Rabinově kapitole [70] příručky [4] a na Cohenově článku [12]. Použijeme také některé myšlenky z [51].

Nejprve definujme *teorii uspořádaných těles*. Tato teorie má jazyk $\{+, \cdot, 0, 1, <\}$, axiomy R1–R10 teorie komutativních těles uvedené v oddílu 3.2 a dále následujících pět axiomů týkajících se uspořádání:

R11: $\forall x \forall y \forall z (x < y \ \& \ y < z \ \rightarrow \ x < z)$,

R12: $\forall x \forall y (x < y \ \rightarrow \ \neg (y < x))$,

R13: $\forall x \forall y (x < y \ \vee \ x = y \ \vee \ y < x)$,

R14: $\forall x \forall y \forall z (y < z \ \rightarrow \ y + x < z + x)$,

R15: $\forall x \forall y \forall z (y < z \ \& \ 0 < x \ \rightarrow \ y \cdot x < z \cdot x)$.

Axiomy R11–R13 jsou totožné s axiomy LO1–LO3 teorie lineárního uspořádání. Axiomy R14 a R15 postulují, že sčítání a násobení v rozumném smyslu zachovávají uspořádání.

Objektům teorie uspořádaných těles říkáme stejně jako v oddílu 3.2 *čísla*, někdy také *body*. Nejzákladnější fakty o počítání s čísly (tj. o vlastnostech operací $+$ a $\cdot$), které lze dokázat v teorii uspořádaných těles, jsme uvedli už v lemmatu 3.2.14. Protože ke každému x existuje právě jedno y opačné k x, můžeme ono y opačné k x označit $-x$. Jinými slovy, sentence $\forall x \forall y (y = -x \ \equiv \ y + x = 0)$ definuje unární funkční symbol „$-$“ v souladu s větou 3.5.3. V následujícím lemmatu jsou vyjmenovány nejzákladnější fakty, které lze v teorii uspořádaných těles dokázat o uspořádání a o operaci „$-$“. Zápis $x - y$ je ovšem zkratka pro $x + (-y)$. Číslům větším než nula říkejme *kladná*, číslům menším než nula *záporná*. Bude-li se to hodit, místo $x < y$ budeme psát $y > x$. Stejně jako v teorii LO je zápis $x \leq y$ zkratkou pro formuli $x < y \ \vee \ x = y$.

Lemma 3.5.18 *Následující sentence jsou dokazatelné v teorii uspořádaných těles.*

(a) $\forall x \forall y (0 < x \ \rightarrow \ (0 < x \cdot y \ \equiv \ 0 < y))$,
(b) $\forall x \forall y (x < 0 \ \rightarrow \ (0 < x \cdot y \ \equiv \ y < 0))$,
(c) $\forall x (x < 0 \ \equiv \ 0 < -x)$,
(d) $\forall x (-(-x) = x)$,
(e) $\forall x \forall y (x \cdot (-y) = -(x \cdot y))$,
(f) $\forall x \forall y (-(x - y) = y - x)$,
(g) $\forall x (0 \neq x \ \equiv \ 0 < x^2)$,
(h) $\overline{m} < \overline{r}$, *je-li* $m < r$,
(i) $\forall x \exists y_1 \exists y_2 (y_1 < x \ \& \ x < y_2)$,
(j) $\forall x \forall y (x < y \ \rightarrow \ \exists z (x < z < y))$.

Důkaz Předpokládáme, že všechny důkazy čtenář zná nebo si je dovede vymyslet. Uvádíme jen několik nejdůležitějších myšlenek.

Platí-li v (c) $x < 0$, můžeme dle axiomu R14 přičíst $-x$ na obě strany a dostaneme $0 < -x$.

Protože $-(x \cdot y)$ je ono číslo, které přičteno k $x \cdot y$ dá nulu, v (e) stačí ověřit, že $x \cdot (-y) + x \cdot y = 0$.

V (g), platí-li $x \neq 0$, pak $0 < x$ nebo $x < 0$. Když $0 < x$, axiom R15 dává $0 < x^2$. Když $x < 0$, pak $0 < -x$ dle (c). Obě strany této nerovnosti můžeme vynásobit kladným číslem $-x$, tedy $0 < (-x)^2$. Platí tedy $0 < x^2$, protože $(-x)^2 = x^2$ dle (e).

Volbou $x = 1$ v (g) dostaneme $0 < 1$. Z této nerovnosti plynou i ostatní instance v (h).

Nechť z je inverzní k $\overline{2}$, tj. nechť $z \cdot \overline{2} = 1$. Snadno lze ověřit, že $0 < z$ a že je-li $x < y$, pak také $x < z \cdot (x + y) < y$. Tím je dokázáno (j).

QED

Z dokazatelnosti sentencí (i) a (j) je jasné, že je-li $\langle D, +, \cdot, 0, 1, < \rangle$ libovolný model teorie uspořádaných těles, pak $\langle D, < \rangle$ je model teorie DNO. Každý model teorie uspořádaných těles je tedy nekonečný. Dále je zřejmé, že struktury $\mathbf{R}$ i $\mathbf{Q}$ jsou modely teorie uspořádaných těles. To je vše, co jsme schopni říci o modelech této teorie. Protože o modelech už tady (téměř) mluvit nebudeme, domluvme se, že písmena a, b, c, d, která obvykle značí prvky struktur, značí ve zbytku tohoto oddílu proměnné, případně termy.

Teorie reálně uzavřených těles má jazyk stejný jako teorie uspořádaných těles, axiomy R1–R15, a dále všechny sentence tvaru

$$\text{R16:} \qquad \forall \underline{y} \forall a \forall b (a < b \ \&\ t(a, \underline{y}) \cdot t(b, \underline{y}) < 0 \ \rightarrow\ \exists x (a < x < b \ \&\ t(x, \underline{y}) = 0)),$$

kde t je libovolný term v jazyce $\{+, \cdot, 0, 1, <\}$. Je zřejmé, že by se nic nestalo, kdybychom mezi symboly termu t připustili i symbol „$-$“. Z (a) a (b) lemmatu 3.5.18 plyne, že součin $t(a, \underline{y}) \cdot t(b, \underline{y})$ je záporný, právě když čísla $t(a, \underline{y})$ a $t(b, \underline{y})$ jsou obě nenulová a mají opačná znaménka. Z lemmatu 3.2.15 víme, že term $t(x, \underline{y})$ je vlastně polynom v x s koeficienty, které jsou termy v $\underline{y}$. Schéma R16 tedy tvrdí, že je-li $a < b$ a je-li f polynom takový, že čísla $f(a)$ a $f(b)$ mají opačná znaménka, pak f má kořen v intervalu (a, b). Teorii s axiomy R1–R16 značíme RCF (real closed fields). Snadno lze zdůvodnit, že struktura $\mathbf{Q}$ není modelem teorie RCF. Vezmeme-li například term $x^2 - \overline{2}$ za $t(x)$, platí (tj. v RCF lze dokázat, že) $t(\overline{1}) \cdot t(\overline{2}) < 0$, ale mezi jedničkou a dvojkou neexistuje racionální číslo x takové, že $t(x) = 0$. Kdybychom se museli obejít bez odčítání, zvolili bychom term $x^2 + y$. Ten v $\mathbf{Q}$ také porušuje schéma R16. O zdůvodnění, proč schéma R16 platí v $\mathbf{R}$, se ještě zmíníme.

Sentenci

$$\begin{aligned}
\forall z_0 \forall z_1 \forall z_2 \forall x_0 \forall x_1 \forall x_2 (\neg (z_0 = 0 \ \&\ z_1 = 0 \ \&\ z_2 = 0) \ \&\ \\
\&\ z_0 \cdot x_0^2 + z_1 \cdot x_0 + z_2 = 0 \\
\&\ z_0 \cdot x_1^2 + z_1 \cdot x_1 + z_2 = 0 \\
\&\ z_0 \cdot x_2^2 + z_1 \cdot x_2 + z_2 = 0 \\
\rightarrow\ x_0 = x_1 \ \vee\ x_0 = x_2 \ \vee\ x_1 = x_2)
\end{aligned}$$

lze číst každý netriviální polynom stupně 2 má nejvýše dva různé kořeny. Označme tuto sentenci ρ_2. Naprosto analogicky lze pro každé $n \geq 0$ napsat sentenci ρ_n,

která tvrdí, že každý netriviální polynom stupně n má nejvýše n různých kořenů. Sentence ρ_n má v závorce v prvním řádku negaci $(n+1)$-členné konjunkce, pak $n+1$ řádků vyjadřujících, že x_0 až x_n jsou kořeny polynomu s koeficienty $z_0, .., z_n$, a v posledním řádku disjunkci s $\binom{n+1}{2}$ členy vyjadřující, že některá dvě čísla mezi x_0 až x_n jsou si rovna. Netriviální polynom je ovšem takový, jehož koeficienty nejsou samé nuly. Protože o hodnotách nebo kořenech polynomu s koeficienty $z_0, .., z_n$ mluvíme uvnitř teorie RCF, ale o stupni polynomu mluvíme na metamatematické úrovni, neklademe si podmínku (na rozdíl od toho, co je běžné v algebře), že nejvyšší koeficient polynomu je nenulový. Polynom stupně n je tedy pro nás libovolná $(n+1)$-tice $z_0, .., z_n$ a za touto $(n+1)$-ticí vidíme term $z_0 \cdot x^n + .. + z_n$.

K důkazu sentencí ρ_n použijeme následující lemma, které lze označit jako lemma o dělení polynomu lineárním faktorem.

Lemma 3.5.19 *Nechť $n \geq 1$ a nechť $t_0(\underline{y}), .., t_n(\underline{y})$ a $u(\underline{y})$ jsou termy neobsahující proměnnou x. Pak existují termy $s_0(\underline{y}), .., s_{n-1}(\underline{y})$ neobsahující x takové, že označíme-li $f(x)$ polynom s koeficienty $t_0(\underline{y}), .., t_n(\underline{y})$ a označíme-li $g(x)$ polynom s koeficienty $s_0(\underline{y}), .., s_{n-1}(\underline{y})$, je sentence*

$$\forall \underline{y} \forall x (f(x) = (x - u) \cdot g(x) + f(u))$$

dokazatelná v teorii RCF.

Důkaz Nechť n a termy $t_i(\underline{y})$ a $u(\underline{y})$ jsou dány. Zvolme za $s_0(\underline{y})$, $s_1(\underline{y})$ až $s_{n-1}(\underline{y})$ termy $t_0(\underline{y})$, $t_0(\underline{y}) \cdot u(\underline{y}) + t_1(\underline{y})$ až $t_0(\underline{y}) \cdot u^{n-1}(\underline{y}) + t_1(\underline{y}) \cdot u^{n-2}(\underline{y}) + .. + t_{n-1}(\underline{y})$. Pišme t_i a u místo $t_i(\underline{y})$ a $u(\underline{y})$, vynechme všechny symboly „$\cdot$“ a dokažme požadovanou sentenci počítáním v teorii RCF:

$$\begin{aligned}
(x-u)[t_0 x^{n-1} + (t_0 u + t_1)x^{n-2} + .. + (t_0 u^{n-1} + .. + t_{n-1})] + f(u) = \\
&= t_0 x^n + (t_0 u + t_1)x^{n-1} + .. + (t_0 u^{n-1} + .. + t_{n-1})x \\
&\quad - t_0 u x^{n-1} - (t_0 u^2 + t_1 u)x^{n-2} - .. - (t_0 u^n + .. + t_{n-1} u) + f(u) = \\
&= t_0 x^n + t_1 x^{n-1} + .. + t_{n-1} x - \textstyle\sum_{i=0}^{n-1} t_i u^{n-i} + \sum_{i=0}^{n} t_i u^{n-i} = \\
&= t_0 x^n + t_1 x^{n-1} + .. + t_{n-1} x + t_n = \\
&= f(x).
\end{aligned}$$

QED

Lemma 3.5.20 *Sentenci ρ_n lze pro každé $n \geq 0$ dokázat v teorii* RCF.

Důkaz Když $n = 0$, pak $\binom{n+1}{2} = 0$, disjunkce nula členů je spor, a ρ_n je sentence $\forall z_0 (z_0 \neq 0 \ \& \ z_0 = 0 \rightarrow \bot)$, kde $\bot$ je onen spor. Tato sentence je v RCF dokazatelná, netriviální polynom stupně nula opravdu nemá žádné kořeny.

Nechť $n > 0$ a nechť $\rho_0, .., \rho_{n-1}$ jsou již dokázány. Dokažme ρ_n:

Nechť jsou dány koeficienty $z_0, .., z_n$ netriviálního polynomu f stupně n a nechť f má $n+1$ navzájem různých kořenů $a_0, .., a_n$. Když $z_0 = 0$, pak $a_0, .., a_n$

jsou zároveň různé kořeny polynomu stupně $n-1$ s koeficienty $z_1,..,z_n$, což je ale spor s ρ_{n-1}. Nechť tedy $z_0 \neq 0$. Vezměme čísla z_0, $z_0a_0 + z_1$ atd., tj. čísla tvaru $\sum_{i=0}^{k} z_i a_0^{k-i}$, kde $0 \leq k < n$. Z 3.5.19 víme, že tato čísla tvoří koeficienty polynomu g stupně $n-1$, pro který platí $\forall x(f(x) = (x-a_0)g(x) + f(a_0))$. Protože a_0 je kořen polynomu f, máme $\forall x(f(x) = (x-a_0)g(x))$. Když $i \neq 0$, v součinu $(a_i - a_0)g(a_i)$ je první činitel nenulový. Celý součin je ale nulový, protože a_i je kořen polynomu f. Lemma 3.2.14(d) dává $g(a_i) = 0$. Tedy $a_1,..,a_n$ je n navzájem různých kořenů polynomu g. Polynom g je netriviální, protože má nenulový koeficient z_0. To je spor s ρ_{n-1}.

QED

Z lemmatu 3.5.20 okamžitě plyne, že polynom f stupně n je identicky nulový, právě když je triviální, tj. právě když jeho koeficienty jsou samé nuly.

Všimněme si, že v důkazech lemmat 3.5.19 a 3.5.20 jsme se obešli bez axiomů R11–R16. Obě lemmata tedy platí i pro teorii komutativních těles. Lze tvrdit ještě trochu víc: z axiomů teorie komutativních těles jsme nepotřebovali axiom R8 o existenci inverzních čísel, použili jsme jen jeho slabší důsledek vyjádřený tvrzením (d) lemmatu 3.2.14.

Je-li f polynom stupně $n \geq 1$ s koeficienty $z_0,..,z_n$, definujme jeho *derivaci* f' jako polynom stupně $n-1$ s koeficienty $\overline{n} \cdot z_0$, $\overline{n-1} \cdot z_1$ až z_{n-1}. Je-li f polynom stupně 0 s (jediným) koeficientem z_0, definujme jeho derivaci f' jako polynom stupně 0 s koeficientem 0. V definici derivace jsme se tedy obešli bez pojmu limita, což je možné díky tomu, že neuvažujeme jiné funkce než polynomy. Uvnitř teorie RCF se na derivaci díváme nikoliv jako na jedinou operaci, ale jako na nekonečně mnoho operací: derivace polynomů stupně n je operace z $(n+1)$-tic do $\max\{1,n\}$-tic čísel. Derivace vyšších řádů definujeme jako obvykle: $f^{(0)} = f$, $f^{(k+1)} = (f^{(k)})'$. Polynom $f^{(k)}$ je k-tou derivací polynomu f. Má-li f stupeň n, pak $f^{(k)}$ je polynom stupně $n-k$ pro $k \leq n$, a $f^{(k)}$ je identicky nulový polynom pro $k > n$.

V následujících pěti lemmatech a jejich důkazech se dopouštíme nedůslednosti a formalizovatelné podmínky a důkazy nevyznačujeme bezpatkovým písmem. Předpokládáme, že čtenář dovede odlišit, co se děje na metamatematické úrovni a co uvnitř teorie RCF. Ostatně na metamatematické úrovni se mluví vždy pouze o stupních polynomů. K pečlivějšímu odlišení metamatematické a formální úrovně se vrátíme za důkazem lemmatu 3.5.25, až budeme mluvit o eliminaci kvantifikátorů pro teorii RCF.

Lemma 3.5.21 *Známá pravidla pro počítání derivací součtu a součinu*

$$(f+g)' = f' + g' \quad a \quad (f \cdot g)' = f' \cdot g + f \cdot g'$$

lze pro polynomy dokázat v teorii RCF.

Důkaz Obě rovnosti lze ověřit počítáním se sumami podobně jako v důkazu lemmatu 3.5.19 a předtím lemmatu 3.2.15. QED

Lemma 3.5.22 *Mezi každými dvěma kořeny libovolného polynomu f stupně n leží nějaký kořen polynomu f'.*

Důkaz Nechť stupeň n je dán, uvažujme v teorii RCF. Nechť pro čísla a a b platí $a < b$ a $f(a) = f(b) = 0$. Můžeme předpokládat, že f není identicky nulový. Dále předpokládejme, že v intervalu $(\!(a, b)\!)$ není žádný další kořen polynomu f. Jinak bychom užili fakt, že všech kořenů je nejvýše n, a od dvojice a, b bychom přešli k dvojici a_0, b_0 sousedních kořenů takových, že $a \leq a_0 < b_0 \leq b$.

Lemma 3.5.19 tvrdí, že z polynomu f můžeme vytknout činitele $(x - a)$ a $(x - b)$. Vytýkání lze opakovat, dokud a nebo b je kořenem zbývajícího polynomu. Existuje tedy polynom g takový, že pro každé x platí $f(x) = (x - a)^m(x - b)^r g(x)$. Přitom $m, r \geq 1$ a g nemá žádné kořeny v intervalu $[\![a, b]\!]$. Užijme lemma 3.5.21 a spočítejme derivaci f' polynomu f:

$$\begin{aligned} f'(x) = \overline{m}(x-a)^{m-1}(x-b)^r g(x) + \overline{r}(x-a)^m(x-b)^{r-1}g(x) + \\ + (x-a)^m(x-b)^r g'(x) = \\ = (x-a)^{m-1}(x-b)^{r-1}[\overline{m}(x-b)g(x) + \overline{r}(x-a)g(x) + (x-a)(x-b)g'(x)]. \end{aligned}$$

Označme $h(x)$ polynom v hranaté závorce. Dosazení a a b dává $h(a) = \overline{m}(a-b)g(a)$ a $h(b) = \overline{r}(b-a)g(b)$. Čísla $g(a)$ a $g(b)$ jsou nenulová. Kdyby čísla $g(a)$ a $g(b)$ měla různá znaménka, dle axiomu R16 by g měl nějaký kořen v $(\!(a, b)\!)$ a tento kořen by byl zároveň kořenem polynomu f. Čísla $g(a)$ a $g(b)$ mají tedy stejná znaménka. Čísla $a - b$ a $b - a$ mají ovšem různá znaménka. Tedy $h(a) \cdot h(b) < 0$. Dle axiomu R16 polynom h má nějaký kořen v $(\!(a, b)\!)$. Tento kořen je zároveň kořenem polynomu f'. QED

Lemma 3.5.23 *Když $a < b$ a f je polynom, pak existuje číslo $\xi \in (\!(a, b)\!)$ takové, že $f(b) - f(a) = f'(\xi)(b - a)$.*

Důkaz Nechť a, b a f jsou dány. Vezměme číslo ε takové, že $\varepsilon(b-a) = 1$. Uvažujme polynom g definovaný předpisem

$$g(x) = f(x) - f(a) - \varepsilon(f(b) - f(a))(x - a).$$

Platí $g'(x) = f'(x) - \varepsilon(f(b) - f(a))$ a dále $g(a) = 0$ a $g(b) = 0$. Dle lemmatu 3.5.22 existuje číslo $\xi \in (\!(a, b)\!)$ takové, že $g'(\xi) = 0$. Tedy $0 = f'(\xi) - \varepsilon(f(b) - f(a))$, dále $\varepsilon(f(b) - f(a)) = f'(\xi)$, a tedy opravdu $f(b) - f(a) = f'(\xi)(b - a)$. QED

Lemma 3.5.22 je známo jako *Rolleova věta*. Důkaz, který jsme uvedli, vznikl přizpůsobením důkazu *Sturmovy věty*, který je uveden v knize [97]. Sturmova věta umožňuje určit počet kořenů polynomu f stupně n v intervalu $(\!(a, b)\!)$, známe-li znaménka čísel $f^{(i)}(a)$ a $f^{(i)}(b)$, kde $0 \leq i \leq n$. Lemma 3.5.23 je *věta o střední hodnotě*. Její důkaz lze označit jako „obvyklý“.

Definujme v teorii RCF *pravé* a *levé okolí* čísla (bodu). Pravé okolí bodu a je libovolný interval $(\!(a, b)\!)$, kde $a < b$. Pravé okolí „nevlastního bodu“ $-\infty$ je libovolný

interval tvaru $(\!(-\infty, b)\!)$, tj. množina $\{\, x\,;\, x < b\,\}$. Analogicky se definuje levé okolí bodu a levé okolí nevlastního bodu $+\infty$. Dále definujme *funkci signum*: $\mathrm{sgn}(x) = 1$ pro $x > 0$, $\mathrm{sgn}(x) = -1$ pro $x < 0$, $\mathrm{sgn}(0) = 0$. Místo hodnot 1, -1 a 0 funkce signum budeme někdy psát $+$, $-$ a 0.

Axiom R16 tvrdí, že je-li f polynom, pak mezi každými dvěma body, ve kterých má funkce $\mathrm{sgn}(f(x))$ hodnoty $+$ a $-$, existuje nějaký další bod, ve kterém má funkce $\mathrm{sgn}(f(x))$ hodnotu 0. Je-li tedy číslo a libovolné a $b > a$ je nejmenší kořen polynomu f větší než a, buď všechny hodnoty funkce $\mathrm{sgn}(f(x))$ v intervalu $(\!(a, b)\!)$ jsou $+$, nebo jsou všechny $-$. Z toho dále plyne, že je-li f libovolný polynom a a libovolný bod, funkce $\mathrm{sgn}(f(x))$ je konstantní v (jistém) pravém okolí bodu a: buď je f identicky nulový, a v tom případě všechny hodnoty funkce $\mathrm{sgn}(f(x))$ jsou nuly, nebo $\mathrm{sgn}(f(x))$ má tutéž hodnotu $+$ až do nejbližšího většího kořenu (nebo do $+\infty$, neexistují-li kořeny větší než a), nebo $\mathrm{sgn}(f(x))$ má tutéž hodnotu $-$ až do nejbližšího většího kořenu (nebo do $+\infty$). Je-li $f(a) \neq 0$, pak ovšem $\mathrm{sgn}(f(x))$ má v pravém okolí bodu a hodnotu $\mathrm{sgn}(f(a))$. Následující lemma umožňuje určit hodnotu funkce $\mathrm{sgn}(f(x))$ v pravém okolí bodu a bez ohledu na to, zda $f(a) = 0$. Lemma 3.5.25 má podobný účel, umožňuje určit hodnotu funkce $\mathrm{sgn}(f(x))$ v okolí nevlastních bodů $-\infty$ a $+\infty$.

Lemma 3.5.24 *Nechť a je číslo a nechť f je polynom stupně n. Když všechna čísla $f(a), f'(a), \ldots, f^{(n)}(a)$ jsou nuly, pak f je identicky nulový. Když první nenulové číslo v posloupnosti $f(a), f'(a), \ldots, f^{(n)}(a)$ je kladné (záporné), pak f je kladný (resp. záporný) v pravém okolí bodu a.*

Důkaz Označme $z_0, \ldots, z_n$ koeficienty polynomu f a spočítejme f' a f'':

$$f'(x) = \overline{n} z_0 x^{n-1} + \overline{n-1} z_1 x^{n-2} + \ldots + z_{n-1},$$
$$f''(x) = \overline{n(n-1)} z_0 x^{n-2} + \overline{(n-1)(n-2)} z_1 x^{n-3} + \ldots + \overline{2} z_{n-2}.$$

Obecně pro k-tou derivaci platí

$$f^{(k)}(x) = \sum_{i=0}^{n-k} \overline{(n-i)!/(n-k)!}\, z_i x^{n-k-i}.$$

Dosadíme-li $x := a$, snadno zjistíme, že všechna čísla $f^{(k)}(a)$ mohou být najednou nulová jen v případě, kdy všechny koeficienty $z_0, \ldots, z_n$ jsou nuly: $f^{(n)}(a) = \overline{n!}\, z_0$, a platí-li $f^{(n)}(a) = 0$, pak i $z_0 = 0$, dále $f^{(n-1)}(a) = \overline{n!/1!}\, z_0 a + \overline{(n-1)!}\, z_1$, a platí-li $f^{(n)}(a) = 0$ i $f^{(n-1)}(a) = 0$, pak i $z_0 = 0$ a $z_1 = 0$ atd.

Nechť $0 \leq k \leq n$, nechť $f(a) = f'(a) = \ldots = f^{(k-1)}(a) = 0$, nechť $f^{(k)}(a) > 0$. Zvolme b takové, že pro každé $x \in (\!(a, b)\!)$ je $f^{(k)}(x) > 0$. Platí-li $k = 0$, jsme hotovi, f je kladný v $(\!(a, b)\!)$. Jinak vezměme v úvahu toto pomocné tvrzení: *je-li g polynom takový, že $g(a) = 0$ a jeho derivace g' je kladná v $(\!(a, b)\!)$, pak g je kladný v $(\!(a, b)\!)$.* Skutečně, pokud pro nějaké $x \in (\!(a, b)\!)$ platí $g(x) < 0$, pak dle 3.5.23 pro nějaké $\xi \in (\!(a, x)\!)$ platí $g(x) - g(a) = g'(\xi)(x - a)$, a z $g(a) = 0$, $g(x) < 0$ a $x - a > 0$

plyne $g'(\xi) < 0$. Užijeme-li toto pomocné tvrzení na $f^{(k-1)}$, $f^{(k-2)}$ až f v roli g, dostaneme, že f je kladný v $(\!(a, b)\!)$.

Důkaz tvrzení, že je-li první nenulové číslo v posloupnosti $f(a), f'(a), .., f^{(n)}(a)$ záporné, pak f je záporný v pravém okolí bodu a, je naprosto analogický. QED

Lemma 3.5.25 *Nechť f je netriviální polynom stupně n s koeficienty $z_0, .., z_n$, nechť z_i je první koeficient v posloupnosti $z_0, .., z_n$, který je nenulový. Pak existuje $w > 0$ takové, že pro všechna $x > w$ platí* $\mathrm{sgn}(f(x)) = \mathrm{sgn}(z_i)$ *a pro všechna $x < -w$ platí* $\mathrm{sgn}(f(x)) = \mathrm{sgn}((-1)^n z_i)$.

Důkaz Definujme pro účely tohoto důkazu a případně některých cvičení *absolutní hodnotu*: $|x|$ je ono z čísel x a $-x$, které je nezáporné. Snadno lze ověřit, že (dokazatelně v teorii uspořádaných těles) platí obvyklá pravidla pro počítání s absolutními hodnotami: $|x \cdot y| = |x| \cdot |y|$ a $|x + y| \leq |x| + |y|$.

Nechť jsou dány koeficienty $z_0, .., z_n$ netriviálního polynomu f. Můžeme předpokládat, že první nenulový koeficient je z_0. Dále předpokládejme například, že n je liché a že $z_0 > 0$. Tedy z_0 je kladné a $(-1)^n z_0$ je záporné. Máme najít $w > 0$ takové, že pro všechna $x > w$ platí $z_0 x^n > -(z_1 x^{n-1} + .. + z_n)$ a pro všechna $x < -w$ platí $z_0 x^n < -(z_1 x^{n-1} + .. + z_n)$. Protože pro $x < -w$ je $|z_0 x^n| = -z_0 x^n$, stačí zdůvodnit najednou, že $|z_1 x^{n-1} + .. + z_n| < z_0 |x|^n$. Pro $x \geq 1$ platí $|z_i x^i| \leq |z_i x^{n-1}|$ pro každé $i \leq n - 1$, tedy

$$|z_1 x^{n-1} + .. + z_n| \leq (|z_1| + .. + |z_n|) \cdot |x|^{n-1}. \qquad (*)$$

Označme ε číslo inverzní k z_0. Platí $\varepsilon > 0$ a $\varepsilon \cdot z_0 = 1$. Je-li $|x| > \varepsilon \cdot (|z_1| + .. + |z_n|)$, pak

$$\varepsilon \cdot z_0 \cdot (|z_1| + .. + |z_n|) \cdot |x|^{n-1} < z_0 \cdot |x|^n. \qquad (**)$$

Z $(*)$ a $(**)$ plyne, že za w můžeme vzít číslo $\max\{1, \varepsilon \cdot (|z_1| + .. + |z_n|)\}$, neboť je-li $|x| > w$, opravdu platí $|z_1 x^{n-1} + .. + z_n| < z_0 \cdot |x|^n$. QED

Tím máme pohromadě všechna tvrzení o dokazatelnosti v teorii RCF, která budeme potřebovat, a můžeme se vrátit k logice, tj. definovat konzervativní rozšíření teorie RCF a uvažovat o eliminaci kvantifikátorů.

Nechť $1 \leq i \leq n$. V teorii RCF definujme, že $\mathrm{NR}_{n,i}(z_0, .., z_n)$, jestliže polynom $z_0 x^n + .. + z_n$ není identicky nulový a má alespoň i navzájem různých kořenů. Symbol $\mathrm{NR}_{n,i}$ je $(n+1)$-ární predikátový symbol. Dále v teorii RCF definujme, že číslo $\xi_{n,i}(z_0, .., z_n)$ je i-tý nejmenší kořen polynomu $f(x) = z_0 x^n + .. + z_n$, pokud $\mathrm{NR}_{n,i}(z_0, .., z_n)$, a $\xi_{n,i}(z_0, .., z_n)$ je nula v ostatních případech (tj. kdy f je identicky nulový, nebo má méně než i kořenů). Symbol $\xi_{n,i}$ je $(n+1)$-ární funkční symbol. Označme L_{RCF} jazyk $\{+, \cdot, 0, 1, <, -\}$ (tj. počítejme i unární symbol „$-$“ k základním symbolům teorie RCF) a označme L^+_{RCF} jazyk vzniklý přidáním všech symbolů $\mathrm{NR}_{n,i}$ a $\xi_{n,i}$, kde $1 \leq i \leq n$, k jazyku L_{RCF}. Označme RCF^+ konzervativní rozšíření teorie RCF o právě uvedené definice symbolů $\mathrm{NR}_{n,i}$ a $\xi_{n,i}$.

Příklad 3.5.26 Je-li $z > 0$, pak $\xi_{2,2}(1, 0, -z)$ je to, co se obvykle zapisuje jako $\sqrt{z}$. Je-li $z \leq 0$, pak v teorii RCF víme, že $\neg \mathrm{NR}_{2,2}(1, 0, -z)$ a $\xi_{2,2}(1, 0, -z) = 0$.

Termům obsahujícím symboly $\xi_{n,i}$ říkejme *algebraické termy*. *Atomická algebraická formule* je každá atomická formule jazyka L_{RCF} a dále každá formule jazyka L^{+}_{RCF}, která má některý z následujících tří tvarů:

- $c_0(\underline{y}) \cdot \xi^m_{n,i}(a_0(\underline{y}), \ldots, a_n(\underline{y})) + c_1(\underline{y}) \cdot \xi^{m-1}_{n,i}(a_0(\underline{y}), \ldots, a_n(\underline{y})) + \ldots + c_m(\underline{y}) \bowtie 0$,
- $\xi_{n,i}(a_0(\underline{y}), \ldots, a_n(\underline{y})) < \xi_{m,k}(b_0(\underline{y}), \ldots, b_m(\underline{y}))$,
- $\mathrm{NR}_{n,i}(a_0(\underline{y}), \ldots, a_n(\underline{y}))$,

kde $\bowtie$ je jeden ze symbolů $<$, $=$ nebo $>$ a $a_i(\underline{y})$, $b_i(\underline{y})$ a $c_i(\underline{y})$ jsou termy, které jsou sestaveny z proměnných $y_1, \ldots, y_q$ pomocí symbolů $+, \cdot, 0, 1, -$. *Algebraická formule* je formule sestavená z atomických algebraických formulí pomocí logických spojek. Dále budeme pro stručnost většinou vypouštět $\underline{y}$. Protože $(n+1)$-tici argumentů symbolu $\mathrm{NR}_{n,i}$ a $\xi_{n,i}$ vždy interpretujeme jako koeficienty polynomu, budeme psát například f místo $a_0, \ldots, a_n$. Atomické algebraické formule jsou tedy formule tvaru $g(\xi_{n,i}(f)) \bowtie 0$, nebo $\xi_{n,i}(f) < \xi_{m,k}(g)$, nebo $\mathrm{NR}_{n,i}(f)$, kde f a g jsou polynomy, jejichž koeficienty jsou termy jazyka L_{RCF}, a dále všechny atomické formule jazyka L_{RCF}.

Definujme *řád* algebraických formulí: řád atomické formule neobsahující symboly $\mathrm{NR}_{n,i}$ a $\xi_{n,i}$ je 0, řád formulí $g(\xi_{n,i}(f)) \bowtie 0$ a $\mathrm{NR}_{n,i}(f)$ je n, řád formule $\xi_{n,i}(f) < \xi_{m,k}(g)$ je $\max\{n, m\}$, řád algebraické formule je maximum řádů všech jejích atomických podformulí.

Příklad 3.5.27 Formule $\xi_{n,i}(f) \cdot \xi_{m,k}(g) > 0$ ani formule tvaru $\mathrm{NR}_{m,k}(\xi_{n,i}(f), \ldots)$ není algebraickou formulí. Jsou-li f a g polynomy, jejichž koeficienty neobsahují algebraické termy, a má-li f stupeň n, pak formule polynom g je pozitivní v pravém okolí bodu $\xi_{n,i}(f)$ je podle lemmatu 3.5.24 algebraickou formulí řádu n.

Term tvaru $\xi_{n,i}(\ldots)$ se v algebraické formuli nikdy nemůže vyskytnout uvnitř termu tvaru $\xi_{m,k}(\ldots)$ ani uvnitř atomické formule tvaru $\mathrm{NR}_{m,k}(\ldots)$. Algebraické formule neobsahují kvantifikátory. Každá atomická podformule algebraické formule obsahuje nejvýše jeden term tvaru $\xi_{n,i}(f)$ (který se v ní může vyskytovat vícekrát) s výjimkou formule tvaru $\xi_{n,i}(f) < \xi_{m,k}(g)$, která může obsahovat dva různé algebraické termy.

Lemma 3.5.28 *Každá algebraická formule A řádu $n \geq 1$ je ekvivalentní s algebraickou formulí B řádu nejvýše n takovou, že v každé atomické podformuli formule B tvaru $g(\xi_{n,i}(f)) \bowtie 0$ má polynom g nižší stupeň než polynom f.*

Důkaz Nechť $g(\xi_{n,i}(f)) > 0$ je některá podformule formule A taková, že pro stupeň m polynomu g platí $m \geq n$. Nechť ax^m je nejvyšší člen polynomu g a nechť bx^n je nejvyšší člen polynomu f. Polynom $b^2 g(x) - abx^{m-n} f(x)$ je polynom stupně m, jehož nejvyšší koeficient (tj. koeficient u x^m) je 0. Označme $g_1(x)$

polynom stupně $m-1$ vzniklý odstraněním onoho nejvyššího (nulového) členu z polynomu $b^2g(x) - abx^{m-n}f(x)$. Označme dále $f_1(x)$ polynom stupně $n-1$ vzniklý odstraněním nejvyššího (nulového) členu z polynomu $f(x) - bx^n$, tj. odstraněním nejvyššího členu z polynomu $f(x)$. Z předpokladu $b \neq 0$ v teorii RCF vyplývá ekvivalence $g(\xi) > 0 \equiv b^2g(\xi) > 0$. Dále z předpokladu číslo ξ je kořenem polynomu f v teorii RCF vyplývá ekvivalence $b^2g(\xi) > 0 \equiv g_1(\xi) > 0$. Podformuli $g(\xi_{n,i}(f)) > 0$ formule A můžeme tedy nahradit s ní ekvivalentní formulí

$$\begin{aligned}(\neg \mathrm{NR}_{n,i}(f) \ \&\ g(0) > 0) \ \vee \\ \vee\ (\mathrm{NR}_{n,i}(f) \ \&\ b = 0 \ \&\ g(\xi_{n-1,i}(f_1)) > 0) \\ \vee\ (\mathrm{NR}_{n,i}(f) \ \&\ b \neq 0 \ \&\ g_1(\xi_{n,i}(f)) > 0).\end{aligned}$$

Touto záměnou se nezvýšil řád formule, neboť formule $\mathrm{NR}_{n,i}(f)$ má řád n a formule $g(\xi_{n-1,i}(f_1))$ má řád $n-1$. Bylo-li $m = n$, snížil se počet nežádoucích formulí, tj. formulí tvaru $g(\xi_{n,i}(..)) \bowtie 0$, které mají maximální možný řád n a v nichž polynom g má stupeň $m \geq n$. Bylo-li $m > n$, počet nežádoucích formulí zůstal zachován, ale v jedné se snížil stupeň polynomu. Opakováním tohoto postupu dospějeme k požadované formuli. Stejně se uvažuje, když $\bowtie$ je jeden ze symbolů $>$ a $=$. QED

Nechť $\alpha < \beta$ jsou dva sousední kořeny derivace f' polynomu f. Užitím axiomu R16 a lemmat 3.5.22 a 3.5.23 lze snadno ověřit, že (i) je-li $f(\alpha) = 0$, pak α je jediný kořen polynomu f v $[\![\alpha, \beta]\!]$, (ii) je-li $f(\beta) = 0$, pak β je jediný kořen polynomu f v $[\![\alpha, \beta]\!]$, (iii) mají-li čísla $f(\alpha)$ a $f(\beta)$ opačná nenulová znaménka, pak f má v $(\!(\alpha, \beta)\!)$ kořen, který je jediným kořenem v $[\![\alpha, \beta]\!]$, a (iv) mají-li čísla $f(\alpha)$ a $f(\beta)$ totéž nenulové znaménko, pak f nemá žádný kořen v $[\![\alpha, \beta]\!]$. Například tvrzení (iv) se zdůvodní následovně. Nechť $f(\alpha)$ a $f(\beta)$ mají totéž nenulové znaménko a nechť $x \in (\!(\alpha, \beta)\!)$ je kořen polynomu f. Pak dle 3.5.23 existují čísla $\eta_1 \in (\!(\alpha, x)\!)$ a $\eta_2 \in (\!(x, \beta)\!)$, ve kterých má f' různá a nenulová znaménka, a v $(\!(\eta_1, \eta_2)\!)$ je nějaký kořen polynomu f', což je spor s předpokladem, že α a β jsou sousední kořeny polynomu f'.

Když β je největší kořen polynomu f', pak f má v intervalu $[\![\beta, +\infty)\!)$ nejvýše jeden kořen, a má-li $f(\beta)$ totéž znaménko, jako mají všechna čísla $f(x)$ pro dost velká x (ve smyslu lemmatu 3.5.25), pak f nemá v $[\![\beta, +\infty)\!)$ žádný kořen. Analogická tvrzení lze odvodit o kořenech polynomu f vlevo od nejmenšího kořenu polynomu f'.

Můžeme tedy shrnout, že mezi každými dvěma kořeny polynomu f' a také před prvním a za posledním je vždy nejvýše jeden kořen polynomu f. Odpověď na otázku, zda je právě jeden, je určena znaménky polynomu f v kořenech jeho derivace f' a v okolí nevlastních bodů $-\infty$ a $+\infty$.

Lemma 3.5.29 *Každá formule* $\mathrm{NR}_{n,i}(a_0, .., a_n)$*, kde* $1 \leq i \leq n$*, je ekvivalentní s algebraickou formulí řádu menšího než* n*.*

Důkaz Je-li $n = 1$, pak formule $\mathrm{NR}_{1,1}(a_0, a_1)$, tj. formule polynom $a_0x + a_1$ je netriviální a má alespoň jeden kořen, je ekvivalentní s formulí $a_0 \neq 0$, což je alge-

$-\infty$	$+$	$-$	$*$	$*$	$+$	$-$	$+$	$-$	$+$	$-$
$\xi_{2,1}(f')$	$-$	$+$	0	0	$-$	$+$	$-$	$+$	$*$	$*$
$\xi_{2,2}(f')$			$+$	$-$	0	0	$+$	$-$	$-$	$+$
$+\infty$	$+$	$-$	$-$	$+$	$*$	$*$	$*$	$*$	$+$	$-$

Obrázek 3.5.1: Určení počtu kořenů polynomu

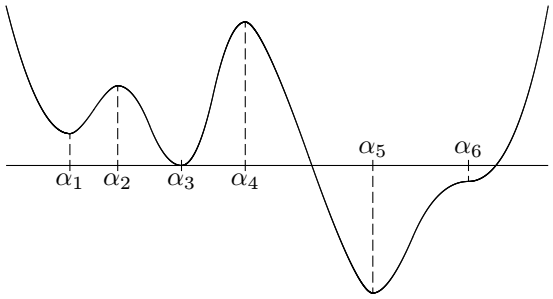
braická formule řádu 0. Předpokládejme tedy nadále, že $n > 1$. Označme f polynom s koeficienty $a_0, .., a_n$. Jeho derivace f' má koeficienty $\overline{n}a_0, \overline{n-1}a_1, .., a_{n-1}$. Máme za úkol vyjádřit podmínku $\mathrm{NR}_{n,i}(f)$ bez užití symbolů $\mathrm{NR}_{m,k}(..)$ a $\xi_{m,k}(..)$, kde $m \geq n$.

Utvořme tabulku s $n+1$ řádky označenými $-\infty, \xi_{n-1,1}(f'), .., \xi_{n-1,n-1}(f'), +\infty$, ve které sloupce odpovídají všem příznivým kombinacím znamének polynomu f v bodech $-\infty, \xi_{n-1,1}(f'), .., \xi_{n-1,n-1}(f'), +\infty$. Příznivá kombinace je taková, při které f nutně má alespoň i kořenů. Například pro $n = 3$ a $i = 2$ je tato tabulka uvedena na obrázku 3.5.1. Hvězdičky označují hodnoty, na kterých nezáleží. První dva sloupce odpovídají případům, kdy f' má jeden kořen (pole příslušná ke $\xi_{2,2}(f')$ jsou prázdná), třetí až šestý sloupec odpovídají případům, kdy f' má dva kořeny, z nichž jeden je zároveň kořenem polynomu f, a sedmý až desátý sloupec odpovídají případům, kdy žádný ze dvou kořenů polynom f' není současně kořenem polynomu f. V našem případě, a obecně kdykoliv $i \geq 2$, žádné příznivé kombinace neodpovídají případu, kdy f' nemá kořeny, ani případu, kdy f' má jen jeden kořen, který je zároveň kořenem polynomu f. Tehdy má totiž f nejvýše jeden kořen. Při konstrukci tabulky využíváme fakt, že v posloupnosti znamének $\mathrm{sgn}(f(-\infty))$, $\mathrm{sgn}\, f(\xi_{n-1,1}(f'))$ až $\mathrm{sgn}\, f(\xi_{n-1,n-1}(f'))$ a $\mathrm{sgn}(f(+\infty))$ nemůže být nula na začátku ani na konci a nemohou se v ní vyskytnout dvě nuly těsně za sebou.

Máme-li tabulku, snadno sestavíme z atomických formulí jazyka L_{RCF} a z formulí tvaru $\mathrm{NR}_{n-1,k}(f')$ a $f(\xi_{n-1,k}(f')) \bowtie 0$, kde $1 \leq k \leq n-1$, algebraickou formuli řádu $n-1$ ekvivalentní s původní formulí $\mathrm{NR}_{n,i}(f)$. V našem příkladu s $n = 3$ a $i = 2$ je to formule

$$
\begin{aligned}
&(\mathrm{NR}_{2,1}(f') \ \&\ \neg\mathrm{NR}_{2,2}(f') \ \&\ f(\xi_{2,1}(f')) \neq 0 \ \& \\
&\qquad \& \ \mathrm{sgn}\, f(-\infty) \neq \mathrm{sgn}\, f(\xi_{2,1}(f')) \ \&\ \mathrm{sgn}\, f(\xi_{2,1}(f')) \neq \mathrm{sgn}\, f(+\infty)) \ \vee \\
&\quad \vee \ (\mathrm{NR}_{2,2}(f') \ \&\ f(\xi_{2,1}(f')) = 0 \ \&\ \mathrm{sgn}\, f(\xi_{2,2}(f')) \neq \mathrm{sgn}\, f(+\infty)) \\
&\quad \vee \ (\mathrm{NR}_{2,2}(f') \ \&\ f(\xi_{2,2}(f')) = 0 \ \&\ \mathrm{sgn}\, f(-\infty) \neq \mathrm{sgn}\, f(\xi_{2,1}(f'))) \\
&\quad \vee \ (\ldots \text{ podobně pro sedmý až desátý sloupec tabulky } \ldots).
\end{aligned}
$$

Zápis jsme trochu zkrátili použitím funkce sgn. Například v prvním disjunktu, kde se probírá případ, kdy f' má právě jeden kořen, zápis $\mathrm{sgn}\, f(\xi_{2,1}(f')) \neq \mathrm{sgn}\, f(+\infty)$ značí disjunkci buď $f(\xi_{2,1}(f')) > 0$ a polynom f je záporný v levém okolí bodu $+\infty$, nebo $f(\xi_{2,1}(f')) < 0$ a polynom f je kladný v levém okolí bodu $+\infty$. Formule poly-



Obrázek 3.5.2: Kořeny derivace a průběh polynomu

nom f je takový a takový v levém okolí bodu $+\infty$ je algebraickou formulí řádu 0 díky lemmatu 3.5.25. QED

Porovnejme statický popis všech příznivých případů, který vyjadřuje formule sestrojená v důkazu lemmatu 3.5.29, s následujícím „algoritmem“ pro určení počtu kořenů polynomu f:

> Urči počet r kořenů polynomu f'. Označ tyto kořeny $\alpha_1, .., \alpha_r$. Dále polož $a_0 = -\infty$, $a_{r+1} = +\infty$. Urči počet nul plus počet změn v posloupnosti $\operatorname{sgn} f(\alpha_0)$ až $\operatorname{sgn} f(\alpha_{r+1})$, přičemž za změnu se považuje pouze změna z „+“ na „−“ nebo naopak. Výsledek je počet kořenů polynomu f.

Například derivace polynomu f z obrázku 3.5.2 má šest kořenů $\alpha_1, .., \alpha_6$ a posloupnost znamének polynomu f v bodech $\alpha_0, .., \alpha_7$ je posloupnost $+, +, +, 0, +, -, -, +$, ve které je jedna nula a dvě změny. Náš „algoritmus“ tedy pro polynom z obrázku 3.5.2 určil správně, že má tři kořeny. Uvozovky píšeme proto, že o skutečný algoritmus tu ovšem nejde: nepracuje se s konečnými posloupnostmi symbolů, ale s abstraktními objekty formální teorie. Tvrdíme ale, že takovýto pseudoalgoritmus je stejně dobrý jako formule, kterou jsme sestrojili v důkazu lemmatu 3.5.29: z návodu, jak převést platnost podmínky $\mathrm{NR}_{n,i}(f)$ na platnost podmínek tvaru $\mathrm{NR}_{n-1,k}(..)$ a $g(\xi_{n-1,k}(..)) \bowtie 0$, lze sestrojit formuli, která podmínku $\mathrm{NR}_{n,i}(f)$ vyjádří jako booleovskou kombinaci podmínek tvaru $\mathrm{NR}_{n-1,k}(..)$ a $g(\xi_{n-1,k}(..)) \bowtie 0$.

V důkazu následujícího lemmatu se tedy spokojíme s uvedením stručného a názorného pseudoalgoritmu a spolehneme se na to, že čtenář si za ním umí představit algebraickou formuli řádu $n - 1$.

Lemma 3.5.30 *Každá algebraická formule je ekvivalentní s jistou otevřenou formulí v jazyce* L_{RCF}.

Důkaz Dokažme indukcí podle n, že každá algebraická formule řádu n je ekvivalentní s jistou otevřenou formulí v jazyce L_{RCF}. Pro $n = 0$ je to pravda, algebraické formule řádu 0 jsou otevřenými formulemi v jazyce L_{RCF}. Zbývá tedy dokázat, že každá algebraická formule A řádu n je ekvivalentní s jistou algebraickou formulí B

řádu menšího než n. Toto tvrzení dokažme opět indukcí, a to podle počtu atomických algebraických podformulí formule A, jejichž řád je n. Stačí tedy dokázat, že každá algebraická formule A řádu $n \geq 1$ je ekvivalentní s jistou algebraickou formulí B, jejíž řád je nejvýše n a která má méně atomických algebraických podformulí řádu n, než má formule A. Přitom nevadí, má-li B více atomických podformulí řádů menších než n.

Nechť tedy A je dána a nechť D je některá její atomická podformule řádu n. Tvrdíme, že formuli D lze nahradit s ní ekvivalentní formulí řádu menšího než n. Formule D má jeden z tvarů $\mathrm{NR}_{n,i}(f)$, nebo $g(\xi_{n,i}(f)) \bowtie 0$, nebo $\xi_{n,i}(f) \bowtie \xi_{m,k}(g)$, kde $0 < m \leq n$. Je-li D tvaru $\mathrm{NR}_{n,i}(f)$, jsme hotovi, D je ekvivalentní s algebraickou formulí řádu menšího než n díky lemmatu 3.5.29.

Uvažujme tedy případ, kdy D má tvar $g(\xi_{n,i}(f)) \bowtie 0$. Vzhledem k lemmatu 3.5.28 můžeme předpokládat, že g má stupeň n' nižší než stupeň n polynomu f. Má-li g stupeň 0, formule $g(\xi_{n,i}(f)) \bowtie 0$ je formule $a_0 \bowtie 0$, kde a_0 je jediný koeficient polynomu g. Předpokládejme tedy, že g má nenulový stupeň. Jak jsme se dohodli, stačí napsat pseudoalgoritmus, který určí pravdivostní hodnotu formule $g(\xi_{n,i}(f)) \bowtie 0$, tj. který „vypočítá“ hodnotu $\operatorname{sgn} g(\xi_{n,i}(f))$ pomocí „podprogramů“, které počítají pravdivostní hodnoty algebraických formulí řádů menších než n. Pišme ξ místo $\xi_{n,i}(f)$.

> Urči kořeny $\alpha_1, .., \alpha_r$ polynomu f'. Polož $a_0 = -\infty$, $\alpha_{r+1} = +\infty$. Zjisti znaménka čísel $f(\alpha_0), .., f(\alpha_r)$. Nalezni $j \in \{0, .., r\}$ takové, že počet nul plus počet změn v posloupnosti $\operatorname{sgn} f(\alpha_0)$ až $\operatorname{sgn} f(\alpha_{j+1})$ je i a navíc platí $\operatorname{sgn} f(\alpha_{j+1}) \neq 0$. Neexistuje-li takové j, pak $\neg\mathrm{NR}_{n,i}(f)$ a $\operatorname{sgn} g(\xi) = \operatorname{sgn} g(0)$. Jinak $\mathrm{NR}_{n,i}(f)$.

Tím je znovu určena platnost podmínky $\mathrm{NR}_{n,i}(f)$, postup byl téměř stejný jako v lemmatu 3.5.29. Dále je určena hodnota $\operatorname{sgn} g(\xi)$ v případě, kdy $\neg\mathrm{NR}_{n,i}(f)$. Zbývající část pseudoalgoritmu pracuje za předpokladu, že $\mathrm{NR}_{n,i}(f)$.

> Protože $\mathrm{NR}_{n,i}(f)$, číslo ξ je i-tým kořenem polynomu f a zároveň je jediným kořenem polynomu f v intervalu $[\![\alpha_j, \alpha_{j+1})\!]$. Pokud $f(\alpha_j) = 0$ (což nemůže nastat, je-li $j = 0$), platí $\xi = \alpha_j$ a $\operatorname{sgn} g(\xi) = \operatorname{sgn} g(\alpha_j)$.
>
> Jinak platí $\alpha_j < \xi$. Číslo ξ je ovšem stále jediným kořenem polynomu f v intervalu $[\![\alpha_j, \alpha_{j+1})\!]$.
>
> Urči kořeny $\beta_1, .., \beta_l$ polynomu g. Polož $\beta_0 = -\infty$. Uvažuj všechna čísla $\beta \in \{b_0, .., \beta_l\}$, pro která platí některá z podmínek
>
> - $\beta \leq \alpha_j$,
> - $\beta \in (\!(\alpha_j, \alpha_{j+1})\!)$ a $\operatorname{sgn} f(\beta) = \operatorname{sgn} f(\alpha_j)$,
> - $\beta \in (\!(\alpha_j, \alpha_{j+1})\!)$ a $f(\beta) = 0$.
>
> Nechť β_k je maximální takové β. Splňuje-li β_k poslední podmínku, tj. platí-li $\beta_k \in (\!(\alpha_j, \alpha_{j+1})\!)$ a $f(\beta_k) = 0$, musí být $\beta_k = \xi$. V tom případě $\operatorname{sgn}(g(\xi)) = 0$. Jinak platí $\beta_k < \xi$ a β_k je buď maximálním kořenem polynomu g v intervalu $(\!(-\infty, \xi]\!]$, nebo $k = 0$, $\beta_k = -\infty$ a g nemá kořeny v $(\!(-\infty, \xi]\!]$. V obou případech

se $\operatorname{sgn} g(\xi)$ pozná podle toho, jaké má g znaménko v pravém okolí bodu β_k, tedy na základě lemmatu 3.5.24 nebo lemmatu 3.5.25.

Stejně jako v lemmatu 3.5.29 lze tento pseudoalgoritmus přepsat na algebraickou formuli sestavenou z atomických algebraických formulí tvaru $f(\xi_{n-1,j}(f')) \bowtie 0$, $g(\xi_{n-1,j}(f')) \bowtie 0$, $\xi_{n',k}(g) \bowtie \xi_{n-1,j}(f')$ a $f(\xi_{n',k}(g)) \bowtie 0$, tedy na algebraickou formuli řádu $n-1$. Tato formule vyjmenovává všechny příznivé případy, které mohou nastat pro kořeny polynomů f' a g v případě, kdy $g(\xi_{n,i}) \bowtie 0$, přičemž je jasné, že jeden z oněch případů nastat musí.

Nakonec uvažujme případ, kdy formule D má tvar $\xi_{n,i}(f) \bowtie \xi_{m,k}(g)$, kde $m \leq n$ a m je nenulové. Pišme ξ_1 a ξ_2 místo $\xi_{n,i}(f)$ a $\xi_{m,k}(g)$. Máme určit vzájemnou polohu kořenů ξ_1 a ξ_2.

Urči čísla $\alpha_0, \ldots, \alpha_{r+1}$ taková, že $a_0 = -\infty$, $\alpha_{r+1} = +\infty$ a $\alpha_1, \ldots, \alpha_r$ je rostoucí posloupnost všech kořenů derivací f' a g'. Prohlédnutím hodnot $\operatorname{sgn} f(\alpha_i)$ a $\operatorname{sgn} g(\alpha_i)$ stanov pro každý z kořenů ξ_1 a ξ_2 interval $\langle\!\langle \alpha_j, \alpha_{j+1} \rangle\!\rangle$, v němž leží. Jsou-li tyto intervaly různé, je jasné, jaká (ostrá) nerovnost platí mezi ξ_1 a ξ_2.

Jinak máme j takové, že $\alpha_j \leq \xi_1 < \alpha_{j+1}$ a $\alpha_j \leq \xi_2 < \alpha_{j+1}$. Platí-li $f(\alpha_j) = 0$ a $g(\alpha_j) = 0$, pak $\xi_1 = \xi_2$. Platí-li $f(\alpha_j) = 0$ a $g(\alpha_j) \neq 0$, pak $\xi_1 < \xi_2$. Platí-li $f(\alpha_j) \neq 0$ a $g(\alpha_j) = 0$, pak naopak $\xi_2 < \xi_1$.

Zbývá uvážit poslední případ, kdy znaménka $\operatorname{sgn} f(\alpha_j)$ a $\operatorname{sgn} g(\alpha_j)$ jsou obě nenulová, tedy oba kořeny ξ_1 a ξ_2 jsou větší než α_j. Znaménka $\operatorname{sgn} f(\alpha_{j+1})$ a $\operatorname{sgn} g(\alpha_{j+1})$ jsou ovšem také nenulová, a navíc platí $\operatorname{sgn} f(\alpha_j) \neq \operatorname{sgn} f(\alpha_{j+1})$ a $\operatorname{sgn} g(\alpha_j) \neq \operatorname{sgn} g(\alpha_{j+1})$. Platí-li $g(\xi_1) = 0$, pak $\xi_1 = \xi_2$. Platí-li $g(\xi_1) > 0$, pak $\xi_1 < \xi_2$ nebo $\xi_2 < \xi_1$ podle toho, je-li g klesající nebo rostoucí v intervalu $\langle\!\langle \alpha_j, \alpha_{j+1} \rangle\!\rangle$. Platí-li $g(\xi_1) < 0$, pak $\xi_1 < \xi_2$ nebo $\xi_2 < \xi_1$ podle toho, je-li g rostoucí nebo klesající v intervalu $\langle\!\langle \alpha_j, \alpha_{j+1} \rangle\!\rangle$. To, zda g je rostoucí nebo klesající v intervalu $\langle\!\langle \alpha_j, \alpha_{j+1} \rangle\!\rangle$ se ovšem pozná podle hodnot $\operatorname{sgn} g(\alpha_j)$ a $\operatorname{sgn} g(\alpha_{j+1})$.

Tím je formule D přepracována na ekvivalentní booleovskou kombinaci formulí $\mathrm{NR}_{n,j}(f)$, $\mathrm{NR}_{n,j}(g)$ a $g(\xi_{n,i}(f)) \bowtie 0$ a atomických algebraických formulí řádu nižšího než n, tedy na algebraickou formuli řádu n neobsahující atomické algebraické formule tvaru $\xi_{n_1,i_1}(..) \bowtie \xi_{n_2,i_2}(..)$ maximálního možného řádu n. Vzhledem k úvahám uvedeným výše lze tuto formuli dále přepracovat na ekvivalentní algebraickou formuli řádu menšího než n. QED

Zbývající úvahy o eliminaci kvantifikátorů pro teorii RCF jsou téměř stejné jako v případě teorií DOS a IAdd.

Lemma 3.5.31 *Nechť $A(x, y_1, \ldots, y_q)$ je formule v jazyce L_{RCF}, která je konjunkcí atomických formulí. Pak formule $\exists x A$ je v teorii* RCF *ekvivalentní s jistou otevřenou formulí, jejíž všechny volné proměnné jsou mezi $y_1, \ldots, y_q$.*

Důkaz Užitím lemmatu 3.2.15 můžeme každou atomickou podformuli formule A upravit na tvar $\sum_{i=1}^{n} a_i x^{n-i} = \sum_{i=1}^{m} b_i x^{m-i}$ nebo $\sum_{i=1}^{n} a_i x^{n-i} < \sum_{i=1}^{m} b_i x^{m-i}$,

kde a_i a b_i jsou termy v jazyce L_{RCF} neobsahující proměnnou x. Protože za chybějící koeficienty lze doplnit nuly, můžeme předpokládat, že $n = m$. Formule $\sum_{i=1}^{n} a_i x^{n-i} \bowtie \sum_{i=1}^{m} b_i x^{m-i}$ je ekvivalentní s formulí $\sum_{i=1}^{n} (a_i - b_i) x^{n-i} \bowtie 0$. Můžeme tedy předpokládat, že každá atomická podformule formule A má tvar $f(x) = 0$ nebo $f(x) < 0$, kde f je polynom, jehož koeficienty jsou termy v jazyce L_{RCF} neobsahující proměnnou x.

Uvažme nejprve případ, kdy alespoň jedna z atomických podformulí formule A je rovnost. Pak A má tvar $f(x) = 0 \ \& \ D(x, \underline{y})$, kde polynom f má nějaký stupeň n. Formule $\exists x A$ je v teorii RCF^+ ekvivalentní s formulí

$$\bigvee_{i=1}^{n} (\mathrm{NR}_{n,i}(f) \ \& \ D(\xi_{n,i}(f), \underline{y})). \tag{$*$}$$

Formule $(*)$ je dle lemmatu 3.5.30 ekvivalentní s jistou otevřenou formulí $B(\underline{y})$ v jazyce L_{RCF}. Protože RCF^+ je konzervativním rozšířením teorie RCF, formule $\exists x A$ a B jsou spolu ekvivalentní v teorii RCF.

Zbývá případ, kdy žádná z atomických podformulí formule A není rovnost. Pak formule A má tvar $f_1(x) < 0 \ \& \ \ldots \ \& \ f_k(x) < 0$, kde polynomy $f_1, \ldots, f_k$ mají stupně $n_1, \ldots, n_k$. Formule $\exists x A$ je v teorii RCF ekvivalentní s formulí

$$\begin{aligned} \bigvee_{j=1}^{k} \bigvee_{i=1}^{n_j} (\mathrm{NR}_{n_j,i}(f_j) \ \& \ \bigwedge_{r=1}^{k} (f_r \text{ je záporný v pravém okolí bodu } \xi_{n_j,i}(f_j))) \ \vee \\ \vee \ \bigwedge_{r=1}^{k} (f_r \text{ je záporný v pravém okolí bodu } -\infty). \end{aligned} \tag{$**$}$$

Formule $(**)$ je algebraickou formulí, jak vyplývá z lemmat 3.5.24 a 3.5.25. Díky lemmatu 3.5.30 je tedy opět ekvivalentní s jistou otevřenou formulí $B(\underline{y})$ v jazyce L_{RCF}, a opět platí, že formule $B(\underline{y})$ je ekvivalentní s původní formulí $\exists x A$. QED

Lemma 3.5.32 *Nechť φ je otevřená formule v jazyce L_{RCF}. Pak formule $\exists x \varphi$ je v teorii RCF ekvivalentní s jistou otevřenou formulí, která nemá jiné volné proměnné než ty, které jsou volné také ve formuli $\exists x \varphi$.*

Důkaz Formule $\neg(t = u)$ a formule $\neg(t < u)$ je v teorii RCF ekvivalentní s formulí $t < u \ \vee \ u < t$ resp. s formulí $t = u \ \vee \ u < t$. Zbývající úvahy jsou úplně stejné jako v důkazu lemmatu 3.5.7. QED

Lemma 3.5.33 *Každá atomická sentence v jazyce $\{+, \cdot, 0, 1, <, -\}$ je v teorii RCF dokazatelná nebo vyvratitelná.*

Důkaz je podobný jako v 3.5.8 a v 3.5.16. Uplatní se tvrzení 3.2.14 (g) a (h) a tvrzení 3.5.18(h). QED

Věta 3.5.34 *Teorie RCF připouští eliminaci kvantifikátorů a je úplná.*

Důkaz je úplně stejný jako u vět 3.5.9 a 3.5.17. QED

Všimněme si, že konzervativní rozšíření teorie RCF hrálo trochu jinou roli než konzervativní rozšíření teorií DO a IAdd. K teoriím DO a IAdd jsme přidali definice symbolů 0 a S resp. symbolů $=_n$, abychom získali teorii, která připouští eliminaci kvantifikátorů. Naproti tomu v případě teorie RCF jsme s pomocí dodatečných symbolů $\mathrm{NR}_{n,i}$ a $\xi_{n,i}$ dokázali, že už původní teorie, tj. teorie RCF, připouští eliminaci kvantifikátorů.

Alfred Tarski v souvislosti se svým výsledkem o struktuře $\mathbf{R}$ reálných čísel položil otázku, co by se stalo, kdybychom k jazyku L_{RCF} teorie RCF přidali unární funkční symbol, řekněme E, který bychom realizovali funkcí $x \mapsto \mathrm{e}^x$. O výsledné struktuře, kterou můžeme dočasně označit $\langle \mathbf{R}, E\rangle$, je dnes známo, že její teorie $\mathrm{Th}(\langle \mathbf{R}, E\rangle)$ nepřipouští eliminaci kvantifikátorů. Okolo roku 1991 ale dokázal A. Wilkie, že teorie $\mathrm{Th}(\langle \mathbf{R}, E\rangle)$ splňuje slabší podmínku, než je eliminovatelnost kvantifikátorů: každá formule v jazyce $L_{\mathsf{RCF}} \cup \{E\}$ je v teorii $\mathrm{Th}(\langle \mathbf{R}, E\rangle)$ ekvivalentní s jistou univerzální formulí a také s jistou existenční formulí. Další zajímavé otázky o struktuře $\mathrm{Th}(\langle \mathbf{R}, E\rangle)$ zůstávají dodnes otevřené. Čtenáři, který se chce dozvědět více o historii a souvislostech Tarského výsledku o struktuře $\mathbf{R}$, doporučujeme van den Driesův přehledový článek [16] a dále článek [17] téhož autora. Výsledek A. Wilkieho je v [99].

Postup, kterým jsme ukázali, že teorie IAdd axiomatizuje strukturu $\langle \mathrm{Z}, +, 0, \mathrm{s}\rangle$, vznikl zjednodušením obdobného výsledku o struktuře $\langle \mathrm{N}, +, 0, \mathrm{s}, <\rangle$, který dokázal M. Presburger v roce 1929 ([66]). Teorie struktury $\langle \mathrm{N}, +, 0, \mathrm{s}, <\rangle$ se dnes nazývá *Presburgerovou aritmetikou*. Někdy se tímto názvem označuje také teorie blízce příbuzné struktury $\langle \mathrm{Z}, +, 0, \mathrm{s}, <\rangle$. O Presburgerově výsledku na rozdíl od Tarského výsledku o struktuře $\mathbf{R}$ pravděpodobně nelze říci, že podnítil důležitý výzkum probíhající v následujících desetiletích. Je ale také počítán k důležitým událostem v logice 20. století.

Cvičení

1. Zdůvodněte, že formule $\neg\exists y(y < x)$ není v teorii DO ekvivalentní s žádnou otevřenou formulí, a že tedy teorie DO nepřipouští eliminaci kvantifikátorů.

   Návod. Přizpůsobte argument z cvičení 21 v oddílu 3.1.

2. Zdůvodněte podrobně, že je-li $\mathbf{D}_1$ struktura pro jazyk L_1 a $\mathbf{D}_2$ expanze struktury $\mathbf{D}_1$, pak každá sentence jazyka L_1 platí v $\mathbf{D}_1$ právě tehdy, platí-li v $\mathbf{D}_2$. (Totéž se již tvrdilo ve cvičení 18 oddílu 3.1.)

3. Dokažte, že struktura $\langle \mathrm{N}, 0, \mathrm{s}\rangle + \langle \mathrm{Z}, \mathrm{s}\rangle$ z obrázku 3.4.1 nemá žádnou expanzi, která je modelem teorie $\mathrm{Th}(\langle \mathrm{N}, +, 0, \mathrm{s}\rangle)$.

   Návod. Zdůvodněte, že ať je sčítání definováno jakkoliv, žádný z prvků oblasti $\langle \mathrm{Z}, \mathrm{s}\rangle$ nesplňuje formuli $\exists y(x = y + y \vee x = \mathrm{S}(y + y))$.

4. Je-li T úplná, pak každé bezesporné rozšíření T' teorie T je jejím konzervativním rozšířením. Dokažte.

5. Zdůvodněte na základě předchozích dvou cvičení, že větu 3.5.2 nelze obrátit.

6. Zdůvodněte užitím věty 3.5.2 nebo užitím cvičení 4, že teorie DOS je konzervativním rozšířením teorie SUCC.

7. Nechť T_2 je teorie vzniklá z teorie DOS odstraněním axiomu DO3 a nechť T_1 je teorie vzniklá z teorie SUCC odstraněním axiomu Q3. Dokažte, že teorie T_2 je konzervativním rozšířením teorie T_1.

8. Když je teorie T_2 konzervativním rozšířením teorie T_1, pak ke každému modelu $\mathbf{A}$ teorie T_1 existuje s ním elementárně ekvivalentní model $\mathbf{B}$, který má expanzi, která je modelem teorie T_2. Dokažte.

9. Zdůvodněte, že je-li T' konzervativní rozšíření teorie T a je-li φ sentence v jazyce teorie T, pak $(T' + \varphi)$ je konzervativní rozšíření teorie $(T + \varphi)$.

10. Nechť $F \notin L$ je n-ární funkční symbol, $\eta(\underline{x}, y)$ je formule v L a T je teorie s jazykem L. Nechť dále T' je teorie s jazykem $L \cup \{F\}$, jejímiž axiomy jsou všechny axiomy teorie T a navíc sentence $\forall \underline{x} \eta(\underline{x}, F(\underline{x}))$. Dokažte s užitím věty 3.5.2, že platí-li $T \vdash \forall \underline{x} \exists y \eta(\underline{x}, y)$, pak teorie T' je konzervativním rozšířením teorie T.

11. Dokažte, že je-li T' rozšíření teorie T o definice, pak každá formule v jazyce teorie T' je v teorii T' ekvivalentní s jistou formulí v jazyce teorie T.

    Návod. Nechť například T' je rozšířením teorie T o definici tvaru (d2) a nechť je dána formule φ v jazyce teorie T'. Stačí zabývat se atomickými podformulemi formule φ. Když $P(t_1, .., t_m)$ je atomická podformule formule φ, v níž term t_i obsahuje symbol F, pak formule $P(t_1, .., t_m)$ je ekvivalentní s formulí $\exists v(t_i = v \ \& \ P(t_1, .., t_{i-1}, v, t_{i+1}, .., t_m))$. Opakováním tohoto postupu pro symboly P jiné než rovnítko a všechny možné termy získáme formuli $\varphi^{(1)}$ ekvivalentní s formulí φ, ve které se symbol F vyskytuje pouze v rovnostech. Dále lze získat formuli $\varphi^{(2)}$ ekvivalentní s φ, ve které se symbol F vyskytuje vždy pouze na *levé* straně rovnosti, a pak formuli $\varphi^{(3)}$, ve které se symbol F vyskytuje vždy pouze v kontextu $F(t_1, .., t_n) = s$, kde termy t_i a s neobsahují symbol F. Každou podformuli tvaru $F(\underline{t}) = s$ lze pak nahradit formulí $\eta(\underline{t}, s)$.

12. Dokažte formuli $x \leq \overline{m} \equiv x = \overline{0} \vee \ .. \ \vee x = \overline{m}$ v teorii DOS.

13. Dokažte formuli $\neg(x =_n y) \equiv x =_n y + \overline{1} \vee \ .. \ \vee x =_n y + \overline{n-1}$ v teorii IAdd.

14. Dokažte, že formule z příkladu 3.5.13 je v teorii IAdd ekvivalentní s formulí $y_1 =_2 y_2 \ \& \ y_1 =_5 y_3 \ \& \ y_2 =_7 y_3$.

15. Dokažte, že teorie SUCC připouští eliminaci kvantifikátorů.

    Návod. Postupujte obdobně jako v případě teorie DOS, ale nepokoušejte se odstranit negativní literály. Lemma analogické lemmatu 3.5.5 formulujte pro konjunkci formulí tvaru $\mathrm{S}^{(m)}(x) = t$ a $\mathrm{S}^{(m)}(x) \neq t$.

16. Dokažte úplnost teorie DNO pomocí eliminace kvantifikátorů.

    Návod. Z triviálního důvodu není pravda, že každá sentence je v teorii DNO ekvivalentní s otevřenou sentencí, v jazyce teorie DNO totiž žádné otevřené sentence neexistují. Tuto potíž lze ale překonat přidáním symbolu $\bot$, tj. zkratky pro spor, mezi logické spojky.

17. Definujeme-li na množině $\mathrm{Z} \times \mathrm{Q}$ sčítání předpisem $[a,b]+[c,d]=[a+c,b+d]$ (tj. sčítá se „po složkách“) a dodefinujeme-li vhodně realizace symbolů 0 a 1, dostaneme model teorie IAdd. Dokažte. Toto cvičení a úvahy v souvisejícím příkladu 3.6.16 navrhl I. Korec.

18. Je-li f polynom s koeficienty $c_0,\ldots,c_n$ a platí-li pro číslo a, že $f(a)>0$ (nebo že $f(a)<0$), pak f je kladný (resp. záporný) v jistém okolí bodu a. Dokažte toto tvrzení v teorii uspořádaných těles.

    Návod. Zdůvodněte a užijte rovnost

    $$|f(x)-f(a)| = |x-a| \cdot \sum_{i=0}^{n} |c_i| \cdot |x^{i-1}+x^{i-2}a+\,\ldots\,+xa^{i-2}+a^{i-1}|.$$

    První činitel je pro x blízké k a velmi malý, součet lze omezit konstantou nezávislou na x.

19. Z faktů, že ve struktuře $\mathbf{R}$ reálných čísel platí axiomy R1–R15 a že ve struktuře $\langle \mathrm{R}, <\rangle$ platí věta o supremu, zdůvodněte užitím předchozího cvičení, že v $\mathbf{R}$ platí schéma R16.

    Návod. Platí-li $a<b$, $f(a)>0$, $f(b)<0$, označte γ supremum množiny $\{\, x \in (a,b) \,;\, f(x) \geq 0 \,\}$. Musí platit $f(\gamma)=0$.

20. V důkazu lemmatu 3.5.29 byla formule $\mathrm{NR}_{3,2}(f)$ přepracována na algebraickou formuli řádu 2. Udělejte totéž s formulí $\mathrm{NR}_{3,3}(f)$.

21. Navrhněte teorii, která axiomatizuje strukturu $\langle \mathrm{N}, +, 0, \mathrm{s}, <\rangle$, a dokažte její úplnost pomocí eliminace kvantifikátorů.

3.6 Rozhodnutelnost, definovatelnost, interpretovatelnost

Vraťme se ještě jednou k některému příkladu na eliminaci kvantifikátorů z oddílu 3.5. Prohlédneme-li si například důkaz věty 3.5.9 a důkazy předchozích lemmat 3.5.5–3.5.8, můžeme konstatovat, že v těchto důkazech jsou vlastně obsaženy dva *algoritmy*: jeden převede libovolnou formuli na formuli, která je s ní ekvivalentní a neobsahuje kvantifikátory, druhý rozhodne o dokazatelnosti otevřené sentence. Z obou algoritmů lze utvořit ještě další algoritmus, který rozhodne o dokazatelnosti libovolné sentence. Úloha rozpoznat, zda daná sentence v jazyce teorie DOS

je v teorii DOS dokazatelná, je tedy algoritmicky rozhodnutelnou úlohou. Nyní budeme chtít říci více o takovýchto úlohách.

Připomeňme si, že chceme-li uvažovat o algoritmech pracujících s formulemi, musíme mít jasno v tom, jak přesně se formule zapisují pomocí symbolů. Pro tento účel jsme se na začátku kapitoly domluvili, že množina Var všech proměnných je nekonečná spočetná, $\mathrm{Var} = \{v_0, v_1, \dots\}$, a že každý její prvek v_i zapisujeme jako písmeno `v` následované zápisem čísla i. Pro určitost k tomu nyní dodejme, že čísla zapisujeme binárně. Například je-li φ formule $\exists v_2(\mathrm{S}(v_2) = \mathrm{S}(0))$, pak φ je ve skutečnosti posloupností `∃v10=(S(v10),S(0))` sestávající z osmnácti symbolů. Nijak nevadí fakt, že symbol `0` má dvojí roli, vyskytuje se v indexech proměnných a jako konstanta je také prvkem některých jazyků.

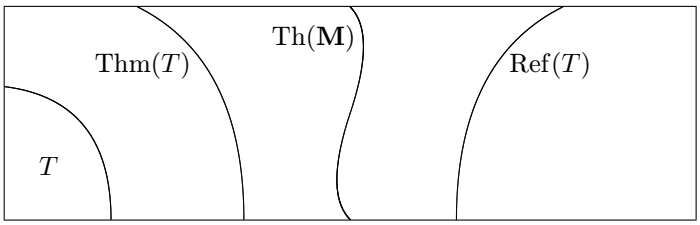
Budeme-li v tomto oddílu mluvit o axiomatické teorii, vždy předpokládáme, že její jazyk je nejvýše spočetný a že je-li nekonečný, byla pro zapisování jeho prvků přijata podobná dohoda jako pro zapisování nekonečně mnoha proměnných. Dále se pro účely strojového zpracování důkazů domluvme, že za prvotní v tomto oddílu považujeme hilbertovský kalkulus a že pro oddělování formulí od sebe užíváme při zapisování důkazů znak `#`. Důkaz tedy nyní není posloupností formulí, nýbrž je slovem tvaru $\varphi_1\#\varphi_2\#\dots\#\varphi_m$, kde každé podslovo φ_i je formulí, která je buď takovým či onakým axiomem, nebo je odvozena z některých dříve se vyskytujících podslov φ_j pomocí jednoho ze tří odvozovacích pravidel.

Od kapitoly 2 máme k dispozici kódovou tabulku, která přiřazuje číselné kódy všem znakům, které kdy můžeme potřebovat. Nejsou-li číselné kódy znaků důležité (což nikdy nejsou), můžeme kód znaku psát jako levý apostrof následovaný tímto znakem. Od kapitoly 2 máme také k dispozici kódování konečných posloupností přirozených čísel, které nám dovoluje libovolnou konečnou posloupnost přirozených čísel považovat za jediné přirozené číslo. Například pro formuli φ uvedenou výše můžeme tedy psát $\varphi = \langle\text{`∃`v`1`0`=`(`S`(`v`1`0`)`,`S`(`0`)`)}\rangle$. Kdo by na tom trval, mohl by případně do kódové tabulky nahlédnout a zjistit, že $\varphi = \langle 11, 91, 33, 32, 27, 12, 61, 12, 91, 33, 32, 13, 16, 61, 12, 32, 13, 13\rangle$. Šlo by také připomenout si definici kódování posloupností a určit číslo $\varphi = 2^{11+1} \cdot \dots \cdot 67^{13+1}$. To už ale pro náš výklad opravdu nemá význam. Navíc v kapitole 4 budeme potřebovat jiné kódování než ono založené na rovnosti $\langle a_0, \dots, a_{n-1}\rangle = 2^{a_0+1} \cdot \dots \cdot \mathrm{p}_{n-1}^{a_{n-1}+1}$, které jsme definovali v kapitole 2.

Důležité je pouze to, že díky kódové tabulce a díky jednoznačné kódovatelnosti a dekódovatelnosti konečných posloupností přirozených čísel můžeme formule a ostatní syntaktické objekty ztotožnit s přirozenými čísly a množiny syntaktických objektů pak považovat za množiny přirozených čísel. O libovolné množině formulí se tedy můžeme ptát, zda je například rekurzívní.

Připomeňme si, že $\mathrm{Thm}(T)$ označuje množinu všech sentencí dokazatelných v teorii T a dále že $\mathrm{Ref}(T)$ označuje množinu všech sentencí vyvratitelných v teorii T, tj. množinu všech sentencí φ takových, že $T \vdash \neg\varphi$. Evidentně platí, že množiny $\mathrm{Thm}(T)$ a $\mathrm{Ref}(T)$ jsou disjunktní právě tehdy, když teorie T je bezesporná (viz 3.2.7(c)), a že je-li $\mathbf{M}$ libovolný model teorie T, pak $\mathrm{Thm}(T) \subseteq \mathrm{Th}(\mathbf{M})$ a $\mathrm{Th}(\mathbf{M}) \cap \mathrm{Ref}(T) = \emptyset$. Vztahy mezi množinami $\mathrm{Thm}(T)$, $\mathrm{Ref}(T)$, $\mathrm{Th}(\mathbf{M})$ a T

jsou pro případ, kdy $\mathbf{M}$ je model teorie T, znázorněny na obr. 3.6.1, přičemž velký obdélník znázorňuje množinu všech sentencí v jazyce teorie T. Dále je zřejmé, že každá z množin $\mathrm{Thm}(T)$ a $\mathrm{Ref}(T)$ je m-převeditelná na druhou a že množina $\mathrm{Th}(\mathbf{M})$ je m-převeditelná na svůj komplement. Ve všech případech lze vystačit s (dokonce logaritmicky počitatelnou) funkcí $\varphi \mapsto \neg\varphi$, tj. s pouhým připsáním negace.



Obrázek 3.6.1: Vztahy mezi množinami $\mathrm{Thm}(T)$, $\mathrm{Ref}(T)$ a $\mathrm{Th}(\mathbf{M})$, platí-li $\mathbf{M} \models T$

Definice 3.6.1 *Teorie T je* rozhodnutelná*, jestliže množina* $\mathrm{Thm}(T)$ *je obecně rekurzívní. Jinak je* nerozhodnutelná*. Struktura* $\mathbf{D}$ *je* rozhodnutelná *nebo* nerozhodnutelná*, jestliže množina* $\mathrm{Th}(\mathbf{D})$ *je resp. není obecně rekurzívní.*

Jak již bylo řečeno, eliminace kvantifikátorů pro teorii DOS poskytuje algoritmus, který rozhoduje o náležení do množiny Thm(DOS). Tento algoritmus by se samozřejmě dal přepsat do formalismu jazyka RASP nebo do formalismu rekurzívních funkcí. Teorie DOS je tedy rozhodnutelná. Ze stejného důvodu jsou rozhodnutelné i teorie IAdd a RCF. Je zřejmé, že *úplná* teorie T je rozhodnutelná, právě když některý její model je rozhodnutelný, a to je právě tehdy, když každý její model je rozhodnutelný. Z toho plyne, že struktury $\langle \mathrm{N}, 0, \mathrm{s}, < \rangle$, $\langle \mathrm{Z}, +, 0, 1 \rangle$ a $\mathbf{R}$ jsou rozhodnutelné. Protože redukt rozhodnutelné struktury je evidentně opět rozhodnutelnou strukturou, také struktury $\langle \mathrm{N}, 0, \mathrm{s} \rangle$, $\langle \mathrm{N}, < \rangle$ a $\langle \mathrm{R}, < \rangle$ jsou rozhodnutelné. Z toho dále plyne rozhodnutelnost teorií SUCC, DO a DNO, všechny jsou totiž úplné. Také struktury z obrázků 3.4.1 a 3.4.2 jsou rozhodnutelné. Rozhodnutelnost teorií SUCC a DNO plyne také z faktu uvedeného ve cvičeních předchozího oddílu, totiž že obě tyto teorie (vlastně) připouštějí eliminaci kvantifikátorů.

Příklad 3.6.2 Přidejme k jazyku $\{0, \mathrm{S}\}$ teorie SUCC unární predikátový symbol P, zvolme nerekurzívní množinu $A \subseteq \mathrm{N}$ a označme T_1 teorii $\mathsf{SUCC} \cup \{\, P(\overline{n}) \,;\, n \in A \,\}$. Když $n \notin A$, lze zvolit expanzi $\mathbf{M} = \langle \mathrm{N}, 0, \mathrm{s}, P^{\mathbf{M}} \rangle$ struktury $\langle \mathrm{N}, 0, \mathrm{s} \rangle$, ve které neplatí sentence $P(\overline{n})$. Platí tedy $\forall n (n \in A \Leftrightarrow P(\overline{n}) \in \mathrm{Thm}(T_1))$. Z toho plyne $A \leq_{\mathrm{m}} \mathrm{Thm}(T_1)$. Teorie T_1 je tedy příkladem nerozhodnutelné teorie. Struktura $\langle \mathrm{N}, 0, \mathrm{s}, \mathrm{N} \rangle$, ve které je predikát P realizován celou množinou N, je modelem teorie T_1, o němž lze zdůvodnit, že je rozhodnutelnou strukturou. Naopak struktura $\langle \mathrm{N}, 0, \mathrm{s}, A \rangle$ je příkladem nerozhodnutelného modelu teorie T_1.

Příklad 3.6.3 Zvolme jazyk a množinu $A \notin \mathit{OR}$ stejně jako v předchozím příkladu a položme $T_2 = T_1 \cup \{\neg P(\overline{n}) \,;\, n \notin A\}$. Teorie T_2 je nerozhodnutelná ze stejného důvodu jako teorie T_1. Oproti příkladu 3.6.2 máme navíc $\overline{A} \leq_{\mathrm{m}} \mathrm{Thm}(T_2)$. Tentokrát

platí, že všechny modely teorie T_2 jsou nerozhodnutelné. Pro pořádek dodejme, že teorie T_2 není úplná; stačí uvážit například sentenci $\forall x(P(x) \vee P(\mathrm{S}(x)))$.

Příklad 3.6.4 Zvolme množinu A jako v předchozích dvou příkladech, zvolme jazyk $\{c, P_0, P_1, \dots\}$ s jednou konstantou a nekonečně mnoha unárními predikáty a položme $T_3 = \{P_n(c); n \in A\}$. Stejně jako v příkladu 3.6.2 platí, že T_3 je nerozhodnutelnou teorií, jejíž některé modely jsou a některé nejsou rozhodnutelné. Teorie T_3 má ale dokonce jednoprvkový model, který je nerozhodnutelnou strukturou.

Věta 3.6.5 *Je-li* $\mathbf{D}$ *konečná struktura pro konečný jazyk, pak* $\mathbf{D}$ *je rozhodnutelná.*

Důkaz Nechť $a_1, \dots, a_n$ jsou všechny prvky nosné množiny D struktury $\mathbf{D}$, která je strukturou pro konečný jazyk L. Snadno lze navrhnout datové struktury pro zapisování prvků množiny D a pro zapisování ohodnocení proměnných ve struktuře $\mathbf{D}$. Můžeme si myslet, že realizace $F^{\mathbf{D}}$ libovolného funkčního symbolu $F \in L$ je definována tabulkou, podobně jako v případě struktury $\mathbf{A}$ z obrázku 3.1.1 na straně 141. Tyto tabulky umožňují určit pro daný term t a ohodnocení e hodnotu $t^{\mathbf{D}}[e]$ termu t ve struktuře $\mathbf{D}$. Dále si můžeme myslet, že podobnou tabulku máme i pro realizaci $P^{\mathbf{D}}$ každého predikátového symbolu $P \in L$. Podmínka $\mathbf{D} \models \varphi[e]$ je tedy v případě, kdy formule φ je atomická, algoritmicky rozhodnutelná. Podmínky T8 a T9 v našem případě říkají

$$\mathbf{D} \models (\exists x\varphi)[e] \;\Leftrightarrow\; \mathbf{D} \models \varphi[e(x/a_1)] \;\vee\; \dots \;\vee\; \mathbf{D} \models \varphi[e(x/a_n)],$$
$$\mathbf{D} \models (\forall x\varphi)[e] \;\Leftrightarrow\; \mathbf{D} \models \psi[e(x/a_1)] \;\&\; \dots \;\&\; \mathbf{D} \models \varphi[e(x/a_n)].$$

Platí také ekvivalence

$$\mathbf{D} \models (\varphi \to \psi)[e] \;\Leftrightarrow\; \mathbf{D} \not\models \varphi[e] \;\vee\; \mathbf{D} \models \psi[e]$$

a tři další ekvivalence týkající se zbývajících logických spojek. Na těchto šesti ekvivalencích lze založit proceduru, která otázku, zda daná formule je splněna daným ohodnocením, převádí na analogické otázky týkající se jednodušších a jednodušších formulí. Přesněji řečeno, jde o proceduru, která pro dané vstupy φ a e pomocí rekurzívního volání sebe sama rozhodne, zda platí $\mathbf{D} \models \varphi[e]$. Struktura $\mathbf{D}$ ovšem není vstupem, ta je známa už v době psaní oné procedury. Zbytek, tj. hlavní program, který rozhoduje o platnosti dané sentence φ v $\mathbf{D}$, je zřejmý: sentence φ je v $\mathrm{Th}(\mathbf{D})$, právě když pro libovolně zvolené ohodnocení e naše procedura řekne ano na otázku $[\varphi, e]$. QED

Definujme $\mathrm{Proof}_T(\varphi, d)$ jako zkratku pro podmínku „φ je sentence, d je její důkaz v teorii T“.

Věta 3.6.6 *Nechť teorie* T *(jako množina sentencí) je primitivně rekurzívní, rekurzívní nebo rekurzívně spočetná. Pak i podmínka* $\mathrm{Proof}_T(\varphi, d)$ *je primitivně rekurzívní, resp. rekurzívní, resp. rekurzívně spočetná. Množiny* $\mathrm{Thm}(T)$ *a* $\mathrm{Ref}(T)$ *jsou ve všech třech případech rekurzívně spočetné.*

Důkaz Platí $\varphi \in \mathrm{Thm}(T) \;\Leftrightarrow\; \exists d \mathrm{Proof}_T(\varphi, d)$. Je-li podmínka $\mathrm{Proof}_T(\varphi, d)$ rekurzívně spočetná, pak množina $\mathrm{Thm}(T)$ je rekurzívně spočetná díky implikaci $\Leftarrow$ ve větě 2.2.25 resp. díky tvrzení 2.2.35(e). Množina $\mathrm{Ref}(T)$ je rekurzívně spočetná z podobného důvodu, anebo také proto, že $\mathrm{Ref}(T) \leq_{\mathrm{m}} \mathrm{Thm}(T)$.

Zabývejme se tedy klasifikací podmínky $\mathrm{Proof}_T(\varphi, d)$. Nejprve nechť $\mathrm{Number}(z)$ znamená „z je binárním zápisem přirozeného čísla“ (tj. „z je numerickým kódem slova, které je binárním zápisem přirozeného čísla“) a nechť $\mathrm{Var}(v)$ znamená „v je proměnná“. Platí

$$\begin{aligned}\mathrm{Number}(z) \;\Leftrightarrow\; &\mathrm{Seq}(z) \;\&\; \mathrm{Lh}(z) \neq 0 \;\&\; (\mathrm{Lh}(z) > 1 \;\Rightarrow\; (z)_0 \neq \text{`}\mathtt{0}) \;\&\\ &\&\; \forall i{<}\mathrm{Lh}(z)\,((z)_i = \text{`}\mathtt{0} \;\vee\; (z)_i = \text{`}\mathtt{1}),\\ \mathrm{Var}(v) \;\Leftrightarrow\; &\exists z{<}v\,(\mathrm{Number}(z) \;\&\; v = \langle\text{`}\mathtt{v}\rangle * z),\end{aligned}$$

kde $*$ označuje operaci spojení posloupností definovanou v oddílu 2.2. Podmínky $\mathrm{Number}(z)$ a $\mathrm{Var}(v)$ jsou evidentně primitivně rekurzívní. Dále nechť $\mathrm{Term}(t)$ znamená „t je term“. Předpokládejme ve zbytku tohoto důkazu, že jazyk teorie T je aritmetický. U všech úvah bude zřejmé, jak je třeba je modifikovat pro jiné jazyky. Platí

$$\begin{aligned}\mathrm{Term}(t) \;\Leftrightarrow\; &\mathrm{Var}(t) \;\vee\; t = \langle\text{`}\mathtt{0}\rangle \;\vee\; \exists s_1{<}t\,\exists s_2{<}t\,(\mathrm{Term}(s_1) \;\&\\ &\&\; \mathrm{Term}(s_2) \;\&\; t = \langle\text{`}\mathtt{(}\rangle * s_1 * \langle\text{`}\mathtt{+}\rangle * s_2 * \langle\text{`}\mathtt{)}\rangle) \;\vee\\ &\vee\; (\ldots \text{ podobně pro symboly } \cdot \text{ a } \mathtt{S} \ldots).\end{aligned}$$

Číslo (posloupnost symbolů) je term, je-li to proměnná, nebo je-li to posloupnost, jejímž jediným členem je konstanta nula, nebo lze-li je získat z jednodušších termů pomocí závorek, operačního znaménka a příslušného počtu (jednoho nebo dvou) menších termů. To je odvození charakteristické funkce množiny všech aritmetických termů pomocí zobecněné primitivní rekurze (tj. na základě lemmatu 2.2.20). Zdůvodnění, že podmínka $\mathrm{Term}(t)$ je primitivně rekurzívní, je tedy stejné jako zdůvodnění z oddílu 2.2, že množina všech výrokových formulí je primitivně rekurzívní. Také následující podmínky a funkce jsou primitivně rekurzívní:

$\mathrm{FmAt}(\varphi)$	φ je atomická formule,
$\mathrm{Fm}(\varphi)$	φ je formule,
$\mathrm{SubT}(t, v, s)$	výsledek substituce termu t za proměnnou v v termu s,
$\mathrm{SubF}(t, v, \varphi)$	výsledek substituce termu t za proměnnou v ve formuli φ,
$\mathrm{OccT}(v, t)$	proměnná v se vyskytuje v termu t,
$\mathrm{OccF}(v, \varphi)$	proměnná v má volné výskyty ve formuli φ,
$\mathrm{Sent}(\varphi)$	φ je sentence,
$\mathrm{FreeSub}(t, v, \varphi)$	t je term substituovatelný za proměnnou v ve formuli φ,
$\mathrm{LogAx}(\varphi)$	φ je logický axiom,

přičemž v případě funkce SubF je samozřejmě řeč o substituci za všechny volné výskyty proměnné v. Kteroukoliv z těchto sedmi podmínek a dvou funkcí lze totiž odvodit z funkcí týkajících se kódování posloupností a z funkcí a podmínek vyskytujících se na seznamu dříve, a to většinou s užitím zobecněné primitivní rekurze. Například $\mathrm{FreeSub}(t,v,\varphi)$, právě když nastane některý z následujících případů:

- $\mathrm{FmAt}(\varphi)$,
- φ je utvořena pomocí logické spojky z jedné nebo dvou menších formulí, v níž nebo v obou z nichž je term t substituovatelný za v,
- φ je utvořena z menší formule ψ pomocí kvantifikace užité na proměnnou u, přičemž $\neg\mathrm{OccF}(v,\varphi)$,
- φ je utvořena z menší formule ψ pomocí kvantifikace užité na proměnnou u, přičemž $\mathrm{FreeSub}(t,v,\psi)$ a $\neg\mathrm{OccT}(u,t)$.

Přitom si všimněme, že podmínka $\neg\mathrm{OccF}(v,\varphi)$, „$v$ nemá volné výskyty ve formuli φ“, je splněna mimo jiné tehdy, jsou-li u a v tytéž proměnné. Dále si všimněme, že je-li φ tvaru $\langle\text{`}\forall\rangle * u * \psi$ nebo $\langle\text{`}\forall\rangle * u * \psi$, pak $u < \varphi$ a $\psi < \varphi$. Při popisu kvantifikace jako syntaktické operace a v odvození celé podmínky $\mathrm{FreeSub}(t,v,\varphi)$ se tedy obejdeme bez neomezených kvantifikátorů. Poslední podmínka $\mathrm{LogAx}(\varphi)$ je disjunkcí několika podmínek, neboť φ je logickým axiomem, právě když φ má jeden z tvarů B1, B2, A1–A7 nebo E1–E5. Přitom například φ je logickým axiomem tvaru B2, právě když

$$\exists\psi{<}\varphi\,\exists v{<}\varphi\,\exists t{<}\varphi\,(\mathrm{Term}(t)\ \&\ \mathrm{Var}(v)\ \&\ \mathrm{Fm}(\psi)\ \&\ \mathrm{FreeSub}(t,v,\psi)\ \&\ \&\ \varphi = \langle\text{`(}, \text{`}\forall\rangle * v * \psi * \langle\text{`}\neg\rangle * \mathrm{SubF}(v,t,\psi) * \langle\text{`)}\rangle),$$

což je primitivně rekurzívní podmínka, víme-li již, že podmínky $\mathrm{Term}(t)$, $\mathrm{Var}(v)$, $\mathrm{Fm}(\psi)$ a $\mathrm{FreeSub}(t,v,\psi)$ a funkce SubF jsou primitivně rekurzívní.

Definujme dvě pomocné podmínky $\mathrm{Beg}(c,d)$ a $\mathrm{Ends}(d,\varphi)$:

$$\mathrm{Beg}(c,d) \Leftrightarrow c = d \vee \exists x{<}d\,(d = c * \langle\text{`\#}\rangle * x),$$
$$\mathrm{Ends}(d,\varphi) \Leftrightarrow \forall i{<}\mathrm{Lh}(\varphi)\,((\varphi)_i \neq \text{`\#}) \ \&\ (\varphi = d \vee \exists x{<}d\,(d = x * \langle\text{`\#}\rangle * \varphi)).$$

Tyto podmínky budeme potřebovat v situaci, kdy c a d budou důkazy a φ formule. Podmínku $\mathrm{Beg}(c,d)$ můžeme číst „(důkaz) c je počátečním úsekem (důkazu) d“, podmínku $\mathrm{Ends}(d,\varphi)$ můžeme číst „(formule) φ je závěrem (důkazu) d“. Obě jsou evidentně primitivně rekurzívní. Nyní už můžeme posoudit to, o co nám jde. Platí totiž $\mathrm{Proof}_T(\varphi,d)$, právě když

$$\begin{aligned}
&\mathrm{Ends}(d,\varphi)\ \&\ \forall c{<}d\,\forall\psi{<}d\,(\mathrm{Beg}(c,d)\ \&\ \mathrm{Ends}(c,\psi) \Rightarrow \mathrm{Fm}(\psi)\ \&\\
&\quad\&\ (\exists b{<}c\,\exists\alpha{<}c\,\exists\beta{<}c\,\exists v{<}c\,(\mathrm{Fm}(\alpha)\ \&\ \mathrm{Fm}(\beta)\ \&\ \mathrm{Var}(v)\ \&\\
&\qquad\qquad\&\ \mathrm{Beg}(b,c)\ \&\ \mathrm{Ends}(b, \langle\text{`(}\rangle * \alpha * \langle\text{`}\neg\rangle * \beta\langle\text{`)}\rangle)\ \&\ \neg\mathrm{OccF}(v,\alpha)\ \&\\
&\qquad\qquad\&\ \psi = \langle\text{`(}\rangle * \alpha * \langle\text{`}\neg, \text{`}\forall\rangle * v * \beta * \langle\text{`)}\rangle)\ \vee\\
&\qquad\vee\ (\ldots\ \text{podobně pro pravidla Gen-E a MP}\ \ldots)\ \vee\\
&\qquad\vee\ \mathrm{LogAx}(\psi)\ \vee\ \psi \in T)).
\end{aligned}$$

Vidíme, že podmínku $\mathrm{Proof}_T(\varphi, d)$ lze sestavit z podmínky $\psi \in T$ a primitivně rekurzívních podmínek pomocí logických spojek a omezených kvantifikátorů. Odtud plyne tvrzení věty pro případ $T \in \mathit{PR}$ nebo $T \in \mathit{OR}$. Zápis podmínky $\mathrm{Proof}_T(..)$ lze snadno ekvivalentně přepsat tak, aby se v něm podmínka $\psi \in T$ nevyskytovala v rozsahu platnosti žádné implikace ani negace, tj. aby celá podmínka $\mathrm{Proof}_T(..)$ byla z podmínky $\psi \in T$ sestavena pouze pomocí konjunkce, disjunkce a omezené kvantifikace. Odtud plyne tvrzení věty pro případ, kdy $T \in \mathit{RS}$. QED

Například axiomatika Zermelovy-Fraenkelovy teorie množin je obvykle formulována jako několik jednotlivých sentencí a několik schémat. Protože schémata jsou definována čistě syntakticky (každá sentence takového a takového tvaru je axiomem), teorie ZF má primitivně rekurzívní množinu axiomů. Věta 3.6.6 pro tento případ říká, že množina $\mathrm{Thm}(\mathsf{ZF})$ je rekurzívně spočetná. Také podmínka $\mathrm{Proof}_{\mathsf{GB}}(\varphi, d)$ je primitivně rekurzívní a množina $\mathrm{Thm}(\mathsf{GB})$ je rekurzívně spočetná. To platí buď ze stejného důvodu, nebo proto, že teorie GB je dokonce konečně axiomatizovatelná.

Věta 3.6.7 (Craigův trik) *Nechť T je teorie taková, že množina $\mathrm{Thm}(T)$ je rekurzívně spočetná. Pak existuje teorie S ve stejném jazyce a s primitivně rekurzívní množinou axiomů, která je ekvivalentní s teorií T.*

Důkaz Dle věty o projekci 2.2.25 k množině $\mathrm{Thm}(T)$ existuje relace $R \subseteq \mathrm{N}^2$ taková, že R je primitivně rekurzívní a platí $\forall\varphi(\varphi \in \mathrm{Thm}(T) \Leftrightarrow \exists n R(\varphi, n))$. Můžeme předpokládat, že $R(m, n)$ platí pouze v případě, kdy m je sentence. Pro účely tohoto důkazu definujme pro sentenci φ a přirozené číslo $n \geq 1$ sentenci φ^n jako $(\varphi \,\&\, (\varphi \,\&\, (..\,\&\,\varphi)\,..))$, tj. jako konjunkci n exemplářů sentence φ se závorkami kumulujícími se doprava. Pro libovolnou sentenci ψ existuje mezi čísly $n \geq 2$ nejvýše jedno takové, že $\psi = \varphi^n$. Navíc podmínka $\psi = \varphi^{n+2}$ je PR. Položme

$$S = \{\, \varphi^{n+2} \,;\, R(\varphi, n) \,\} = \{\, \psi \,;\, \exists n{<}\psi\, \exists \varphi{<}\psi\, (\psi = \varphi^{n+2} \;\&\; R(\varphi, n)) \,\}.$$

Množina S je primitivně rekurzívní. Když sentence ψ tvaru φ^{n+2} je v S, pak $R(\varphi, n)$ a $\varphi \in \mathrm{Thm}(T)$. Z φ lze ovšem v T dokázat i φ^{n+2}. Tedy $\mathrm{Thm}(S) \subseteq \mathrm{Thm}(T)$. Když $\varphi \in \mathrm{Thm}(T)$, pak $\varphi^{n+2} \in S$ pro jisté n. Z φ^{n+2} lze ovšem v S dokázat φ. Tedy $\mathrm{Thm}(T) \subseteq \mathrm{Thm}(S)$. QED

Vidíme, že „trik“ spočíval v nahrazení každé sentence z $\mathrm{Thm}(T)$ jinou sentencí, která říká přesně totéž, způsob jejího zápisu ale navíc kóduje jistou numerickou informaci.

Řekneme, že teorie T je *rekurzívně axiomatizovatelná*, jestliže je ekvivalentní s nějakou teorií S, která má rekurzívní množinu axiomů. Z věty 3.6.7 plyne, že nezáleží na tom, řekneme-li v této definici „primitivně rekurzívní“ nebo naopak „rekurzívně spočetná“ místo „rekurzívní“.

Věta 3.6.8 *Je-li teorie T rekurzívně axiomatizovatelná a úplná, pak T je rozhodnutelná.*

Důkaz Množiny $\mathrm{Thm}(T)$ a $\mathrm{Ref}(T)$ jsou rekurzívně spočetné díky větě 3.6.6. Z úplnosti teorie T plyne, že jsou navzájem komplementární. Zbytek je věta 2.2.27, tj. Postova věta. Trochu přesněji řečeno, množiny $\mathrm{Thm}(T)$ a $\mathrm{Ref}(T)$ sice jako množiny čísel komplementární nejsou, jejich sjednocení je ale rekurzívní množina Sent všech (číselných kódů všech) sentencí příslušného jazyka. Takže můžeme vzít množiny $A = \mathrm{Thm}(T)$ a $B = \mathrm{Ref}(T) \cup (\mathrm{N} - \mathrm{Sent})$. Ty jsou navzájem komplementární a rekurzívně spočetné, lze na ně tedy užít Postovu větu. Z $B \in \mathit{OR}$ ovšem plyne $\mathrm{Ref}(T) \in \mathit{OR}$, neboť $\mathrm{Ref}(T) = B \cap \mathrm{Sent}$. Viz též cvičení 21 oddílu 2.2. QED

Z věty 3.6.8 například plyne rozhodnutelnost teorie DNO (víme-li z komentáře k větě 3.4.15, že teorie DNO je úplná), a to i bez okliky přes eliminovatelnost kvantifikátorů pro teorii RCF.

Z věty 3.6.8 a z faktu, že rozhodnutelná teorie je rekurzívně axiomatizovatelná, dále plyne, že není-li množina tvaru $\mathrm{Thm}(T)$ rekurzívní, pak není ani ve sjednocení $\Sigma_1 \cup \Pi_1$, tj. ona ani její komplement nejsou rekurzívně spočetné.

Věta 3.6.9 *Je-li T bezesporná a rekurzívně axiomatizovatelná teorie v jazyce L, pak existuje úplná teorie S v témže jazyce L, která je rozšířením teorie T a pro niž platí* $\mathrm{Thm}(S) \in \Sigma_2 \cup \Pi_2$.

Důkaz Definujme nekonečnou posloupnost $S_0, S_1, \ldots$ teorií v jazyce L následující rekurzí:

$$S_0 = T,$$
$$S_{n+1} = \begin{cases} S_n \cup \{n\} & \text{pokud } n \text{ je sentence v } L \text{ a platí } S_n \nvdash \neg n \\ S_n & \text{jinak.} \end{cases}$$

Z lemmatu 3.2.7(d) plyne (indukcí), že každá teorie S_n je bezesporná. Položme $S = \bigcup_n S_n$. Také S je bezesporná. Uvažujme libovolnou sentenci φ v L. V okamžiku $n = \varphi$ byla buď do S_{n+1} přijata sentence φ, nebo nebyla a platilo $S_n \vdash \neg\varphi$. V prvním případě platí $\varphi \in S_{n+1}$ a $S \vdash \varphi$. V druhém případě máme $S \vdash \neg\varphi$. Tím je zdůvodněno, že teorie S je úplná. Uvažujme následující podmínku $C(w)$ pro číslo w:

$$\mathrm{Seq}(w)\ \&\ \forall n{<}\mathrm{Lh}(w)\,((w)_n \le 1\ \&$$
$$\&\ ((w)_n = 1 \Leftrightarrow \mathrm{Sent}(n)\ \&\ T \nvdash (\bigwedge_{\psi<n,(w)_\psi=1} \psi) \to \neg n)).$$

Lze ověřit, že podmínka C má tyto vlastnosti:

(i) $\forall m \exists! w(C(w)\ \&\ \mathrm{Lh}(w) = m)$,

(ii) $\forall w \forall n{<}\mathrm{Lh}(w)\,((w)_n = 1 \Rightarrow \mathrm{Sent}(n))$,

(iii) $\forall w(T \cup \{\, n\,;\ n < \mathrm{Lh}(w)\ \&\ (w)_n = 1\,\} = S_{\mathrm{Lh}(w)})$,

(iv) $C \in \Sigma_2$.

Přitom (i)–(iii) se dokáže indukcí dle m či dle $\mathrm{Lh}(w)$. Protože T je rekurzívně axiomatizovatelná, podmínka $T \nvdash (\bigwedge_{\psi<n,(w)_\psi=1} \psi) \to \neg n$ je Π_1 díky větě 3.6.6. Podmínka C je tedy sestavena z Π_1-podmínky a primitivně rekurzívních podmínek pomocí logických spojek a omezené kvantifikace. Odtud plyne (iv). Platí také $C \in \Pi_2$, to ale nepotřebujeme. Z (i) plyne, že podmínky

$$\exists w(C(w) \ \&\ n < \mathrm{Lh}(w) \ \&\ (w)_n = 1) \quad \text{a} \quad \forall w(C(w) \ \&\ n < \mathrm{Lh}(w) \Rightarrow (w)_n = 1)$$

pro číslo n jsou spolu ekvivalentní. Přitom první je Σ_2 a druhá je Π_2. Z (iii) je vidět, že každá z těchto podmínek je ekvivalentní s $n \in S$. Tedy $S \in \Sigma_2 \cap \Pi_2$. QED

Věta 3.6.10 *Nechť φ je sentence v jazyce teorie T a T je rozhodnutelná. Pak i teorie $(T + \varphi)$ je rozhodnutelná.*

Důkaz Platí $\mathrm{Thm}(T + \varphi) \leq_{\mathrm{m}} \mathrm{Thm}(T)$, neboť $\forall\psi((T + \varphi) \vdash \psi \ \Leftrightarrow\ T \vdash \varphi \to \psi)$. QED

Tato věta boří občas se vyskytující představu, že nerozhodnutelné teorie obvykle vznikají z rozhodnutelných přidáním silných axiomů. Pravda je spíš opačná, přidání axiomů zakazuje určité situace, tj. vylučuje některé z dosud možných modelů, což může usnadnit úvahy o případné rozhodovací proceduře.

Větu 3.6.10 lze číst také takto: odebráním axiomu z nerozhodnutelné teorie T vznikne opět nerozhodnutelná teorie. Má-li ale teorie T jen konečně mnoho axiomů, můžeme odebírání opakovat a odstranit všechny! Podaří-li se nám pro nějaký jazyk L najít nerozhodnutelnou konečně axiomatizovatelnou teorii T v jazyce L, budeme zároveň vědět, že teorie s tímže jazykem a s prázdnou množinou axiomů je nerozhodnutelná, tj. že množina všech logicky platných formulí v jazyce L je nerozhodnutelná. Zatím pouze víme, že existují nerozhodnutelné teorie s primitivně rekurzívní množinou axiomů, viz cvičení.

Definice 3.6.11 *Nechť $\mathbf{D} = \langle D, .. \rangle$ je struktura pro jazyk L.* Formule $\varphi(x_1, .., x_k)$ definuje *ve struktuře $\mathbf{D}$ množinu $A \subseteq D^k$, jestliže $A = \{\, [a_1, .., a_k] \,;\, \mathbf{D} \models \varphi[\underline{a}] \,\}$. Množina A je* definovatelná *ve struktuře $\mathbf{D}$, existuje-li formule $\varphi(x_1, .., x_k)$, která ji v $\mathbf{D}$ definuje.* Prvek *a množiny D je* definovatelný *ve struktuře $\mathbf{D}$, jestliže $\{a\}$ je množina definovatelná v $\mathbf{D}$.*

Příklad 3.6.12 Ve struktuře $\langle \mathrm{N}, + \rangle$ definuje formule $\exists y(y + y = x)$ množinu všech sudých čísel a formule $\forall y(y + x = y)$ definuje prvek 0. V téže struktuře formule $x_1 \neq x_2 \ \&\ \exists y(x_1 + y = x_2)$ definuje relaci $<$.

Příklad 3.6.13 Věta o čtyřech čtvercích (důkaz lze vyčíst např. z [35]) tvrdí, že každé přirozené číslo je součtem čtyř druhých mocnin přirozených čísel. Z věty o čtyřech čtvercích plyne, že formule

$$\exists v_1 \exists v_2 \exists v_3 \exists v_4 (v_1 \cdot v_1 + v_2 \cdot v_2 + v_3 \cdot v_3 + v_4 \cdot v_4 = x)$$

definuje množinu N ve struktuře $\langle \mathrm{Z}, +, \cdot \rangle$.

Řekneme, že funkce f je *automorfismus* struktury $\mathbf{D}$, platí-li $f : \mathbf{D} \to_0 \mathbf{D}$ a navíc $\mathrm{Rng}(f) = D$. Automorfismus struktury $\mathbf{D}$ je tedy vnoření struktury $\mathbf{D}$ do sebe, které je *na*. Snadno lze ověřit, že pro libovolný automorfismus f struktury $\mathbf{D}$ platí $f : \mathbf{D} \to_\mathrm{e} \mathbf{D}$. Jinými slovy, každý automorfismus je elementárním vnořením.

Lemma 3.6.14 *Když f je automorfismus struktury $\mathbf{D}$, pak pro libovolnou definovatelnou množinu $A \subseteq D^k$ platí $A = \{\, [f(a_1), .., f(a_k)] \,;\, [a_1, .., a_k] \in A \,\}$. Jinými slovy, každá definovatelná množina nebo relace se libovolným automorfismem zobrazí sama na sebe.*

Důkaz ponecháváme za cvičení.

Příklad 3.6.15 Množina N není definovatelnou množinou ve struktuře $\langle \mathrm{Z}, +, 0 \rangle$. Automorfismem $a \mapsto -a$ se tato množina totiž nezobrazí sama na sebe.

Struktura $\langle \mathrm{Z}, +, 0, 1 \rangle$ nemá žádný netriviální (tj. různý od identického) automorfismus. Na základě lemmatu 3.6.14 tedy nemůžeme přímo usoudit, že množina N není definovatelná ve struktuře $\langle \mathrm{Z}, +, 0, 1 \rangle$. I. Korec navrhl následující úvahu.

Příklad 3.6.16 Nechť $\varphi(x)$ je formule v jazyce $\{+, 0, 1\}$, která definuje množinu N ve struktuře $\langle \mathrm{Z}, +, 0, 1 \rangle$. Pak v této struktuře platí sentence

$$\forall x \forall y (x + y = 0 \;\to\; x = 0 \;\vee\; (\varphi(x) \;\equiv\; \neg\varphi(y))),$$

neboť z dvojice $[a, -a]$ je v N pro $a \neq 0$ vždy právě jeden prvek. Tato sentence tedy musí platit i ve struktuře $\mathbf{D}$ s nosnou množinou $\mathrm{Z} \times \mathrm{Q}$ ze cvičení 17 oddílu 3.5. Struktura $\mathbf{D}$ je totiž elementárně ekvivalentní se strukturou $\langle \mathrm{Z}, +, 0, 1 \rangle$, protože obě jsou modely téže úplné teorie IAdd. Množina, kterou definuje formule φ ve struktuře $\mathbf{D}$, se však automorfismem $[a, b] \mapsto [a, -b]$ jistě nezobrazí sama na sebe. Tudíž N není množina definovatelná ve struktuře $\langle \mathrm{Z}, +, 0, 1 \rangle$.

V předchozím příkladu jsme použili vědomost, že IAdd je úplná teorie. Tuto vědomost jsme v předchozím oddílu získali pomocí eliminace kvantifikátorů. Ukažme si ještě jiné zdůvodnění faktu, že množina N není ve struktuře $\langle \mathrm{Z}, +, 0, 1 \rangle$ definovatelná. Odvoláme se v něm opět na eliminaci kvantifikátorů, obejdeme se ale bez lemmatu 3.6.14.

Definujme dočasně, že množina $X \subseteq \mathrm{Z}$ je *periodická*, jestliže existuje přirozené číslo $m > 0$ takové, že $\forall a \in \mathrm{Z}(a \in X \;\Leftrightarrow\; a + m \in X)$. Dále definujme rovněž dočasně, že množina $X \subseteq \mathrm{Z}$ je *skoro periodická*, jestliže se od některé periodické množiny liší o nejvýše konečně mnoho prvků. Lze ověřit, že každá atomická formule $\varphi(x)$ v jazyce L^+_{IAdd} definuje ve struktuře $\langle \mathrm{Z}, +, 0, 1, =_1, =_2, \ldots \rangle$ množinu, která je skoro periodická. Pomocí booleovských operací může ze skoro periodických množin vzniknout opět pouze skoro periodická množina. To znamená, že otevřené formule v jazyce L^+_{IAdd} definují pouze skoro periodické množiny. Víme, že každá formule $\varphi(x)$ v jazyce $\{+, 0, 1\}$ je v teorii IAdd^+ ekvivalentní s otevřenou

formulí v jazyce L^{+}_{IAdd}. To znamená, že každá množina definovatelná ve struktuře $\langle \mathrm{Z}, +, 0, 1\rangle$ je skoro periodická. Množina N není skoro periodická, není tedy ve struktuře $\langle \mathrm{Z}, +, 0, 1\rangle$ definovatelná.

Vidíme, že nedefinovatelnost určitých množin lze někdy dokázat pomocí eliminace kvantifikátorů pro jisté teorie. Možná, že význam eliminace kvantifikátorů pro určitou teorii T spočívá především v tom, že poskytuje informaci o množinách definovatelných v modelech teorie T. Řada dalších příkladů definovatelných a nedefinovatelných množin je uvedena ve cvičeních.

Obraťme pozornost k poslední problematice tohoto oddílu i kapitoly, k interpretacím a interpretovatelnosti. Předpokládejme, že T a S jsou axiomatické teorie. Interpretovat teorii T v teorii S znamená vyčlenit v teorii S určité objekty (objekty teorie T „v novém smyslu“) a definovat na těchto objektech operace a relace příslušné k symbolům jazyka teorie T (funkce a predikáty „v novém smyslu“) tak, aby „v novém smyslu“ platily všechny axiomy teorie T. Přitom „vyčlenit“ znamená stanovit formuli $\delta(x)$ v jazyce teorie S zvanou obor interpretace, „definovat“ znamená rozšířit teorii S o definice a „aby platilo“ znamená „dokazatelně v S“.

Než přistoupíme k formulaci definice, ukažme si jednoduchý příklad. Zvolme za S teorii s jazykem $\{<\}$ a s axiomy LO1–LO3, DO1 a DO2. Rozšiřme teorii S o tytéž definice, jako když jsme formulovali teorii DOS: objekt $\mathrm{S}(x)$ je definován jako nejmenší z objektů větších než x a dále objekt 0 je nejmenší z objektů vůbec. Uvnitř takto definovaného rozšíření S' teorie S víme, že různé objekty nemají stejného následníka, 0 není následníkem žádného objektu, konečným nenulovým počtem skoků následnické funkce nelze z žádného objektu x dospět zpět do x. Protože právě vyslovené sentence (jde o axiomy Q1, Q2 a Ln teorie SUCC) jsou univerzální, zůstanou v platnosti, když se omezíme na objekty z jakéhokoliv oboru $\delta(x)$. Jako obor $\delta(x)$ interpretace zvolme formuli

$$\forall y{\leq}x\,(\exists v(v < y) \;\rightarrow\; \exists v(v < y \;\&\; \forall u(u < y \;\rightarrow\; u \leq v))),$$

kde $\leq$ má obvyklý význam menší nebo rovno. Prvkem oboru interpretace čili objektem v novém smyslu je tedy každý objekt x splňující podmínku, že objekt x i všechny menší objekty, kromě ovšem úplně nejmenšího, mají bezprostředního předchůdce. Máme $S' \vdash \forall x(\delta(x) \rightarrow \delta(\mathrm{S}(x))$, obor interpretace je uzavřen na následnickou funkci. Dále máme $S' \vdash \forall x(\delta(x) \;\&\; x \neq 0 \;\rightarrow\; \exists y(\delta(y) \;\&\; x = \mathrm{S}(y)))$, „v novém smyslu platí“ či „v interpretaci platí“ axiom Q3. Definice symbolů 0 a S a obor δ tedy určují interpretaci teorie SUCC v teorii S.

Nechť tedy T a S jsou axiomatické teorie a S' je rozšíření teorie S o definice. Nechť $L(U)$ označuje jazyk libovolné teorie U. Funkce $\sharp$ z $L(T)$ do $L(S')$ je *překlad symbolů*, jestliže zachovává četnost i kategorii symbolů, tj. jestliže každý n-ární funkční či predikátový symbol jazyka $L(T)$ se funkcí $\sharp$ zobrazí opět na n-ární funkční resp. predikátový symbol jazyka $L(S')$. Nechť $\delta(x)$ je formule jazyka $L(S)$ s nejvýše jednou volnou proměnnou x. Řekneme, že funkce $*$ z množiny všech formulí jazyka $L(T)$ do množiny všech formulí jazyka $L(S')$ je *překlad formulí* založený na překladu symbolů $\sharp$ a na oboru $\delta(x)$, jestliže platí:

- je-li φ atomická formule, pak φ^* je formule vzniklá z φ záměnou každého funkčního symbolu F a každého predikátového symbolu P symbolem $F^\sharp$ resp. $P^\sharp$,
- je-li $\bowtie$ libovolná binární logická spojka, pak $(\varphi \bowtie \psi)^*$ je $\varphi^* \bowtie \psi^*$, a dále $(\neg\varphi)^*$ je $\neg\varphi^*$ pro kterékoliv formule φ a ψ jazyka L,
- $(\exists x\varphi)^*$ je $\exists x(\delta(x)\ \&\ \varphi^*)$ a konečně $(\forall x\varphi)^*$ je $\forall x(\delta(x) \to \varphi^*)$ pro kteroukoliv formuli φ jazyka L.

K tomu poznamenejme, že při nahrazování funkčních a predikátových symbolů se nic neděje se symbolem $=$, tj. rovnítko se překládá samo na sebe. Řekneme, že trojice $[S', \sharp, \delta]$, kde S' je rozšíření teorie S o definice, funkce $\sharp : L(T) \to L(S')$ je překlad symbolů a $\delta(x)$ je formule v jazyce $L(S)$, je *interpretace* teorie T v teorii S, jestliže formule δ, překlad symbolů $\sharp$ a překlad formulí $*$ založený na překladu symbolů $\sharp$ a na oboru $\delta(x)$ splňují podmínky:

(i) $S \vdash \exists x\delta(x)$,

(ii) $S' \vdash \forall x_1 .. \forall x_n(\delta(x_1)\ \&\ ..\ \&\ \delta(x_n) \to \delta(F^\sharp(\underline{x})))$ pro libovolný funkční symbol $F \in L(T)$,

(iii) $S' \vdash \varphi^*$ pro libovolný axiom φ teorie T.

Když $[S', \sharp, \delta]$ je interpretace teorie T v teorii S, pak formuli $\delta(x)$ říkáme *obor interpretace* $[S', \sharp, \delta]$. Řekneme, že teorie T je *interpretovatelná* v teorii S, jestliže existuje interpretace teorie T v teorii S.

Příklad 3.6.17 Než jsme formulovali definici interpretace, zdůvodnili jsme, že teorie SUCC je interpretovatelná v teorii S s jazykem $\{<\}$ a axiomy LO1–LO3, DO1 a DO2. Teorie SUCC je ovšem interpretovatelná také v teorii $(S + \mathrm{DO3})$, tj. v teorii DO.

Příklad 3.6.18 Tento příklad je určen čtenářům s jistou znalostí teorie množin. Nechť S je Zermelova-Fraenkelova teorie množin ZF, nechť AR označuje axiom regularity. V ZF definujme posloupnost množin $\{\ p_\alpha\ ;\ \alpha \in \mathrm{On}\ \}$ rekurzí: $p_0 = \emptyset$, dále $p_{\alpha+1} = \mathcal{P}(p_\alpha)$, kde $\mathcal{P}(p_\alpha)$ označuje potenční množinu množiny p_α, a konečně $p_\lambda = \bigcup_{\alpha<\lambda} p_\alpha$, je-li λ limitní. Jako rozšíření S' teorie T o definice volme opět teorii ZF. V tom případě máme jen jednu možnost pro volbu překladu symbolů: $\in^\sharp = \in$. Jako obor interpretace $\delta(x)$ volme formuli $x \in \bigcup_{\alpha\in\mathrm{On}} p_\alpha$. Lze ověřit, že takto definovaná interpretace $[S', \sharp, \delta]$ je interpretací teorie $(\mathsf{ZF} + \mathrm{AR})$ v teorii ZF.

Věta 3.6.19 *Když teorie T je interpretovatelná v teorii S a S je bezesporná, pak i T je bezesporná.*

Důkaz Nechť $[S', \sharp, \delta]$ je interpretace teorie T v teorii S. Pro libovolný term t jazyka $L(T)$ nechť t^* označuje výsledek záměny každého funkčního symbolu F

v termu t symbolem $F^\sharp$. Pišme $\delta(\underline{x})$ místo konjunkce $\delta(x_1)$ & .. & $\delta(x_n)$. Podmínka (ii) v definici interpretace říká, že je-li t term obsahující právě jeden funkční symbol, platí

$$S' \vdash \forall \underline{x}(\delta(\underline{x}) \to \delta(t^*(\underline{x}))). \tag{1}$$

Pro term obsahující nula funkčních symbolů to ovšem platí také. Indukcí podle složitosti termu t lze snadno dokázat, že podmínka (1) platí pro každý term t. Nechť dále $\forall\varphi$ označuje univerzální uzávěr formule φ. Indukcí podle počtu kroků v důkazu formule φ v teorii T lze dokázat, že pro libovolnou formuli φ v $L(T)$ platí implikace

$$T \vdash \varphi \;\Rightarrow\; S' \vdash (\forall\varphi)^*. \tag{2}$$

Ukažme si podrobněji například krok, kdy φ je axiom specifikace tvaru $\forall y\psi \to \psi_x(t)$. Nechť $x_1, .., x_n$ jsou všechny proměnné, které se vyskytují volně ve formuli $\forall y\psi$, nechť $z_1, .., z_k$ jsou všechny proměnné, které se vyskytují v termu t a přitom nejsou mezi $x_1, .., x_n$. Mezi $z_1, .., z_k$ může nebo nemusí být proměnná y. Formule φ má tedy tvar $\forall y\psi(\underline{x}, y) \to \psi(\underline{x}, t(\underline{x}, \underline{z}))$ a formule $(\forall\varphi)^*$ je formule

$$\forall \underline{x}\forall \underline{z}(\delta(\underline{x}) \,\&\, \delta(\underline{z}) \to (\forall y(\delta(y) \to \psi^*(\underline{x}, y)) \to \psi^*(\underline{x}, t^*(\underline{x}, \underline{z})))).$$

Toto je formule dokazatelná v teorii S', neboť uvnitř S' z podmínky (1) víme, že platí-li $\delta(\underline{x})$ a $\delta(\underline{z})$, pak pro $y = t^*(\underline{x}, \underline{z})$ platí $\delta(y)$. Zbývající úvahy v důkazu podmínky (2) jsou podobné a ponecháváme je za cvičení.

Je-li teorie T sporná, pak v T lze dokázat sentenci $\exists x(x \neq x)$. Označme tuto sentenci φ. Podmínka (2) dává $S' \vdash \varphi^*$, tj. $S' \vdash \exists x(\delta(x) \,\&\, x \neq x)$. Protože S' je konzervativní rozšíření teorie S a φ je sentence jazyka $L(S)$, máme $S \vdash \varphi^*$. Evidentně ale platí i $S \vdash \neg\varphi^*$. QED

Pomocí interpretací lze tedy někdy dokázat bezespornost určitých teorií. Přitom je zajímavé, že jde o čistě syntaktickou metodu pro prokazování bezespornosti. To má význam zejména v situaci, kterou naznačuje příklad 3.6.18, při úvahách o „silných“ teoriích, u kterých nemáme k dispozici přímé konstrukce modelů. Fakt, že (ZF + AR) je interpretovatelná v ZF, znamená, že (ZF + AR) je bezesporná teorie, pokud ovšem ZF je bezesporná teorie. Říká se také, že interpretovatelnost teorie (ZF + AR) v ZF znamená *relativní bezespornost* teorie (ZF + AR) vůči teorii ZF. Tvrdíme-li, že nějaká teorie tvaru $(T + \varphi)$ je relativně bezesporná vůči teorii T, říkáme tím, že teorie $(T + \varphi)$ sice může být sporná, nový axiom φ však za případný spor určitě nemůže.

Pojem interpretace není zvlášť stabilním pojmem, v literatuře lze nalézt jeho různé varianty. Například teorie T je lokálně interpretovatelná v teorii S, jestliže každá konečná množina $F \subseteq T$ je (v našem smyslu) interpretovatelná v S. Všimněme si, že věta 3.6.19 by platila i v případě, kdybychom v ní psali „lokálně interpretovatelná“ místo „interpretovatelná“. Jsou možné také interpretace s neabsolutní rovností nebo vícedimenzionální interpretace. Definice interpretace s neabsolutní rovností připouští, aby překladem rovnítka byl nějaký binární predikátový symbol (ne nutně rovnítko); podmínka (iii) v definici interpretace pak zní „$S' \vdash \varphi^*$, kdykoliv

φ je axiom teorie T nebo axiom rovnosti". Definice vícedimenzionální interpretace teorie T v teorii S připouští (požaduje), aby překladem formule s k volnými proměnnými byla formule s $m \cdot k$ volnými proměnnými, tj. aby objekt teorie T byl interpretován jako m-tice objektů teorie S. Náš pojem interpretace byl definován v knize [92] a lze jej označit za globální jednodimenzionální interpretaci s absolutní rovností.

Studium interpretovatelnosti axiomatických teorií a různých variant pojmu interpretace má v pražském či středoevropském prostředí velmi dobrou tradici, viz např. Hájkovy články [33] nebo [30]. Také větu 3.6.22 a související tvrzení uvedené ve cvičení 24 dokázal Petr Hájek. Novější zdroj relevantních odkazů a informací o interpretovatelnosti axiomatických teorií je například Visserův přehledový článek [96]. Protože se však tento článek týká interpretovatelnosti teorií obsahujících nějakou verzi aritmetiky, lze jej doporučit pouze čtenářům, kteří mají představu o obsahu kapitoly 4 a oddílu 5.3 našeho textu.

Řekneme, že *struktura* $\mathbf{A}$ je *definovatelná* ve struktuře $\mathbf{B}$, jestliže nosná množina A struktury $\mathbf{A}$ a realizace $F^{\mathbf{A}}$ a $P^{\mathbf{A}}$ všech funkčních a predikátových symbolů jsou definovatelné množiny ve struktuře $\mathbf{B}$.

Lemma 3.6.20 *Když teorie T je interpretovatelná v teorii S, pak ke každému modelu $\mathbf{M}$ teorie S existuje model $\mathbf{D}$ teorie T, který je definovatelnou strukturou v modelu $\mathbf{M}$.*

Důkaz Nechť $[S', \sharp, \delta]$ je interpretace teorie T v teorii S, nechť $*$ je překlad formulí založený na překladu symbolů $\sharp$ a na oboru δ a nechť je dán model $\mathbf{M}$ teorie S. Za nosnou množinu struktury $\mathbf{D}$ vezměme množinu $D = \{\, a \in m \,;\, \mathbf{M} \models \delta[a] \,\}$. Nechť $F \in L(T)$ je libovolný n-ární funkční symbol. Když $F^\sharp \in L(S)$, vezměme za formuli $\eta(\underline{x}, y)$ formuli $(F(\underline{x}) = y)^*$, tj. formuli $F^\sharp(\underline{x}) = y$. Když $F^\sharp \in L(S') - L(S)$, vezměme za formuli $\eta(\underline{x}, y)$ formuli užitou k definování symbolu $F^\sharp$, tj. tu formuli, která vystupuje v podmínce (d2) věty 3.5.3. V obou případech je formule $\eta(\underline{x}, y)$ formulí jazyka $L(S)$. Definujme realizaci $F^{\mathbf{D}}$ symbolu F jako množinu $\{\, [\underline{a}, b] \,;\, \mathbf{M} \models \eta[\underline{a}, b] \,\}$. Množina $F^{\mathbf{D}}$ je definovatelnou množinou struktury $\mathbf{M}$. Analogicky definujeme realizaci $P^{\mathbf{D}}$ libovolného predikátového symbolu P. Tím jsme získali strukturu $\mathbf{D}$ definovatelnou ve struktuře $\mathbf{M}$. Snadno lze ověřit, že pro libovolnou formuli $\varphi(x_1, .., x_k)$ jazyka $L(T)$ a prvky $a_1, .., a_k \in D$ platí ekvivalence

$$\mathbf{D} \models \varphi[\underline{a}] \;\Leftrightarrow\; \mathbf{M} \models \varphi^*[\underline{a}].$$

Protože $\mathbf{M} \models \varphi^*$ pro libovolný axiom φ teorie T, struktura $\mathbf{D}$ je modelem teorie T. QED

Příklad 3.6.21 Ukažme pomocí lemmatu 3.6.20, že teorie DO není interpretovatelná v teorii SUCC. Vezměme model $\mathbf{M} = \langle \mathrm{N}, 0, \mathrm{s}\rangle + \langle \mathrm{Z}, \mathrm{s}\rangle + \langle \mathrm{Z}, \mathrm{s}\rangle$, tj. model podobný jako na obrázku 3.4.1, ale se dvěma celočíselnými oblastmi. Nechť $\mathbf{D}$ je struktura definovatelná ve struktuře $\mathbf{M}$, která je modelem teorie DO. Modifikací úvahy z cvičení 15, tj. na základě faktu, že teorie SUCC připouští eliminaci

kvantifikátorů, lze zdůvodnit, že každá množina definovatelná ve struktuře $\mathbf{M}$ je buď konečnou podmnožinou oblasti $\langle \mathrm{N}, 0, \mathrm{s}\rangle$, nebo je komplementem takové podmnožiny. Protože každý model teorie DO je nekonečný, pro nosnou množinu D struktury $\mathbf{D}$ platí druhý případ. Množina D tedy obsahuje všechny prvky obou celočíselných oblastí modelu $\mathbf{M}$ (plus skoro všechny prvky oblasti $\langle \mathrm{N}, 0, \mathrm{s}\rangle$). Zvolme prvky a a b různých celočíselných oblastí. Zvolme automorfismus f, pro který platí $f(a) = b$ a $f(b) = a$. Automorfismus f zobrazí každou z obou celočíselných oblastí na druhou z nich a oblast $\langle \mathrm{N}, 0, \mathrm{s}\rangle$ ponechá na místě. Z platnosti axiomů LO2 a LO3 (viz str. 172) ve struktuře $\mathbf{D}$ plyne ekvivalence $a <^{\mathbf{D}} b \Leftrightarrow \neg(b <^{\mathbf{D}} a)$. Použití lemmatu 3.6.14 na relaci $<^{\mathbf{D}}$ dává $[a, b] \in <^{\mathbf{D}} \Leftrightarrow [f(a), f(b)] \in <^{\mathbf{D}}$, tj. $a <^{\mathbf{D}} b \Leftrightarrow b <^{\mathbf{D}} a$. To je spor.

Někdy se píše $S \rhd T$ jako zkratka pro fakt, že teorie T je interpretovatelná v teorii S. Relace $\rhd$ je reflexivní a tranzitivní, a má některé vlastnosti společné s relací $\leq_{\mathrm{m}}$. Vztah $S \rhd T$ můžeme číst „T není o mnoho silnější než S“. Naše příklady říkají, že teorie (ZF + AR) není o mnoho silnější než teorie ZF, kdežto teorie DO je o dost silnější než teorie SUCC. Snadno lze domyslet, že například teorie LO a SUCC jsou vůči relaci $\rhd$ nesrovnatelné.

Nakonec si ukažme, že je-li teorie T konečně axiomatizovatelná, pak tvrzení lemmatu 3.6.20 lze obrátit. To znamená, že pojem interpretace má (alespoň za jistého předpokladu o interpretované teorii) také sémantickou charakterizaci.

Věta 3.6.22 *Nechť T je konečně axiomatizovatelná a nechť ke každému modelu $\mathbf{M}$ teorie S existuje model teorie T, který je definovatelnou strukturou v modelu $\mathbf{M}$. Pak T je interpretovatelná v S.*

Důkaz Nechť $\varphi_1, \ldots, \varphi_m$ jsou všechny axiomy teorie T. Můžeme si myslet, že jazyk $L(T)$ je konečný a že $L(T) = \{P_1, \ldots, P_q, F_1, \ldots, F_r\}$, kde $P_1, \ldots, P_q$ jsou predikátové symboly a $F_1, \ldots, F_r$ jsou funkční symboly. Uvažujme rozšíření S' teorie S o definice a funkci $\sharp$ z $L(T)$ do $L(S')$, která je překladem symbolů. Teorie S' je z teorie S utvořena přidáním axiomů $\gamma_1, \ldots, \gamma_p$, kde každá sentence γ_i má tvar (d1) nebo (d2) z věty 3.5.3, tj. definuje nějaký funkční nebo predikátový symbol pomocí jisté formule ε nebo η, přičemž ε či η je formule v jazyce $L(S \cup \{\gamma_1, \ldots, \gamma_{i-1}\})$. Protože z cvičení 11 předchozího oddílu víme, že každá formule s definovanými symboly je ekvivalentní s formulí v původním jazyce $L(S)$, můžeme si myslet, že formule ε či η je formule v $L(S)$. Překlad $\sharp$ tedy vlastně každému predikátovému (či funkčnímu) symbolu P (či F) četnosti n přiřazuje buď formuli $\varepsilon(x_1, \ldots, x_n)$ (či $\eta(x_1, \ldots, x_n)$) užitou k definici symbolu $P^\sharp$ (či $F^\sharp$), nebo symbol $P^\sharp \in L(S)$ (či symbol $F^\sharp \in L(S)$). V druhém případě si mysleme, že mu přiřazuje formuli $P^\sharp(x_1, \ldots, x_n)$ (či formuli $F^\sharp(x_1, \ldots, x_n) = y$). Rozšíření S' teorie S o definice spolu s překladem symbolů a překladem formulí je tedy vlastně totéž co posloupnost

$$[\varepsilon_1(\underline{x}), \ldots, \varepsilon_q(\underline{x}), \eta_1(\underline{x}, y), \ldots, \eta_r(\underline{x}, y), \delta(x)], \tag{1}$$

přičemž $\underline{x}$ ve formuli $\varepsilon_i(\underline{x})$ znamená $x_1, \ldots, x_{n_i}$, kde n_i je četnost symbolu P_i, a $\underline{x}$ ve formuli $\eta_i(\underline{x}, y)$ znamená $x_1, \ldots, x_{n_{q+i}}$, kde n_{q+i} je četnost symbolu F_i. Naopak,

máme-li posloupnost s formulí tvaru (1), je určeno rozšíření $S(s)$ teorie S o definice, překlad symbolů $\sharp(s)$ a překlad formulí $*(s)$. Můžeme tedy říci, že posloupnost (1) je interpretací (určuje interpretaci) teorie T v teorii S, je-li v S dokazatelná sentence

$$\bigwedge_{i=1}^{r} \forall \underline{x} \exists ! y \eta_i(\underline{x}, y) \,\&\, \bigwedge_{i=1}^{r} \forall \underline{x} \forall y (\delta(\underline{x}) \,\&\, \eta_i(\underline{x}, y) \to \delta(y)) \,\&\, \exists x \delta(x) \,\&\, \bigwedge_{j=1}^{m} \varphi_j^{*(s)}.$$

Označme tuto sentenci $\xi(s)$.

Dále postupujme sporem. Předpokládejme, že T není interpretovatelná v S a současně že pro každý model $\mathbf{M}$ teorie S existuje model $\mathbf{D}$ teorie T, který je definovatelnou strukturou v modelu $\mathbf{M}$. Protože T není interpretovatelná v S, pro každou posloupnost s tvaru (1) je $S, \neg\xi(s)$ bezespornou teorií. Rozmysleme-si, že je-li

$$s_1 = [\underline{\varepsilon}^{(1)}, \underline{\eta}^{(1)}, \delta^{(1)}], \quad s_2 = [\underline{\varepsilon}^{(2)}, \underline{\eta}^{(2)}, \delta^{(2)}], \quad \ldots, \quad s_k = [\underline{\varepsilon}^{(k)}, \underline{\eta}^{(k)}, \delta^{(k)}]$$

libovolná konečná posloupnost posloupností tvaru (1), pak i $S \cup \{\neg\xi(s_1), \ldots, \neg\xi(s_k)\}$ je bezespornou teorií. Když ne, pak $S \vdash \xi(s_1) \vee \ldots \vee \xi(s_k)$. Definujme formuli $\delta(x)$ předpisem

$$\begin{aligned} \delta(x) \equiv (\delta^{(1)}(x) \,\&\, \xi(s_1)) \vee \\ \vee (\delta^{(2)}(x) \,\&\, \neg\xi(s_1) \,\&\, \xi(s_2)) \vee \\ \vdots \\ \vee (\delta^{(k)}(x) \,\&\, \neg\xi(s_1) \,\&\, \ldots \,\&\, \neg\xi(s_{k-1})). \end{aligned} \tag{2}$$

Přitom u posledního řádku si všimněme, že uvnitř teorie S z $\neg\xi(s_1) \& \ldots \& \neg\xi(s_{k-1})$ plyne $\xi(s_k)$. Překlad $F_i^\sharp$ symbolu F_i, kde $1 \leq i \leq r$, definujme předpisem

$$\begin{aligned} F_i(\underline{x}, y) \equiv (\eta_i^{(1)}(\underline{x}, y) \,\&\, \xi(s_1)) \vee \\ \vee (\eta_i^{(2)}(\underline{x}, y) \,\&\, \neg\xi(s_1) \,\&\, \xi(s_2)) \vee \\ \vdots \\ \vee (\eta_i^{(k)}(\underline{x}, y) \,\&\, \neg\xi(s_1) \,\&\, \ldots \,\&\, \neg\xi(s_{k-1})). \end{aligned} \tag{3}$$

Analogicky definujme překlad $P_i^\sharp$, kde $1 \leq i \leq q$, každého predikátového symbolu $P_i \in L(T)$. Z podmínky $S \vdash \bigvee \xi(s_i)$ plyne, že formule (2), r formulí (3) a příslušných q formulí pro predikátové symboly definují interpretaci teorie T v teorii S, což je spor s předpokladem, že T není interpretovatelná v S. Každé rozšíření $S \cup \{\neg\xi(s_1), \ldots, \neg\xi(s_k)\}$ teorie S, kde $s_1, \ldots, s_k$ jsou posloupnosti tvaru (1), je tedy bezesporné. Dle věty o kompaktnosti či věty o silné úplnosti existuje model $\mathbf{M}$ teorie S, ve kterém současně platí všechny sentence $\neg\xi(s)$, kde s je posloupnost tvaru (1). Podle předpokladu existuje model $\mathbf{D}$ teorie T, který je definovatelnou strukturou v $\mathbf{M}$.

Vezměme formuli δ, která ve struktuře $\mathbf{M}$ definuje nosnou množinu struktury $\mathbf{D}$, formule $\varepsilon_1, \ldots, \varepsilon_q$, které definují realizace $P_1^{\mathbf{D}}, \ldots, P_q^{\mathbf{D}}$ predikátových symbolů, a formule $\eta_1, \ldots, \eta_r$, které definují realizace $F_1^{\mathbf{D}}, \ldots, F_r^{\mathbf{D}}$ funkčních symbolů jazyka $L(T)$.

Protože posloupnost $s = [\underline{\varepsilon}, \underline{\eta}, \delta]$ je tvaru (1), máme $\mathbf{M} \models \neg\xi(s)$. Na druhé straně, pro překlad $*$ založený na posloupnosti s a pro libovolnou sentenci ψ v $L(T)$ platí ekvivalence $\mathbf{M} \models \psi^* \Leftrightarrow \mathbf{D} \models \psi$, a to ze stejných důvodů jako v důkazu lemmatu 3.6.20. Protože $\mathbf{D}$ je model teorie T, máme $\mathbf{M} \models \varphi_j^*$ pro libovolný axiom φ_j teorie T. Tedy $\mathbf{M} \models \xi(s)$, spor. QED

Na závěr této kapitoly o predikátové logice je pravděpodobně užitečné připomenout si otázky vyjmenované v Úvodu a uvědomit si, že alespoň na některé nyní umíme uspokojivě odpovědět. Ano, pojem důkazu lze (více způsoby) formálně definovat. Díky tomu můžeme v některých případech ukázat, že určité tvrzení není dokazatelné z daných předpokladů. Za rozumných předpokladů o množině předpokladů existuje algoritmus, který o dané posloupnosti znaků rozhodne, zda je nebo není důkazem, a pro některé struktury existuje algoritmus, který pro danou formuli rozhodne, zda v oné struktuře platí. Nad rámec otázek uvedených v Úvodu také víme, že existují metody, které dovolují dokázat, že určité vlastnosti struktur nejsou vyjádřitelné v daném jazyce, tj. že určité třídy struktur nejsou axiomatizovatelné. Vynořily se ale také otázky, na které odpovědět zatím neumíme. Nevíme například, zda existují konečně axiomatizovatelné nerozhodnutelné teorie. Také jsme se zatím nepokusili axiomatizovat strukturu $\mathbf{N}$ přirozených čísel.

Cvičení

1. Zdůvodněte, že je-li $\mathbf{D}$ konečná struktura pro konečný jazyk, pak $\mathrm{Th}(\mathbf{D})$ je v PSPACE.

2. Zdůvodněte užitím věty 3.6.6, že když nerekurzívní množina v příkladech 3.6.2 a 3.6.3 je navíc rekurzívně spočetná, pak $\mathrm{Thm}(T_1) \in \mathit{RS}$. Pro teorii T_2 ale v tom případě platí $\mathrm{Thm}(T_2) \notin \mathit{RS}$.

3. Zdůvodněte, že z první části předchozího cvičení a z věty 3.6.7 plyne existence teorií, které mají primitivně rekurzívní množinu axiomů a jsou nerozhodnutelné.

4. Když má teorie T jen konečně mnoho úplných rozšíření a všechna jsou rozhodnutelná, pak T je rozhodnutelná. Dokažte.

5. Dokažte na základě předchozího cvičení, že teorie s jazykem $\{<\}$ a axiomy LO1–LO3 a Dn1 je rozhodnutelná.

6. Dokažte, že množina všech totálních aritmetických funkcí, jejichž graf je současně v Σ_2 i v Π_2, je uzavřená na operace substituce a primitivní rekurze.

7. Dokažte, že ke každé rozhodnutelné teorii existuje její rozšíření v tomtéž jazyce, které je úplné a rozhodnutelné.

8. Dokažte, že každá jednoprvková množina je definovatelná ve struktuře $\langle \mathrm{N}, < \rangle$. Nechť dále R je relace $\{\, [x,y] \,;\, |x-y| = 1 \,\}$. Dokažte, že i ve struktuře $\langle \mathrm{N}, R \rangle$ je každá jednoprvková množina definovatelná.

9. Dokažte, že ve struktuře $\langle \mathrm{N}, 0, \mathrm{s}, \cdot \rangle$ je definovatelné sčítání přirozených čísel.

   Návod. Ověřte a využijte implikaci $a{+}b = c \;\Rightarrow\; (1{+}ac)(1{+}bc) = 1{+}c^2(1{+}ab)$.

10. Dokažte, že ve struktuře $\langle \mathrm{N}, +, 0, \mathrm{s}, f \rangle$, kde f je umocňování na druhou (jako funkce jedné proměnné), je definovatelná operace násobení.

11. Která celá čísla jsou definovatelná ve struktuře $\langle \mathrm{Z}, + \rangle$? A která ve struktuře $\langle \mathrm{Z}, +, 0, 1 \rangle$?

12. Dokažte lemma 3.6.14.

13. Když $f : \mathbf{A} \to_0 \mathbf{B}$ a každý prvek struktury $\mathbf{A}$ je definovatelný, pak $f : \mathbf{A} \to_\mathrm{e} \mathbf{B}$. Dokažte.

14. Když $f : \mathbf{A} \to_\mathrm{e} \mathbf{B}$ a $\mathrm{Rng}(f) \neq B$, pak množina $\mathrm{Rng}(f)$ není ve struktuře $\mathbf{B}$ definovatelná. Dokažte. Vyvoďte z předchozích dvou cvičení, že množina N není definovatelná ve struktuře z obrázku 3.4.1.

15. Zdůvodněte, že množina $X \subseteq \mathrm{N}$ je definovatelná ve struktuře $\langle \mathrm{N}, 0, \mathrm{s} \rangle$, právě když X nebo $\mathrm{N} - X$ je konečná množina. Množina všech sudých čísel tedy ve struktuře $\langle \mathrm{N}, 0, \mathrm{s} \rangle$ není definovatelná.

16. Je-li relace $R \subseteq \mathrm{N}^k$ definovatelná ve struktuře $\langle \mathrm{N}, 0, \mathrm{s} \rangle$, pak existuje číslo m takové, že pro každé i a každou volbu čísel $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k$ množina $\{\, b \,;\, [a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k] \in R \,\}$ nebo její komplement má nejvýše m prvků. Dokažte. Platí analogická věta i pro strukturu $\langle \mathrm{N}, 0, \mathrm{s}, < \rangle$? Vyvoďte z toho, že relace $<$ není ve struktuře $\langle \mathrm{N}, 0, \mathrm{s} \rangle$ definovatelná.

17. Vyvoďte z cvičení 16 oddílu 3.5, že je-li $X \subseteq \mathrm{Q}$ definovatelná ve struktuře $\langle \mathrm{Q}, < \rangle$, pak $X = \emptyset$ nebo $X = \mathrm{N}$, a že je-li $X \subseteq \mathrm{Q}^2$ definovatelná ve struktuře $\langle \mathrm{Q}, < \rangle$, pak X je jedna z osmi množin $\emptyset$, $=$, $<$, $\leq$, $\neq$, $>$, $\geq$, Q^2.

18. Zdůvodněte, že každá množina $X \subseteq \mathrm{R}$ definovatelná ve struktuře $\mathbf{R}$ je konečným sjednocením intervalů a jednoprvkových množin, přičemž se ovšem připouštějí i intervaly s nevlastními konci. Množina N tedy ve struktuře $\mathbf{R}$ není definovatelná.

19. Vypracujte všechny vynechané případy v důkazu věty 3.6.19. V kterých z nich se uplatní podmínka $S \vdash \exists x \delta(x)$?

20. Zdůvodněte, že relace $\rhd$ je reflexivní a tranzitivní.

21. Dokažte, že žádná z teorií LO a SUCC není interpretovatelná v druhé.

22. Dokažte, že teorie DO není interpretovatelná v teorii IAdd.

    Návod. Přizpůsobte úvahu o skoro periodických množinách uvedenou za příkladem 3.6.16 pro model $\mathbf{M}$ z cvičení 17 oddílu 3.5. Úvahu z příkladu 3.6.21 pak přizpůsobte pro automorfismus $[a, b] \mapsto [a, -b]$.

23. Dokažte, že ani teorie IAdd není interpretovatelná v teorii DO.

24. Když φ a ψ jsou sentence v jazyce teorie S a teorie T je interpretovatelná v teorii S, φ i v teorii S, ψ, pak T je interpretovatelná i v teorii $S, \varphi \vee \psi$. Dokažte.

25. Dokažte, že když T je rekurzívně axiomatizovatelná, pak $\{\, \varphi \,;\, T \rhd (T + \varphi) \,\}$, tj. množina všech sentencí φ takových, že teorie $T + \varphi$ je interpretovatelná v teorii T, je Σ_3. Když T je konečně axiomatizovatelná, pak $\{\, \varphi ; T \rhd (T + \varphi) \,\}$ je dokonce rekurzívně spočetná.

4

Peanova a Robinsonova aritmetika

Hilbert ... had, if not criteria, guidelines in the selection of axioms. Completeness and simplicity were two desiderata he cited in the introduction to Grundlagen*; consistency was, of course, another. None of these desiderata was entirely unproblematic.* *(C. Smoryński, [81])*

Z dosavadního textu čtenář jistě vytušil, že strukturu **N** přirozených čísel pokládáme za jednu z nejdůležitějších matematických struktur. V této kapitole se budeme zabývat studiem Peanovy aritmetiky PA, kterou lze chápat jako vážný pokus o axiomatizaci struktury **N**. Budeme se ptát, zda jde o pokus úspěšný, a pokud ne, zda lze uspět s nějakou teorií jinou než Peanova aritmetika. K nalezení odpovědí na tyto otázky použijeme některé vědomosti z teorie rekurzívních funkcí.

Budeme se snažit čtenáře přesvědčit, že bez ohledu na to, jak dopadnou odpovědi na tyto otázky, Peanova aritmetika je životaschopnou teorií, která může být pokládána za (jedno z možných) prostředí pro matematickou práci. Na námitku, že jako standardní prostředí pro matematickou práci je většinou přijímána (taková nebo onaká) teorie množin, odpovídáme ano, je tomu tak, ale všechny důležité výsledky, které získáme pro Peanovu aritmetiku, se budou vztahovat i na teorii množin a obecně na všechny axiomatické teorie, ve kterých lze Peanovu aritmetiku interpretovat.

Kromě Peanovy aritmetiky se budeme zabývat také Robinsonovou aritmetikou Q. Brzy zjistíme, že Robinsonova aritmetika je o mnoho slabší teorií než aritmetika Peanova, takže ji nelze považovat za pokus o axiomatizaci struktury **N**. Bude ale zajímavé pozorovat, že některé důležité vlastnosti, které sdílejí Peanova aritmetika a teorie množin, má už Robinsonova aritmetika. Důležitou výhodou Robinsonovy aritmetiky je také to, že má jen konečně mnoho axiomů.

4.1 Axiomy a modely

Peanova a Robinsonova aritmetika jsou axiomatické teorie formulované ve společném aritmetickém jazyce, s kterým jsme se již setkali v kapitole 3. Jde o jazyk

$\{+, \cdot, 0, \mathrm{S}, \leq, <\}$ obsahující dva binární funkční symboly, jednu konstantu, jeden unární funkční symbol a dva binární predikátové symboly. *Robinsonova aritmetika* Q má následujících devět axiomů:

Q1: $\forall x \forall y(\mathrm{S}(x) = \mathrm{S}(y) \rightarrow x = y)$,

Q2: $\forall x(\mathrm{S}(x) \neq 0)$,

Q3: $\forall x(x \neq 0 \rightarrow \exists y(x = \mathrm{S}(y)))$,

Q4: $\forall x(x + 0 = x)$,

Q5: $\forall x \forall y(x + \mathrm{S}(y) = \mathrm{S}(x + y))$,

Q6: $\forall x(x \cdot 0 = 0)$,

Q7: $\forall x \forall y(x \cdot \mathrm{S}(y) = x \cdot y + x)$,

Q8: $\forall x \forall y(x \leq y \equiv \exists v(v + x = y))$,

Q9: $\forall x \forall y(x < y \equiv \exists v(\mathrm{S}(v) + x = y))$.

Peanova aritmetika PA má týchž devět axiomů Q1–Q9 a navíc *schéma indukce*

Ind: $\forall y_1 \ldots \forall y_n(\varphi(0, \underline{y}) \ \& \ \forall x(\varphi(x, \underline{y}) \rightarrow \varphi(\mathrm{S}(x), \underline{y})) \rightarrow \forall x \varphi(x, \underline{y}))$,

kde φ je formule, která nemá jiné volné proměnné než $x, y_1, \ldots, y_n$. Peanova aritmetika má tedy nekonečně mnoho axiomů. Schéma indukce dovoluje vytvořit axiom indukce z libovolné formule φ; tento axiom označme $\mathrm{Ind}(\varphi)$. Proměnným $y_1, \ldots, y_n$ ve formuli $\mathrm{Ind}(\varphi)$ se říká *parametry* a schéma Ind se někdy označuje přesněji jako schéma *parametrické indukce*.

Všimněme si, že v axiomech Q1–Q3 se vyskytují pouze symboly 0 a S, v Q1–Q5 se nevyskytuje násobení, v Q1–Q7 se nevyskytují symboly $\leq$ a $<$ pro uspořádání. Axiomy Q8 a Q9 dávají do souvislosti sčítání a uspořádání a jsou vlastně definicemi symbolů $\leq$ a $<$ (ve smyslu věty 3.5.3). Za „opravdové“ axiomy lze pokládat jen axiomy Q1–Q7. Axiomy Q1–Q3 sdílí Robinsonova i Peanova aritmetika s teorií SUCC z kapitoly 3.

Ukažme si dvě jednoduchá použití axiomu indukce. Nejprve označme $\varphi(x)$ formuli $0 + x = x$ a uvažujme za předpokladu $\varphi(x)$:

> Nechť $0 + x = x$. Pak $\mathrm{S}(0 + x) = \mathrm{S}(x)$. Axiom Q5 dává $\mathrm{S}(0 + x) = 0 + \mathrm{S}(x)$.
> Tedy $0 + \mathrm{S}(x) = \mathrm{S}(x)$.

Tím jsme v Q, a tedy i v PA, dokázali sentenci $\forall x(\varphi(x) \rightarrow \varphi(\mathrm{S}(x)))$. Sentence $\varphi(0)$, tj. sentence $0+0 = 0$, je ovšem také dokazatelná díky axiomu Q4. V axiomu $\mathrm{Ind}(\varphi)$ příslušném k formuli φ jsou tedy dokazatelné obě premisy. Tedy $\mathsf{PA} \vdash \forall x(0+x = x)$. To je ne zcela triviální výsledek, protože zatím nevíme, zda z axiomů Robinsonovy nebo Peanovy aritmetiky plyne komutativita sčítání.

Nyní za $\varphi(x, y, z)$ vezměme formuli $(z + y) + x = z + (y + x)$. Dokazujme v Peanově aritmetice:

Nechť y a z jsou dána. Axiom Q4 dává $\varphi(0,y,z)$. Nechť dále x je dáno a nechť $(z+y)+x = z+(y+x)$. Pak $\mathrm{S}((z+y)+x) = \mathrm{S}(z+(y+x))$. Užijme axiom Q5 jednou na levou stranu: $\mathrm{S}((z+y)+x) = (z+y)+\mathrm{S}(x)$ a dvakrát na pravou stranu: $\mathrm{S}(z+(y+x)) = z+\mathrm{S}(y+x) = z+(y+\mathrm{S}(x))$. Dohromady: $(z+y)+\mathrm{S}(x) = z+(y+\mathrm{S}(x))$. Ověřili jsme, že $\forall x(\varphi(x,y,z) \to \varphi(\mathrm{S}(x),y,z))$. Aplikujeme-li axiom $\mathrm{Ind}(\varphi)$ na y a z, máme $\forall x\varphi(x,y,z)$. Protože čísla y a z byla libovolná, máme $\forall x\forall y\forall z\varphi(x,y,z)$.

Tím jsme v PA lze dokázali asociativitu sčítání. Další vlastnosti aritmetických operací a uspořádání dokazatelné v PA jsou uvedeny v následující větě.

Věta 4.1.1 *Následující sentence jsou dokazatelné v* PA.

(a) Vlastnosti aritmetických operací:

$\forall x\forall y\forall z((z+y)+x = z+(y+x))$, $\quad \forall x\forall y\forall z(z\cdot(y+x) = z\cdot y + z\cdot x)$,
$\forall x(0+x = x)$, $\quad \forall x\forall y\forall z((z\cdot y)\cdot x = z\cdot(y\cdot x))$,
$\forall x\forall y(\mathrm{S}(y)+x = \mathrm{S}(y+x))$, $\quad \forall x(x \neq \mathrm{S}(x))$,
$\forall x\forall y(y+x = x+y)$, $\quad \forall x\forall y\forall z(y+x = z+x \to y = z)$,
$\forall x(0\cdot x = 0)$, $\quad \forall x\forall y(x+y = 0 \to x = 0 \ \&\ y = 0)$,
$\forall x\forall y(\mathrm{S}(y)\cdot x = y\cdot x + x)$, $\quad \forall x\forall y(x\cdot y = 0 \to x = 0 \vee y = 0)$,
$\forall x\forall y(y\cdot x = x\cdot y)$, $\quad \forall x\forall y\exists u(u+x = y \vee u+y = x)$.

(b) Vlastnosti relace $<$:

$\forall x\forall y\forall z(x<y \ \&\ y<z \to x<z)$, $\quad \forall x\forall y(x<y \vee x=y \vee y<x)$.
$\forall x\neg(x<x)$,

(c) Vztah relací $\leq$ a $<$ k sobě navzájem a k operacím:

$\forall x\forall y(x\leq y \equiv x<y \vee x=y)$, $\quad \forall x\forall y\forall z(x<y \to x+z<y+z)$,
$\forall x\forall y(x<\mathrm{S}(y) \equiv x<y \vee x=y)$, $\quad \forall x\forall y\forall z(x<y \ \&\ z\neq 0 \to x\cdot z<y\cdot z)$.

Důkaz Většinu sentencí v (a) lze dokázat indukcí podobně, jako jsme už dokázali první dvě sentence v levém sloupci. „Indukční proměnná“ je v tom případě vždy označena x. Sentence jsou seřazeny, někdy lze využít už dokázané předchozí sentence. Podívejme se třeba na poslední sentenci vpravo dole. Označme $\varphi(x,y)$ formuli $\exists u(u+x = y \vee u+y = x)$ a ukažme si důkaz formule $\forall x(\varphi(x,y)\to\varphi(\mathrm{S}(x),y))$:

Nechť u je takové, že $u+x = y$ nebo $u+y = x$. Když $u+y = x$, pak dle třetí sentence v levém sloupci $\mathrm{S}(u)+y = \mathrm{S}(x)$. Nechť tedy $u+x = y$. Rozlišme ještě případy $u = 0$ a $u \neq 0$. Když $u \neq 0$, pak, podle Q3, $u = \mathrm{S}(v)$ pro jisté v. Tedy $\mathrm{S}(v)+x = y$. Opětovné užití třetí sentence vlevo a axiomu Q5 dává $v+\mathrm{S}(x) = y$. Když $u = 0$, druhá a třetí sentence vlevo dávají $y = x$ a $\mathrm{S}(0)+y = \mathrm{S}(x)$. Ve všech případech tedy lze k jednomu z čísel $\mathrm{S}(x)$ a y přičíst zleva něco tak, aby výsledek byl roven druhému z nich.

Převedeme-li užitím axiomů Q8 a Q9 sentence v (b) a (c) na ekvivalentní sentence neobsahující symboly $\leq$ a $<$, vždy dostaneme sentence, které lze snadno dokázat ze sentencí v (a), a to bez indukce. QED

V PA lze tedy dokázat, že operace s přirozenými čísly a uspořádání mají očekávané vlastnosti: sčítání i násobení jsou asociativní a komutativní operace, násobení je distributivní vůči sčítání, relace $\leq$ a $<$ skutečně jsou neostré a ostré uspořádání, nula je nejmenší přirozené číso, největší přirozené číslo neexistuje, číslo $\mathrm{S}(x)$ je vždy nejmenší mezi čísly většími než x atd.

Existuje několik axiomatických schémat ekvivalentních se schématem indukce. Jedním z nich je *princip nejmenšího prvku*, anglicky *least number principle*: existuje-li nějaké přirozené číslo s určitou vlastností nebo s určitým vztahem k daným parametrům, pak existuje i nejmenší přirozené číslo s onou vlastností nebo s oním vztahem k týmž parametrům:

LNP: $\quad \forall y_1 \,..\, \forall y_n(\exists x \varphi(x,\underline{y}) \;\to\; \exists x(\varphi(x,\underline{y}) \;\&\; \forall v{<}x\, \neg\varphi(v,\underline{y})))$.

Zápis $\forall v{<}x\, \neg\varphi(v,\underline{y})$ je ovšem zkratka pro $\forall v(v < x \;\to\; \neg\varphi(v,\underline{y}))$. Stejně jako u schématu indukce i tady označme $\mathrm{LNP}(\varphi)$ instanci schématu LNP utvořenou z formule φ. V souladu s úmluvou uzavřenou na str. 152 před příkladem 3.1.25 má proměnná v ve formuli $\mathrm{LNP}(\varphi)$ pouze ty výskyty, které jsou naznačeny (tj. v kvantifikátoru $\forall v$, v atomické formuli $v < x$ a dále výskyty v podformuli $\neg\varphi(v,\underline{y})$, které se tam objevily substitucí za proměnnou x), a nemá tedy žádné volné výskyty ve formuli $\varphi(x,\underline{y})$.

Věta 4.1.2 *Teorie s axiomy Q1–Q9,* $\forall x(x < \mathrm{S}(x))$ *a se schématem LNP je ekvivalentní s* PA.

Důkaz Sentence $\forall x(x < \mathrm{S}(x))$ snadno plyne z druhé formule vlevo v 4.1.1(c), a je tedy dokazatelná v PA. Nechť proměnná v se nevyskytuje volně ve formuli $\varphi(x,\underline{y})$. Dokážeme v PA formuli $\mathrm{LNP}(\varphi)$. Vynechme v $\mathrm{LNP}(\varphi)$ kvantifikátory $\forall y_1 \,..\, \forall y_n$ a výslednou formuli pišme v ekvivalentním tvaru

$$\forall x(\forall v{<}x\, \neg\varphi(v,\underline{y}) \;\to\; \neg\varphi(x,\underline{y})) \;\to\; \forall x \neg\varphi(x,\underline{y}).$$

Uvažujme v PA:

Předpokládejme, že pro daná $\underline{y}$ platí

$$\forall x(\forall v{<}x\, \neg\varphi(v,\underline{y}) \;\to\; \neg\varphi(x,\underline{y})). \tag{1}$$

Z implikace $\to$ v druhé formuli vlevo v 4.1.1(c) víme, že před $\mathrm{S}(x)$ není nic jiného než x a čísla menší než x. Tedy

$$\forall x(\forall v{<}x\, \neg\varphi(v,\underline{y}) \;\to\; \forall v{<}\mathrm{S}(x)\, \neg\varphi(v,\underline{y})). \tag{2}$$

Protože neexistují čísla menší než 0 (cvičení), máme také

$$\forall v{<}0\, \neg\varphi(v,\underline{y}). \tag{3}$$

Axiom $\mathrm{Ind}(\forall v{<}x\, \neg\varphi(v,\underline{y}))$ spolu s (2) a (3) dává $\forall x \forall v{<}x\, \neg\varphi(v,\underline{y})$. Z toho dále plyne $\forall x \forall v{<}\mathrm{S}(x)\, \neg\varphi(v,\underline{y})$, a také $\forall x \neg\varphi(x,\underline{y})$, protože mezi čísly v menšími než $\mathrm{S}(x)$ je i x. To jsme měli dokázat.

Nechť nyní formule φ a proměnná x jsou dány. Dokažme formuli $\mathrm{Ind}(\varphi)$ v teorii, jejíž axiomy jsou Q1–Q9, $\forall x(x < \mathrm{S}(x))$ a schéma LNP:

> Nechť $\varphi(0, \underline{y})$ a $\forall x(\varphi(x, \underline{y}) \to \varphi(\mathrm{S}(x), \underline{y}))$. Platí-li $\neg\forall x\varphi(x, \underline{y})$, pak podle $\mathrm{LNP}(\neg\varphi)$ existuje nejmenší číslo, pro které neplatí φ. Označme toto číslo z. Máme tedy $\neg\varphi(z, \underline{y})$ a $\forall v{<}z\,\varphi(v, \underline{y})$. Z $\neg\varphi(z, \underline{y})$ a $\varphi(0, \underline{y})$ plyne $z \neq 0$. Dle Q3 tedy platí $z = \mathrm{S}(u)$ pro jisté u. Takže $\neg\varphi(\mathrm{S}(u), \underline{y})$ a $\forall v{<}\mathrm{S}(u)\,\varphi(v, \underline{y})$. Mezi čísly v menšími než $\mathrm{S}(u)$ je i u. Tedy $\neg\varphi(\mathrm{S}(u), \underline{y})$ a $\varphi(u, \underline{y})$. To je spor s předpokladem $\forall x(\varphi(x, \underline{y}) \to \varphi(\mathrm{S}(x), \underline{y}))$.

QED

O sentenci $\forall x(x < \mathrm{S}(x))$ v tomto okamžiku není zřejmé, je-li dokazatelná s užitím schématu LNP. Zatím není vyloučeno ani to, že je dokazatelná už v Q. O všech případech, kdy jsme dosud použili schéma Ind nebo LNP, vlastně z dosavadního výkladu není zřejmé, že použití některého z těchto schémat bylo nutné.

- *Lze ty sentence z věty 4.1.1, které jsme dokázali užitím schématu Ind, dokázat i bez užití indukce? Jinými slovy, lze je dokázat už v* Q*?*
- *Lze sentenci $\forall x(x < \mathrm{S}(x))$ dokázat v teorii s axiomy Q1–Q9 a se schématem LNP?*

Odpovědi na tyto otázky se ozřejmí ještě v tomto oddílu, jakmile obrátíme pozornost k modelům Robinsonovy aritmetiky.

Před větou 4.1.1 jsme uvedli dva příklady užití axiomu indukce. V druhém z nich jsme axiom indukce utvořili z formule $(z + y) + x = z + (y + x)$, a v příslušném axiomu tedy vystupovaly dva parametry y a z. V prvním příkladu jsme se obešli bez parametrů. Lze se vždy obejít bez parametrů? *Schéma neparametrické indukce* připouští jako axiom každou sentenci tvaru $\varphi(0)\ \&\ \forall x(\varphi(x) \to \varphi(\mathrm{S}(x)) \to \forall x\varphi(x)$, kde formule φ nemá jiné volné proměnné než x.

- *Jsou schémata parametrické a neparametrické indukce navzájem ekvivalentní?*

Na tuto otázku můžeme odpovědět okamžitě.

Věta 4.1.3 *Schémata parametrické a neparametrické indukce jsou nad Robinsonovou aritmetikou ekvivalentní. Jinými slovy, každou instanci schématu parametrické indukce lze dokázat s užitím neparametrické indukce a případně axiomů Q1–Q9.*

Důkaz Mějme axiom indukce $\mathrm{Ind}(\varphi(x, \underline{y}))$ utvořený z formule $\varphi(x, \underline{y})$, která obsahuje parametry $y_1, \ldots, y_n$, kde $n \geq 1$. Tento axiom máme dokázat neparametrickou indukcí. Označme $\psi(z)$ formuli

$$\forall \underline{y}(\varphi(0, \underline{y})\ \&\ \forall x(\varphi(x, \underline{y}) \to \varphi(\mathrm{S}(x), \underline{y})) \to \varphi(z, \underline{y})).$$

Dívejme se na formuli $\varphi(z, \underline{y})$ tak, že reprezentuje systém množin. Pro každou n-tici (formálních) přirozených čísel $y_1, \ldots, y_n$ máme množinu $A_{\underline{y}} = \{\, z\,;\, \varphi(z, \underline{y})\,\}$. Pro

některé n-tice $y_1,\ldots,y_n$ množina $A_{\underline{y}}$ obsahuje nulu a pro některé n-tice $y_1,\ldots,y_n$ je uzavřena na přičítání jedničky. Nastane-li pro $y_1,\ldots,y_n$ obojí, tj. platí-li zároveň $\varphi(0,\underline{y})$ a $\forall x(\varphi(x,\underline{y}) \to \varphi(\mathrm{S}(x),\underline{y}))$, definujme pro účely tohoto důkazu, že množina $A_{\underline{y}}$ je *induktivní*. Formule $\psi(z)$ vyjadřuje, že z je v průniku všech těch $A_{\underline{y}}$, které jsou induktivní. Domluvme se, že znak $\vdash$ ve zbytku tohoto důkazu značí dokazatelnost v teorii s axiomy Q1–Q9 a se schématem neparametrické indukce. Snadno lze dokázat

$$\vdash \psi(0) \quad \text{a} \quad \vdash \forall z(\psi(z) \to \psi(\mathrm{S}(z))).$$

Průnik všech induktivních množin systému $\{A_{\underline{y}};\underline{y}\}$ tedy obsahuje nulu a je uzavřen na přičítání jedničky, a je tedy také induktivní množinou. Formule ψ nemá jiné volné proměnné než z. Neparametrická indukce dává $\vdash \forall z\psi(z)$, tedy

$$\vdash \forall z\forall\underline{y}(\varphi(0,\underline{y}) \;\&\; \forall x(\varphi(x,\underline{y}) \to \varphi(\mathrm{S}(x),\underline{y})) \to \varphi(z,\underline{y})),$$
$$\vdash \forall\underline{y}(\varphi(0,\underline{y}) \;\&\; \forall x(\varphi(x,\underline{y}) \to \varphi(\mathrm{S}(x),\underline{y})) \to \forall z\varphi(z,\underline{y})).$$

Poslední řádek je ekvivalentní s axiomem $\mathrm{Ind}(\varphi(x,\underline{y}))$. Poznamenejme ještě, že axiomy Q1–Q9 jsme v důkazu nepotřebovali. QED

Máme-li sčítání, násobení a uspořádání, můžeme mluvit také o dalších aritmetických pojmech: o dělení, dělitelnosti, prvočíslech a (v příštím oddílu) o nesoudělnosti. Uvidíme, že vlastnosti těchto pojmů lze dokázat v Peanově aritmetice. Domluvme se, že například místo $\mathrm{S}(u)$ budeme raději psát $u+\overline{1}$ a že závorky ve výrazech budeme pokud možno vypouštět: $b\cdot x\cdot u+z$ znamená $((b\cdot x)\cdot u)+z$ nebo $(b\cdot(x\cdot u))+z$ (což je v PA totéž díky vlastnostem operací dokázaným v 4.1.1). Kromě formulí dokázaných v 4.1.1 budeme v důkazech také užívat formule z cvičení 4.

Označme $x \mid y$ formuli $\exists v(v\cdot x = y)$. Lze ji číst „x dělí y“ nebo „číslo y je dělitelné číslem x“. Použitím formule $x \mid y$ utvořme dále formule $\mathsf{Irred}(x)$ a $\mathsf{Prime}(x)$:

$$\mathsf{Irred}(x) \equiv x > \overline{1} \;\&\; \forall v{<}x\,(v \mid x \to v = \overline{1}),$$
$$\mathsf{Prime}(x) \equiv x > \overline{1} \;\&\; \forall u\forall v(x \mid u\cdot v \to x \mid u \vee x \mid v),$$

které čteme číslo x je ireducibilní resp. číslo x je prvočíslo. Postupně v PA dokážeme, že tyto dvě formule jsou spolu ekvivalentní. Nejprve dokažme větu o dělení se zbytkem, která tvrdí, že každé přirozené číslo lze dělit libovolným nenulovým přirozeným číslem. Výsledkem dělení je podíl a zbytek menší než dělitel.

Věta 4.1.4 *V* PA *lze dokázat sentenci* pro každou dvojici čísel x a y, z nichž y je nenulové, existuje právě jedna dvojice čísel u a v tak, že $x = y\cdot u+v$ a přitom $v<y$.

Důkaz Existenci čísel u a v lze snadno dokázat indukcí podle x, tj. s užitím axiomu $\mathrm{Ind}(y\neq 0 \to \exists u\exists v(x = y\cdot u+v \;\&\; v<y))$:

Když $y\neq 0$, pak $0 = 0\cdot y+0 \;\&\; 0<y$.

Když $x = y\cdot u+v \;\&\; v<y$, pak $\mathrm{S}(x) = y\cdot u+\mathrm{S}(v)$. Z $v<y$ plyne $\mathrm{S}(v)<y$ nebo $\mathrm{S}(v)=y$. Pokud $\mathrm{S}(v)<y$, jsme hotovi. Jinak $\mathrm{S}(x) = y\cdot u+y$ a $\mathrm{S}(x) = y\cdot(u+\overline{1})+0$.

Jednoznačnost čísel u a v plyne z formulí dokázaných v 4.1.1 bez dalšího užití indukce:

> Nechť $y \cdot u_1 + v_1 = y \cdot u_2 + v_2$ a přitom $v_1 < y$ a $v_2 < y$. Když $u_1 \neq u_2$, pak $u_1 < u_2$ nebo $u_2 < u_1$. Nechť například $u_1 < u_2$. Pak $u_1 + \overline{1} \leq u_2$ a $y \cdot (u_1 + \overline{1}) \leq y \cdot u_2$. Tedy $y \cdot u_1 + y \leq y \cdot u_2 \leq y \cdot u_2 + v_2 = y \cdot u_1 + v_1$. Z toho plyne $y \leq v_1$, a to je spor.
>
> Platí tedy $u_1 = u_2$ a $y \cdot u_1 + v_1 = y \cdot u_1 + v_2$. Takže $v_1 = v_2$.

QED

Věta 4.1.5 *V* PA *lze dokázat následující vlastnosti relace dělitelnosti:*

(a) $\forall x \forall y \forall z (x \mid y \ \& \ y \mid z \rightarrow x \mid z)$,
(b) $\forall x (x \mid x)$,
(c) $\forall x \forall y (x \mid y \ \& \ y \mid x \rightarrow x = y)$,
(d) $\forall x (\overline{1} \mid x)$,
(e) $\forall x (x \mid 0)$,
(f) $\forall x \forall y \forall z (x \mid y \rightarrow x \cdot z \mid y \cdot z)$,
(g) $\forall x \forall y \forall z (x \cdot z \mid y \cdot z \ \& \ z \neq 0 \rightarrow x \mid y)$,
(h) $\forall x \forall y (x \mid x \cdot y)$,
(i) $\forall x \forall y \forall v (v \mid x \ \& \ v \mid y \rightarrow v \mid (x + y))$,
(j) $\forall x \forall y \forall z (x \mid x \cdot z + y \rightarrow x \mid y)$.

Důkaz Trochu obtížnější je jen (j):

> Nechť $x \cdot v = x \cdot z + y$. Když $x = 0$, pak $x \cdot z + y = 0$, takže $y = 0$ a $x \mid y$. Nechť tedy $x \neq 0$. Nemůže platit $v < z$, jinak bychom měli $x \cdot v < x \cdot z \leq x \cdot z + y = x \cdot v$. Tudíž $z \leq v$, čili existuje u takové, že $z + u = v$. Pak $x \cdot (z + u) = x \cdot z + y$, takže $x \cdot u = y$ a $x \mid y$.

QED

Klasický důkaz tvrzení, že množina všech prvočísel je nekonečná, tj. že ke každému y existuje prvočíslo, které je větší než y, je založen na myšlence uvažovat rozklad čísla $y! + 1$ na prvočísla. V Peanově aritmetice (zatím) nemůžeme mluvit o funkcích, jako je faktoriál nebo mocnina. Vlastnost „býti prvočíslem“ jsme už v aritmetickém jazyce zapsali, ale tvrzení „každé přirozené číslo je součinem prvočísel“ zapsat (také zatím) neumíme. Přesto uvidíme, že obě potíže jsou překonatelné a že klasický důkaz tvrzení, že prvočísel je nekonečně mnoho, je formalizovatelný v PA. Místo o faktoriálu čísla y postačí mluvit o čísle dělitelném všemi čísly $2, 3, \ldots, y$. A tvrzení, že každé číslo má prvočíselný rozklad, postačí nahradit tvrzením, že každé číslo je dělitelné nějakým prvočíslem. O tom jsou body (a) a (b) následujícího lemmatu. Bod (c) použijeme v důkazu tvrzení 4.1.7(b).

Lemma 4.1.6 *V* PA *lze dokázat sentence*
(a) $\forall y \exists z (z \neq 0 \ \& \ \forall v \leq y (v \neq 0 \rightarrow v \mid z))$,
(b) $\forall w (w > \overline{1} \rightarrow \exists x (\mathsf{Irred}(x) \ \& \ x \mid w))$,
(c) $\forall a \neq 0 \forall b \forall z (\exists x \exists y (a \cdot x + z = b \cdot y) \rightarrow \exists x \exists y (b \cdot x + z = a \cdot y))$.

Důkaz Tvrzení (a) lze dokázat přímočaře indukcí podle y. V důkazu tvrzení (b) použijeme schéma LNP:

Nechť w_0 je nejmenší z čísel větších než $\overline{1}$, která nejsou dělitelná žádným ireducibilním číslem. Protože $w_0 \mid w_0$, číslo w_0 samo není ireducibilní. Tedy existuje $v < w_0$ takové, že $v \mid w_0$ a $v > \overline{1}$. Protože w_0 je nejmenší, v je dělitelné nějakým ireducibilním x. Relace $\mid$ je tranzitivní, tedy $x \mid w_0$. To je spor s předpokladem, že w_0 není dělitelné ireducibilním číslem.

Dokažme tvrzení (c):

Nechť $a \cdot x + z = b \cdot y$. Z $a \neq 0$ plyne $y \leq y \cdot a$. Vezměme v takové, že $v + y = y \cdot a$, a spočítejme číslo $(b \cdot v + z) + a \cdot x$:

$$b \cdot v + z + a \cdot x = b \cdot v + b \cdot y = b \cdot (v + y) = b \cdot y \cdot a.$$

Tedy $a \mid ((b \cdot v + z) + a \cdot x)$. Podle 4.1.5(j) platí $a \mid ((b \cdot v) + z)$. Tedy existuje u takové, že $b \cdot v + z = a \cdot u$.

QED

Věta 4.1.7 *V Peanově aritmetice lze dokázat sentence*
(a) $\forall y \exists x (y < x \ \&\ \mathsf{Irred}(x))$,
(b) $\forall a \neq 0 \forall b \neq 0 \exists x \exists y \exists z (a \cdot x + z = b \cdot y \ \&\ z \mid a \ \&\ z \mid b)$,
(c) $\mathsf{PA} \vdash \forall x (\mathsf{Irred}(x) \equiv \mathsf{Prime}(x))$.

Důkaz (v PA) (a) Nechť y je dáno. Díky tvrzení 4.1.6(a) můžeme vzít číslo $z \neq 0$, které je dělitelné všemi čísly $2, 3, \ldots, y$. Je-li $v \leq y$ a $v \neq 0$, pak $z + \overline{1}$ lze psát ve tvaru $z + \overline{1} = u \cdot v + \overline{1}$. Je-li navíc $v > \overline{1}$, pak díky jednoznačnosti dělení se zbytkem, viz 4.1.4, nelze číslo $z + \overline{1}$ psát ve tvaru $u \cdot v$. Tedy žádné v takové, že $v > \overline{1}$ a $v \leq y$, nedělí $z + \overline{1}$. To znamená, že pro každé ireducibilní číslo x takové, že $x \mid (z + \overline{1})$, platí $x > y$. Podle 4.1.6(b) taková x existují.

(b) Nechť čísla a a b různá od nuly jsou dána. Jistě existují nějaká čísla z splňující podmínku

$$z \neq 0 \ \&\ \exists x \exists y (a \cdot x + z = b \cdot y), \tag{1}$$

například $a \cdot 0 + b = b \cdot \overline{1}$. Dle principu LNP můžeme vzít nejmenší z_0 splňující podmínku (1). Navíc platí

$$z_0 \leq b. \tag{2}$$

Podle 4.1.6(c) je číslo z_0 zároveň nejmenším číslem z splňujícím podmínku

$$z \neq 0 \ \&\ \exists x \exists y (b \cdot x + z = a \cdot y). \tag{3}$$

Vezměme x_0 a y_0 taková, že

$$a \cdot x_0 + z_0 = b \cdot y_0. \tag{4}$$

Protože $z_0 \neq 0$, můžeme dělit číslo b se zbytkem číslem z_0:

$$b = z_0 \cdot u + v \ \&\ v < z_0. \tag{5}$$

Z (2) plyne $u \neq 0$ a z (4) máme $y_0 \neq 0$. Existuje tedy číslo w takové, že $\mathrm{S}(w) = y_0 \cdot u$. Vyjděme z (4) a (5) a počítejme:

$$\begin{aligned} a \cdot x_0 \cdot u + z_0 \cdot u &= b \cdot y_0 \cdot u \\ a \cdot x_0 \cdot u + z_0 \cdot u + v &= b \cdot y_0 \cdot u + v \\ a \cdot x_0 \cdot u + b &= b \cdot (w + \overline{1}) + v \\ a \cdot x_0 \cdot u &= b \cdot w + v. \end{aligned}$$

Kdyby platilo $v \neq 0$, číslo v by bylo menším číslem než z_0 splňujícím podmínku (3). Tedy $v = 0$ a z (5) plyne $z_0 \mid b$. Podobně (o něco jednodušeji) lze ověřit i $z_0 \mid a$.

(c) Nechť $x > \overline{1}$ a $x \mid a \cdot b$. Můžeme předpokládat $a \neq 0$, jinak $x \mid a$. Dle tvrzení (b) existují u, v a z taková, že $x \cdot u + z = a \cdot v$ a přitom $z \mid x$ a $z \mid a$. Je-li x ireducibilní, pak $z = x$ nebo $z = \overline{1}$. Když $z = x$, pak $x \mid a$. Když $z = \overline{1}$, pak $x \cdot u + \overline{1} = a \cdot v$ a $x \cdot u \cdot b + b = a \cdot b \cdot v$. Z 4.1.5(j) plyne $x \mid b$. Důkaz implikace $\leftarrow$ ponecháváme za cvičení. QED

Platí-li pro číslo z rovnost $a \cdot x + z = b \cdot y$, pak dle tvrzení 4.1.5(j) je z dělitelné všemi společnými děliteli čísel a a b. Je-li z takové jako v tvrzení (b) věty 4.1.7, tj. splňuje-li navíc podmínky $z \mid a$ a $z \mid b$, pak z je největším společným dělitelem čísel a a b. Tvrzení 4.1.7(b) je známo jako *Bezoutova věta*. Její důkaz je odvozen z Eukleidova algoritmu pro nalezení největšího společného dělitele, který pracuje takto: máme-li nalézt největší společný dělitel čísel a a b, položíme $d_0 := \max\{a, b\}$, $d_1 := \min\{a, b\}$, a dále vždy $d_{n+2} :=$ zbytek po dělení čísla d_n číslem d_{n+1}; poslední nenulové d_n je hledaný největší společný dělitel.

Bezoutova věta by se trochu snáz formulovala a dokazovala v teorii celých čísel (kdybychom ovšem nějakou zavedli). To bychom pracovali s číslem z tvaru $a \cdot x + b \cdot y$, které má nejmenší možnou nenulovou absolutní hodnotu, a obešli bychom se bez tvrzení 4.1.6(c).

Přemýšlejme nyní o modelech teorií Q a PA. V příkladu 3.1.25 jsme dokázali, že ve struktuře $\mathbf{N} = \langle \mathrm{N}, +, \cdot, 0, \mathrm{s}, \leq, < \rangle$ platí všechny instance schématu Ind. Je jasné, že v $\mathbf{N}$ platí také všechny axiomy Q1–Q9. To znamená, že struktura $\mathbf{N}$ je modelem jak Robinsonovy, tak Peanovy aritmetiky, a platí

$$\mathrm{Thm}(\mathsf{Q}) \subseteq \mathrm{Thm}(\mathsf{PA}) \subseteq \mathrm{Th}(\mathbf{N}).$$

Struktura $\mathbf{N}$ se nazývá *standardní model aritmetiky*. Teorie $\mathrm{Th}(\mathbf{N})$ je *teorie standardního modelu* nebo též *úplná aritmetika* (anglicky *true arithmetic*). Strukturám pro aritmetický jazyk, které nejsou izomorfní se strukturou $\mathbf{N}$, říkáme *nestandardní*.

Než se zamyslíme nad nestandardními strukturami a modely, formulujme první z řady tvrzení (další se objeví v následujících oddílech) o definovatelnosti množin a relací ve struktuře $\mathbf{N}$. Připomeňme, že pro libovolný numerál $\overline{n}$ platí $\overline{n}^{\mathbf{N}} = n$, číslo n je hodnotou numerálu $\overline{n}$ ve standardním modelu aritmetiky. To dále dle lemmatu 3.1.14 znamená, že je-li $\varphi(x_1, \ldots, x_k)$ libovolná aritmetická formule, pak podmínky $\mathbf{N} \models \varphi(\underline{x})[n_1, \ldots, n_k]$ a $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_k})$ jsou navzájem ekvivalentní.

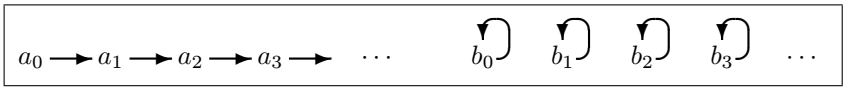
Lemma 4.1.8 *Formule $x \mid y$ definuje v* $\mathbf{N}$ *relaci* $\{[n,m]; n \text{ dělí } m\}$. *Obě formule* $\mathsf{Irred}(x)$ *a* $\mathsf{Prime}(x)$ *definují v* $\mathbf{N}$ *množinu všech prvočísel.*

Důkaz Pro libovolná dvě přirozená čísla n a m platí

$$\begin{aligned} \mathbf{N} \models \overline{n} \mid \overline{m} &\Leftrightarrow \mathbf{N} \models \exists v(v \cdot \overline{n} = \overline{m}) \\ &\Leftrightarrow \exists k \in \mathrm{N}(\mathbf{N} \models \overline{k} \cdot \overline{n} = \overline{m}) \\ &\Leftrightarrow \exists k \in \mathrm{N}(k \cdot n = m) \\ &\Leftrightarrow n \text{ dělí } m. \end{aligned}$$

Použili jsme podmínky T8, T3 a T2 z definice 3.1.9 a dále fakty, že hodnoty termů $\overline{k}$, $\overline{n}$ a $\overline{m}$ jsou čísla k, n a m a že symboly „$\cdot$“ a „$=$“ jsou v $\mathbf{N}$ realizovány násobením přirozených čísel a rovností.

Úvaha pro formuli $\mathsf{Irred}(x)$ je zcela analogická. Protože formule $\mathsf{Irred}(x)$ a $\mathsf{Prime}(x)$ jsou v PA ekvivalentní, definují v $\mathbf{N}$ (a v jakémkoliv jiném modelu Peanovy aritmetiky také) tutéž množinu. QED



$+$	a_m	b_m
a_n	a_{n+m}	b_{m+1}
b_n	b_n	b_{m+1}

$\cdot$	a_0	a_{m+1}	b_m
a_n	a_0	$a_{n\cdot(m+1)}$	b_0
b_n	a_0	b_{n+1}	b_{n+1}

Obrázek 4.1.1: Nestandardní model Robinsonovy aritmetiky

Na obrázku 4.1.1 je znázorněna struktura $\mathbf{M}$ pro aritmetický jazyk, kterou navrhla Marta Vlasáková (tehdy Bendová). Nosná množina M struktury $\mathbf{M}$ je sjednocením dvou disjunktních nekonečných spočetných množin $\{a_0, a_1, a_2, \dots\}$ a $\{b_0, b_1, b_2, \dots\}$. Realizace následnické funkce je znázorněna šipkami, operace jsou definovány tabulkami, a_0 realizuje symbol 0. Relace $\leq^{\mathbf{M}}$ a $<^{\mathbf{M}}$ znázorněny nejsou, protože jsou jednoznačně určeny sčítáním. Snadno lze ověřit $\mathbf{M} \models \mathsf{Q}$ (cvičení).

Sentence $\forall x \forall y(x + y = y + x)$ v $\mathbf{M}$ neplatí (například protože $a_0 +^{\mathbf{M}} b_0$ se liší od $b_0 +^{\mathbf{M}} a_0$). Komutativitu sčítání — a také většinu sentencí dokázaných ve větě 4.1.1, jak uvidíme ve cvičeních — nelze dokázat v Robinsonově aritmetice, a indukce nebo jiné dodatečné axiomy jsou tedy k jejich důkazu nutné.

Rozmysleme si, jak je v $\mathbf{M}$ realizováno uspořádání. Protože $b_m +^{\mathbf{M}} a_n = b_m$, každý z prvků a_n je ve smyslu relace $<^{\mathbf{M}}$ menší než kterýkoliv z prvků b_m. Z tabulky definující sčítání modelu $\mathbf{M}$ je dále zřejmé, že ve smyslu relace $<^{\mathbf{M}}$ před a_n jsou

prvky $a_0, \ldots, a_{n-1}$, a žádné jiné, před b_0 jsou všechny standardní prvky, a žádné jiné, před b_{n+1} je b_n, všechny standardní prvky, a žádné jiné. Relace $<^{\mathbf{M}}$ není tranzitivní: pro libovolné n platí $b_n <^{\mathbf{M}} b_{n+1}$ a $b_{n+1} <^{\mathbf{M}} b_{n+2}$, neplatí ale $b_n <^{\mathbf{M}} b_{n+2}$.

Nechť $\varphi(x, y_1, \ldots, y_k)$ je aritmetická formule a nechť $d_1, \ldots, d_k \in M$ jsou taková, že $\mathbf{M} \models (\exists x \varphi(x, \underline{y}))[\underline{d}]$. Kromě relace $<^{\mathbf{M}}$ máme na M ještě jedno uspořádání, označme je R, definované takto: $a_n \; R \; a_m \Leftrightarrow n < m$, dále $b_n \; R \; b_m \Leftrightarrow n < m$, a konečně $a_n \; R \; b_m$ pro každé n a m. Relace R je dobré uspořádání množiny M typu $\omega + \omega$. Nechť c je R-nejmenší prvek množiny M, splňující $\mathbf{M} \models \varphi(x, \underline{y})[c, \underline{d}]$. Vzhledem k tomu, že všechny $<^{\mathbf{M}}$-menší prvky než c jsou mezi těmi, které jsou R-menší než c, máme $\mathbf{M} \models (\varphi(x, \underline{y}) \;\&\; \forall v{<}x \neg\varphi(v, \underline{y}))[c, \underline{d}]$. Tím jsme ověřili, že v $\mathbf{M}$ platí schéma LNP. Struktura $\mathbf{M}$ je tedy nestandardním modelem teorie $(\mathsf{Q} + \mathrm{LNP})$. Sentence $\forall x(x < \mathrm{S}(x))$ v $\mathbf{M}$ neplatí. To znamená, že ji v Q nelze dokázat ani užitím schématu LNP.

Obraťme pozornost od Robinsonovy aritmetiky k teoriím PA a $\mathrm{Th}(\mathbf{N})$. Mají i tyto teorie nějaké nestandardní modely? Naše dosavadní výsledky dovolují zdůvodnit, že určitě ano. Především, dle Löwenheimovy-Skolemovy věty 3.4.5 mají obě tyto teorie modely všech nekonečných mohutností. Protože nespočetná struktura pro aritmetický jazyk jistě není izomorfní s $\mathbf{N}$, teorie PA a $\mathrm{Th}(\mathbf{N})$ (a ovšem i Q) mají nestandardní modely všech nespočetných mohutností. Dále, dle věty 3.4.3 má teorie $\mathrm{Th}(\mathbf{N})$ spočetný model $\mathbf{M}$ takový, že $\langle M, <^{\mathbf{M}}\rangle$ není dobře uspořádaná množina. A takový model $\mathbf{M}$ je spočetným nestandardním modelem jak teorie $\mathrm{Th}(\mathbf{N})$, tak Peanovy aritmetiky.

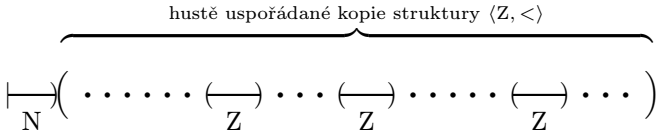
Udělejme si bližší představu o struktuře nestandardního modelu Peanovy aritmetiky, a tím i o struktuře nestandardního modelu teorie $\mathrm{Th}(\mathbf{N})$. Nechť tedy $\mathbf{M}$ je nestandardní model Peanovy aritmetiky. $\mathbf{M}$ je struktura se třemi operacemi, s prvkem $0^{\mathbf{M}}$, který je realizací symbolu 0, a s relacemi $\leq^{\mathbf{M}}$ a $<^{\mathbf{M}}$, které jsou realizacemi symbolů $\leq$ a $<$. Protože v PA lze dokázat, že relace $<$ je uspořádání, musí to platit v každém modelu: $<^{\mathbf{M}}$ je tranzitivní, antireflexivní a trichotomická relace na nosné množině M struktury $\mathbf{M}$. Z podobného důvodu $0^{\mathbf{M}}$ je $<^{\mathbf{M}}$-nejmenší prvek množiny M, největší prvek neexistuje.

Domluvme se, že řekneme-li v následujících odstavcích o prvcích množiny M, že jsou menší nebo větší, znamená to menší nebo větší ve smyslu relace $<^{\mathbf{M}}$.

Pro každé $a \in M$ platí, že a je největší z prvků menších než $\mathrm{S}(a)$ a $\mathrm{S}(a)$ je nejmenší z prvků větších než a. To znamená, že struktura $\langle M, <^{\mathbf{M}}\rangle$ je modelem teorie DO z oddílu 3.4 a platí o ní všechny fakty, o kterých z příkladu 3.4.14 víme, že platí o modelech teorie DO. Zopakujme si je. Na množině M můžeme definovat ekvivalenci „blízkosti“: $a \sim b$, jestliže mezi a a b je jen konečně mnoho prvků. Třída ekvivalence obsahující $0^{\mathbf{M}}$ je izomorfní se strukturou $\langle \mathrm{N}, <\rangle$, je tedy uspořádanou množinou typu ω. Každá jiná třída ekvivalence je izomorfní se strukturou $\langle \mathrm{Z}, <\rangle$, je tedy uspořádanou množinou typu $\omega^* + \omega$. Protože model $\mathbf{M}$ je nestandardní, faktorová množina $M/{\sim}$ má více než jeden prvek. Třídu ekvivalence (tj. prvek množiny $M/{\sim}$) obsahující prvek $a \in M$ značíme $[a]$. Na množině $M/{\sim}$ můžeme definovat relaci R předpisem $[a] \; R \; [b] \Leftrightarrow a < b \;\&\; \neg(a \sim b)$. Struktura $\langle M/{\sim}, R\rangle$ je lineárně uspořádanou množinou, $[0^{\mathbf{M}}]$ je její nejmenší prvek. Lze tedy říci, že

struktura $\langle M, <^{\mathbf{M}}\rangle$ je lineárně uspořádanou množinou typu $\omega + (\omega^* + \omega) \cdot \lambda$, kde λ je lineární uspořádání s nejmenším prvkem. Strukturu $\langle M, <^{\mathbf{M}}\rangle$ tedy lze popsat jako strukturu, která vznikla z nějaké lineárně uspořádané množiny s nejmenším prvkem tak, že nejmenší prvek byl nahrazen strukturou $\langle \mathrm{N}, <\rangle$ a všechny ostatní prvky byly nahrazeny strukturou $\langle \mathrm{Z}, <\rangle$.

Prvkům třídy ekvivalence $[0^{\mathbf{M}}]$ říkáme *standardní prvky* modelu $\mathbf{M}$. Standardní prvky modelu $\mathbf{M}$ jsou právě ty prvky, které jsou realizacemi numerálů. Před realizací libovolného numerálu $\overline{n}$ je v modelu $\mathbf{M}$ právě n menších prvků, totiž prvky $0^{\mathbf{M}}, \overline{1}^{\mathbf{M}}, \ldots, \overline{n-1}^{\mathbf{M}}$. Prvkům, které nejsou realizacemi numerálů, říkáme *nestandardní prvky* modelu $\mathbf{M}$. Nestandardní prvek modelu $\mathbf{M}$ není dosažitelný z nejmenšího prvku $0^{\mathbf{M}}$ konečně mnoha skoky funkce $\mathrm{S}^{\mathbf{M}}$ a ve smyslu uspořádání před ním existuje nekonečně mnoho jiných prvků.



Obrázek 4.1.2: Uspořádání nestandardního modelu Peanovy aritmetiky

Redukt $\langle M, <^{\mathbf{M}}\rangle$ našeho modelu $\mathbf{M}$ pro jazyk $\{<\}$ má kromě vlastností, které musí mít každý model teorie DO, ještě další vlastnosti, které plynou z faktu, že uspořádání $<^{\mathbf{M}}$ má úzký vztah ke sčítání $+^{\mathbf{M}}$. Vezměme prvky a a b modelu $\mathbf{M}$ takové, že $a < b$ a $\neg(a \sim b)$. V PA lze dokázat sentenci

$$\forall x \forall y (x < y \;\rightarrow\; \exists z (x + \overline{2} \cdot z = y \;\vee\; x + \overline{2} \cdot z + \overline{1} = y)).$$

To znamená, že k a a b existuje prvek d takový, že $a + \overline{2} \cdot d = b$ nebo $a + \overline{2} \cdot d + \overline{1} = b$. Protože a a b si nejsou blízké, jejich vzdálenost $\overline{2} \cdot d$ nebo $\overline{2} \cdot d + \overline{1}$ je nestandardní prvek modelu $\mathbf{M}$. Protože $\overline{2} \cdot d = d + d$, i d je nestandardní prvek, a tedy prvek $a + d$ není blízký k a ani k b. Struktura $\langle M, <^{\mathbf{M}}\rangle$ je tudíž typu $\omega + (\omega^* + \omega) \cdot \lambda$, kde λ je *hustě* uspořádaná množina. Podobně lze zdůvodnit, že λ nemá největší prvek. Můžeme tedy shrnout, že z hlediska uspořádání náš nestandardní model $\mathbf{M}$ Peanovy aritmetiky vypadá tak, jak je znázorněno na obrázku 4.1.2: v nějaké lineárně hustě uspořádané množině s nejmenším a bez největšího prvku byl nejmenší prvek nahrazen kopií struktury $\langle \mathrm{N}, <\rangle$ a každý jiný prvek byl nahrazen kopií struktury $\langle \mathrm{Z}, <\rangle$, čímž vznikla struktura typu $\omega + (\omega^* + \omega) \cdot \lambda$, kde λ je husté uspořádání bez nejmenšího a největšího prvku. Víme, že *spočetná* hustě lineárně uspořádaná struktura bez nejmenšího a největšího prvku je až na izomorfismus jen jedna (viz příklad 3.4.12). To znamená, že je-li model $\mathbf{M}$ navíc spočetný, pak struktura $\langle M, <^{\mathbf{M}}\rangle$ má jediný možný tvar $\omega + (\omega^* + \omega) \cdot \eta$, kde η značí strukturu $\langle \mathrm{Q}, <\rangle$ racionálních čísel s uspořádáním.

Nic podobně přehledného nedokážeme říci o sčítání a násobení modelu $\mathbf{M}$. Navíc z věty 4.1.9 plyne, že sčítání a násobení modelu $\mathbf{M}$ není jednoznačně určeno jeho

uspořádáním. V modelu $\mathbf{M}$ ale musí platit všechny formule, které jsou dokazatelné v PA. To například znamená, že za každým prvkem modelu $\mathbf{M}$ existují prvky, o kterých v $\mathbf{M}$ platí, že jsou prvočísly. V $\mathbf{M}$ tedy existují nestandardní prvočísla!

Lze zjistit *počet* neizomorfních nestandardních modelů Peanovy aritmetiky? Třída všech spočetných modelů PA není množinou. Ale: každý spočetný model je izomorfní s modelem, který má jednu předem danou nosnou množinu. Můžeme tedy nosnou množinu D považovat za pevně zvolenou a uvažovat o izomorfních a neizomorfních modelech Peanovy aritmetiky s nosnou množinou D. A v této situaci už má dobrý smysl ptát se na mohutnost. Například realizace symbolu $\leq$ je podmnožina množiny $D \times D$ a takových podmnožin je $2^{|D\times D|} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$. Podobně lze odhadnout počet možností, jak zvolit realizace ostatních pěti symbolů aritmetického jazyka. Horní odhad pro počet všech (izomorfních i neizomorfních) modelů jak Peanovy aritmetiky, tak teorie $\mathrm{Th}(\mathbf{N})$, s předem danou nosnou množinou, která je nekonečná spočetná, je

$$2^{\aleph_0^3} \cdot 2^{\aleph_0^3} \cdot \aleph_0 \cdot 2^{\aleph_0^2} \cdot 2^{\aleph_0^2} \cdot 2^{\aleph_0^2} = 2^{\aleph_0},$$

kde jednotlivé činitele vyjadřují počet možností, jak zvolit realizace symbolů $+$, $\cdot$, 0, S, $\leq$ a $<$. Na první pohled by se mohlo zdát, že počítáme zbytečně velkoryse. Následující věta ale tvrdí, že ne, $2^{\aleph_0}$ je optimální horní odhad.

Věta 4.1.9 *Teorie* $\mathrm{Th}(\mathbf{N})$ *má* $2^{\aleph_0}$ *navzájem neizomorfních spočetných modelů.*

Důkaz Označme P množinu všech prvočísel a zvolme její podmnožinu X. Máme $2^{\aleph_0}$ možností, jak zvolit tuto množinu X.

Další postup je podobný, jako v důkazu o neaxiomatizovatelnosti dobrého uspořádání: přidat k jazyku dočasně další symboly, formulovat teorii v takto rozšířeném jazyce a užít větu o kompaktnosti k důkazu, že ona teorie má nějaké modely. Z dočasných dodatečných symbolů tentokrát vystačíme s jedinou konstantou.

Považujme tedy teorii $\mathrm{Th}(\mathbf{N})$ za teorii v jazyce $\{+, \cdot, 0, \mathrm{S}, \leq, <, c\}$, kde c je konstanta, označme S_X množinu sentencí

$$\{\, \overline{n} \mid c \,;\, n \in X \,\} \cup \{\, \neg(\overline{n} \mid c) \,;\, n \in P - X \,\}$$

a uvažujme o teorii $\mathrm{Th}(\mathbf{N}) \cup S_X$. Nechť $p_1, \ldots, p_n$ jsou libovolné prvky množiny X. Je jasné, a případně to také plyne z tvrzení 4.1.7(c) a faktu, že $\mathbf{N} \models \mathsf{PA}$, že součin $r = \prod_{i=1}^{n} p_i$ je dělitelný všemi čísly $p_1, \ldots, p_n$, ale *není dělitelný* žádným prvočíslem různým od všech $p_1, \ldots, p_n$. Číslo r tedy není dělitelné žádným prvkem množiny $P - X$. To znamená, že sestrojíme-li expanzi struktury $\mathbf{N}$ pro jazyk $\{+, \cdot, 0, \mathrm{S}, \leq, <, c\}$ tak, že konstantu c realizujeme prvkem r, dostaneme model teorie

$$\mathrm{Th}(\mathbf{N}) \cup \{\, \overline{p_i} \mid c \,;\, 1 \leq i \leq n \,\} \cup \{\, \neg(\overline{n} \mid c) \,;\, n \in P - X \,\}.$$

Ověřili jsme, že teorie $\mathrm{Th}(\mathbf{N}) \cup F \cup \{\, \neg(\overline{n} \mid c) \,;\, n \in P - X \,\}$ má model pro každou konečnou podmnožinu F množiny $\{\, \overline{n} \mid c \,;\, n \in X \,\}$. Tím spíše každá

konečná množina $F \subseteq \mathrm{Th}(\mathbf{N}) \cup S_X$ má model. Podle věty o kompaktnosti má teorie $\mathrm{Th}(\mathbf{N}) \cup S_X$ nějaký model, a podle Löwenheimovy-Skolemovy věty má i spočetný model.

Dokázali jsme, že existuje spočetný model $\mathbf{M}$ teorie $\mathrm{Th}(\mathbf{N})$ a jeho prvek a takový, že $\mathbf{M} \models (\overline{n} \mid x)[a]$ pro $n \in X$ a $\mathbf{M} \models \neg(\overline{n} \mid x)[a]$ pro $n \in P - X$. Prvek a je v $\mathbf{M}$ dělitelný všemi prvočísly z množiny X a není dělitelný žádným jiným prvočíslem. Definujme tedy dočasně, že *prvek a modelu* $\mathbf{M}$ teorie $\mathrm{Th}(\mathbf{N})$ *kóduje* množinu prvočísel X, jestliže a je v $\mathbf{M}$ dělitelný každým číslem $\overline{n}$ pro $n \in X$ a není v $\mathbf{M}$ dělitelný žádným číslem $\overline{n}$ pro $n \in P - X$. A *model* $\mathbf{M}$ *kóduje* množinu prvočísel X, jestliže ji kóduje některý prvek a modelu $\mathbf{M}$. Dosud jsme dokázali, že každou množinu prvočísel kóduje nějaký spočetný model teorie $\mathrm{Th}(\mathbf{N})$.

Každý prvek libovolného modelu kóduje právě jednu množinu prvočísel. Spočetný model tedy kóduje nejvýše spočetně mnoho množin. Izomorfní modely jistě kódují tytéž množiny prvočísel. Ke kódování všech $2^{\aleph_0}$ množin prvočísel tedy potřebujeme $2^{\aleph_0}$ navzájem neizomorfních modelů. QED

Máme tedy $2^{\aleph_0}$ různých spočetných modelů teorie $\mathrm{Th}(\mathbf{N})$. Z nich jen jeden je standardní, takže počet všech *nestandardních* navzájem neizomorfních spočetných modelů teorie $\mathrm{Th}(\mathbf{N})$ je také $2^{\aleph_0}$. A každý z nich je zároveň modelem Peanovy aritmetiky. Kdybychom byli zjistili, že spočetných modelů Peanovy aritmetiky je ve smyslu mohutností víc než modelů teorie $\mathrm{Th}(\mathbf{N})$, měli bychom zvláštní nepřímý důkaz, že Peanova aritmetika je neúplná. To ale nenastalo a otázka, zda Peanova aritmetika je úplnou teorií, zůstala v tomto oddílu otevřená.

Peanovu aritmetiku se nám tedy nepodařilo odlišit od teorie $\mathrm{Th}(\mathbf{N})$. Podařilo se nám ale odlišit Peanovu aritmetiku a aritmetiku Robinsonovu: o Robinsonově aritmetice jsme už zjistili, že není ekvivalentní s Peanovou aritmetikou a že není úplná. Naše důkazy existence nestandardních modelů Robinsonovy a Peanovy aritmetiky naznačily další možný rozdíl mezi oběma teoriemi. K důkazu existence nestandardního modelu Peanovy aritmetiky jsme použili větu o kompaktnosti, kdežto nestandardní model Robinsonovy aritmetiky jsme sestrojili „přímo“, zvolili jsme nosnou množinu a definovali jsme na ní operace větvením na konečně mnoho případů.

O žádné z teorií Q, PA a $\mathrm{Th}(\mathbf{N})$ zatím také nevíme, je-li rozhodnutelná. Vyjmenujme tedy otázky, které se vynořily v tomto oddílu a kterými se v dalším výkladu budeme zabývat.

- *Je Peanova aritmetika úplná? Pokud ne, lze ji zúplnit přidáním vhodných axiomů nebo schémat?*
- *Je Robinsonova aritmetika, Peanova aritmetika či teorie* $\mathrm{Th}(\mathbf{N})$ *rozhodnutelná?*
- *Lze nějaký nestandardní model Peanovy aritmetiky sestrojit podobně přímým postupem, jakým jsme sestrojili nestandardní model Robinsonovy aritmetiky, tj. bez užití věty o kompaktnosti?*

- *Je Peanova aritmetika konečně axiomatizovatelná?*

Mezi těmito otázkami samozřejmě existují určité souvislosti. Je-li Peanova aritmetika úplná, pak je ekvivalentní s $\mathrm{Th}(\mathbf{N})$ a podle věty 3.6.8 jsou obě teorie rozhodnutelné. Lze-li Peanovu aritmetiku rozšířit přidáním rekurzívní množiny axiomů na teorii ekvivalentní s $\mathrm{Th}(\mathbf{N})$, pak alespoň $\mathrm{Th}(\mathbf{N})$ je rozhodnutelnou teorií.

Pro hlubší informaci o modelech Peanovy aritmetiky a příbuzných teorií doporučujeme knihu R. Kaye [47]. Touto knihou jsou inspirována některá cvičení a je z ní také převzat obrázek 4.1.2. Zevrubnou informaci o všem, čeho se dotýkáme v této kapitole, a o mnohém dalším souvisejícím s metamatematikou různých aritmetik, lze získat z obsáhlé Hájkovy a Pudlákovy monografie [31].

Cvičení

1. Dokažte, že axiom Q3 je v PA redundantní, tj. lze jej dokázat z ostatních axiomů. Dokažte, že všechny axiomy teorie SUCC jsou dokazatelné v PA.

2. Dokažte v PA všechny zbývající formule z 4.1.1(a).

3. Dokažte, že všechny formule v 4.1.1 (b) a (c) jsou dokazatelné z formulí v (a) a případně axiomů Q1–Q9 bez dalšího užití indukce.

4. Teorie PA^- má aritmetický jazyk a axiomy Q1–Q9 a dále všechny formule z věty 4.1.1. Dokažte, že následující formule jsou dokazatelné v PA^-:

   $\forall x\forall y(x<y \equiv x\le y \;\&\; x\neq y)$,
   $\forall x\forall y(x<y \equiv \mathrm{S}(x)<y \vee \mathrm{S}(x)=y)$,
   $\forall x\forall y(x<y \to \neg(y<x))$,
   $\forall x\forall y\forall z(x+z<y+z \to x<y)$,
   $\forall x(x<\mathrm{S}(x))$,
   $\forall x\forall y\forall z(x\cdot z=y\cdot z \;\&\; z\neq 0 \to x=y)$,
   $\forall x\neg(x<0)$,
   $\forall x\forall y\forall z(x\cdot z<y\cdot z \;\&\; z\neq 0 \to x<y)$.
   $\forall x\forall y(x<y \equiv \mathrm{S}(x)<\mathrm{S}(y))$,

5. Navrhněte pro PA^- úspornější axiomatický systém.

   Návod. Lze například vypustit tranzitivitu relace $<$ v 4.1.1(b), v (a) ponechat jen pět formulí vyjadřujících asociativitu a komutativitu obou operací a distributivitu násobení vůči sčítání, a dále vypustit axiomy Q1, Q2 a Q8.

6. Dokažte, že je-li $\varphi(x,y)$ libovolná aritmetická formule, pak každá z následujících tří sentencí je dokazatelná v PA:

   (a) $\forall u{\le}x\,\exists v\varphi(u,v) \to \exists y\forall u{\le}x\,\exists v{\le}y\,\varphi(u,v)$,

   (b) $\forall x\forall y(\varphi(x,y) \;\&\; x\neq 0 \to \exists u\exists v(\varphi(u,v) \;\&\; v<y)) \to$
   $\to (\exists x\exists y\varphi(x,y) \to \exists y\varphi(0,y))$,

   (c) $\varphi(0,0) \;\&\; \forall x\forall y(\varphi(x,y) \to \varphi(x,\mathrm{S}(y))) \;\&$
   $\&\; \forall x(\forall y\varphi(x,y) \to \varphi(\mathrm{S}(x),0)) \to \forall x\forall y\varphi(x,y)$.

7. Definice axiomatické teorie dovoluje volit libovolně axiomy teorie, nedovoluje ale volit odvozovací pravidla. Zapomeňte na chvíli na toto omezení a zdůvod-

něte, že s použitím „pravidla indukce“

$$\varphi(0)\,,\ \forall x(\varphi(x)\ \to\ \varphi(\mathrm{S}(x)))\ \ /\ \ \forall x\varphi(x)$$

lze v Q dokázat všechny formule dokazatelné v PA.

8. Dokažte podrobně tvrzení 4.1.5 (a)–(i), 4.1.6(a), vynechaný případ v 4.1.7(b) a implikaci $\leftarrow$ v 4.1.7(c).

9. Dokažte, že v modelu z obrázku 4.1.1 platí všechny axiomy Robinsonovy aritmetiky.

10. Přidejme ke struktuře $\mathbf{N}$ přirozených čísel dva nové prvky a, b a rozšiřme následnickou funkci na množinu $M = \mathrm{N} \cup \{a, b\}$ předpisem $\mathrm{S}(a) = b, \mathrm{S}(b) = a$. Dokažte, že sčítání a násobení je možno rozšířit na celou množinu M tak, aby v M platily všechny axiomy Robinsonovy aritmetiky.

11. Rozhodněte, které z následujících formulí jsou dokazatelné v Q.

$\forall x(x \le x)$,
$\forall x(x \le 0\ \to\ x = 0)$,
$\forall x(0 \le x)$,
$\forall x(0 \cdot x = 0)$,
$\forall x(x \cdot \overline{1} = x)$,
$\forall x \forall y \exists z(x \le z\ \&\ y \le z)$,
$\forall x \neg(x < x)$,
$\forall x \forall y(x \le y\ \to\ x < y\ \vee\ x = y)$,
$\forall x \forall y(x + y = 0\ \to\ x = 0\ \&\ y = 0)$,
$\forall x \forall y(x \le y\ \equiv\ \mathrm{S}(x) \le \mathrm{S}(y))$,
$\forall x \forall y(x < y\ \to\ x < \mathrm{S}(y))$,
$\forall x \forall y(\mathrm{S}(x) < y\ \to\ x < y)$,
$\forall x \forall y(x \cdot y = 0\ \to\ x = 0\ \vee\ y = 0)$,
$\forall x(x \le \overline{1}\ \to\ x = 0\ \vee\ x = \overline{1})$,
$\forall x \forall y \forall z((z + y) + x = z + (y + x))$.

12. Nechť $\mathrm{Z}[X]$ je množina všech polynomů v jedné proměnné X s celočíselnými koeficienty. Označme $\mathrm{Z}[X]^+$ množinu všech polynomů $a_0 + a_1X + .. + a_nX^n$ v $\mathrm{Z}[X]$ s nezáporným a_n, tj. s nezáporným koeficientem u nejvyššího členu. Dokažte, že množina $\mathrm{Z}[X]^+$, definujeme-li na ní přirozeným způsobem operace a uspořádání, je modelem teorie PA^-. Dokažte, že v PA^- nelze dokázat sentenci $\forall x \exists y(y + y = x\ \vee\ \mathrm{S}(y + y) = x)$. Které axiomy teorie PA^- neplatí v $\mathrm{Z}[X]$, definujeme-li i na této struktuře přirozeným způsobem operace a uspořádání? Které axiomy teorie PA^- neplatí v množině $\mathrm{N}[X]$ všech polynomů s nezápornými koeficienty?

13. Uvažujte teorii $\mathrm{Th}(\mathbf{N}) \cup \{\, \overline{n} < c\,;\, n \in \mathrm{N}\,\}$ v jazyce, který vznikl z aritmetického jazyka přidáním nové konstanty c. Dokončete jednoduchý důkaz tvrzení, že teorie $\mathrm{Th}(\mathbf{N})$ má alespoň jeden nestandardní model.

14. Dokažte, že množina všech standardních prvků nestandardního modelu $\mathbf{M}$ Peanovy aritmetiky není v $\mathbf{M}$ definovatelná.

15. Nechť $\mathbf{M}$ je nestandardní model Peanovy aritmetiky a nechť relace $\sim$ a R mají stejný význam, jako na str. 285.

(a) Dokažte, že struktura $\langle M/{\sim}, R\rangle$ nemá největší prvek.
(b) Dokažte, že když $a_1 \sim a_2$ a $b_1 \sim b_2$, pak $a_1 + b_1 \sim a_2 + b_2$. Tedy $\sim$ je kongruentní vůči sčítání.
(c) Je $\sim$ kongruentní i vůči násobení?

16. Nechť $\mathbf{M}$ je nestandardní model teorie $\mathrm{Th}(\mathbf{N})$, nechť $\varphi(x)$ je aritmetická formule s jednou volnou proměnnou. Dokažte, že následující podmínky jsou ekvivalentní.
(i) Množina všech standardních prvků modelu $\mathbf{M}$ splňujících v $\mathbf{M}$ formuli φ je nekonečná.
(ii) Existuje nestandardní prvek modelu $\mathbf{M}$ splňující v $\mathbf{M}$ formuli φ.
(iii) $\mathbf{M} \models \forall y \exists x (y < x \ \&\ \varphi(x))$.

Návod. Struktury $\mathbf{M}$ a $\mathbf{N}$ se nemohou lišit platností žádné sentence tvaru $\exists x(\overline{n} < x \ \&\ \varphi(x))$ ani platností sentence v (iii).

17. Zdůvodněte, že pro důkaz implikace (i) $\Rightarrow$ (ii) v předchozím cvičení stačí předpokládat, že $\mathbf{M}$ je model Peanovy aritmetiky.

18. Dokažte, že každá teorie s nejvýše spočetným jazykem má nejvýše $2^{\aleph_0}$ navzájem neizomorfních nejvýše spočetných modelů.

19. Navrhněte teorii se spočetným jazykem, která má $2^{\aleph_0}$ *konečných* navzájem neizomorfních modelů.

20. Které množiny prvočísel jsou ve smyslu důkazu věty 4.1.9 kódované ve struktuře $\mathbf{N}$? Je-li a nestandardní prvek modelu $\mathbf{M}$ Peanovy aritmetiky, musí množina prvočísel, kterou a kóduje v $\mathbf{M}$, být nekonečná?

21. Zdůvodněte, že existuje $2^{\aleph_0}$ spočetných modelů Peanovy aritmetiky takových, že jejich redukty pro jazyk $\{\cdot, 0, \mathrm{S}\}$ jsou po dvou neizomorfní. Modifikujte důkaz věty 4.1.9 a dokažte, že také existuje $2^{\aleph_0}$ spočetných modelů Peanovy aritmetiky takových, že jejich redukty pro jazyk $\{+, 0, \mathrm{S}\}$ jsou po dvou neizomorfní.

4.2 Aritmetizace logické syntaxe

V minulém oddílu jsme ukázali, že v Peanově aritmetice lze dokázat existenci nekonečně mnoha prvočísel. Tímto příkladem jsme chtěli naznačit, že o mnohých vlastnostech přirozených čísel a o operacích s přirozenými čísly můžeme v aritmetickém jazyce mluvit, přestože jim bezprostředně neodpovídají žádné symboly. A v Peanově aritmetice můžeme dokazovat tvrzení o těchto vlastnostech a operacích, ale někdy je třeba známé důkazy poněkud přizpůsobit. Vzpomeňme si, že jedním z dobrých nápadů bylo to, že místo o faktoriálu čísla y stačilo mluvit o číslu z dělitelném všemi čísly $2, 3, \ldots, y$.

Nyní uvidíme, že situace je ještě o něco lepší. V Peanově aritmetice lze mluvit o faktoriálu, o mocnině a o mnoha dalších funkcích a pojmech, které jsou na metamatematické úrovni definovány primitivní rekurzí. Podmínka „z je součinem všech čísel od dvojky do y“ je tedy jiného druhu než podmínka „před z je jen konečně mnoho menších čísel“, kterou (jak víme například z úvah o kompaktnosti) nelze vyjádřit aritmetickou formulí.

Ukažme si postup na příkladu mocniny. Proč platí $2^5 = 32$? Protože existuje šestičlenná posloupnost čísel začínající jedničkou, končící číslem 32 a taková, že každý následující člen je dvojnásobkem předchozího (je samozřejmě řeč o posloupnosti 1, 2, 4, 8, 16, 32). Obecně podmínku $z = 2^y$ budeme moci v aritmetickém jazyce zapsat formulí

$$\exists w(\mathsf{Seq}(w) \;\&\; \mathsf{Lh}(w, y+\overline{1}) \;\&\; \mathsf{B}(w, 0, \overline{1}) \;\&\; \mathsf{B}(w, y, z) \;\& \\ \& \;\forall x{<}y \forall v(\mathsf{B}(w, x, v) \;\rightarrow\; \mathsf{B}(w, x+\overline{1}, \overline{2}\cdot v))),$$

jakmile nalezneme aritmetické formule $\mathsf{Seq}(w)$, $\mathsf{Lh}(w, x)$ a $\mathsf{B}(w, x, v)$, které vyjadřují, že číslo w je kódem posloupnosti, že x je délkou posloupnosti (s kódem) w a že v je členem s indexem x posloupnosti w. Formule $\mathsf{Seq}(w)$, $\mathsf{Lh}(w, x)$ a $\mathsf{B}(w, x, v)$ tedy budou v aritmetickém jazyce vyjadřovat podmínky $\mathrm{Seq}(w)$, $\mathrm{Lh}(w) = x$ a $(w)_x = v$, se kterými jsme pracovali v kapitole 2.

Naším prvním cílem je tedy popsat v aritmetickém jazyce kódování konečných posloupností přirozených čísel přirozenými čísly a dokázat v Peanově aritmetice jeho vlastnosti. Jakmile se to podaří, otevře se nám možnost mluvit v Peanově aritmetice o funkcích, které jsou odvozeny (z funkcí, o kterých už víme, že o nich lze mluvit) pomocí operace primitivní rekurze.

Možnost mluvit v Peanově aritmetice o funkcích odvozených primitivní rekurzí chceme v tomto oddílu vztáhnout zejména na charakteristické funkce množiny všech termů, formulí (v nějakém jazyce) a důkazů (z nějakých předpokladů). V tomto oddílu tedy ukazujeme, že díky možnosti definovat (*formalizovat*) v PA nebo v jiné dostatečně silné axiomatické teorii kódování posloupností lze v PA formalizovat i řadu logických pojmů. Díky tomu si pak budeme moci klást otázky tohoto druhu: co je Peanova aritmetika (nebo teorie množin) schopna dokázat o dokazatelnosti v konkrétních teoriích, jako je Q, PA nebo ZF?

Pro formalizaci v Peanově aritmetice není vhodné kódování posloupností užité v kapitole 2, neboť v jeho definici se vyskytují funkce odvozené primitivní rekurzí (například ona před chvílí zmíněná mocnina), a primitivní rekurzi se nyní musíme vyhnout. Potřebujeme tedy jiné kódování. Čtenář, který se zabýval programováním, si jistě dovede představit situaci, kdy nějaký větší programový celek má být přizpůsoben pro provoz na jiném počítači nebo hardwaru. Naším „novým hardwarem“ je Peanova aritmetika, resp. aritmetický jazyk. A tento hardware nemá zabudovanou operaci primitivní rekurze. S vynaložením určité námahy ji však lze simulovat. A navíc, je-li programový celek rozumně strukturován, jeho velké části zůstanou beze změny, neboť strojově závislé instrukce jsou soustředěny jen do určitých podprogramů, a jen ty postačí nově implementovat.

Užijeme kódování blízké tomu, jaké původně použil Gödel a které je popsáno v Shoenfieldově knize [75]. Ukazuje se, že snažší než definovat rovnou kódování posloupností je definovat nejprve kódování konečných *množin*. Množina se od posloupnosti liší tím, že u ní nelze mluvit o pořadí prvků. Jakmile budeme mít množiny, můžeme posloupnosti definovat stejným způsobem, jako se v teorii množin definují funkce: posloupnost bude taková a taková množina dvojic.

Gödelovo (Shoenfieldovo) kódování je založeno na následujících dvou faktech.

Fakt 1 *Nechť* $B = \{b_0, \ldots, b_{n-1}\}$ *je množina po dvou nesoudělných čísel větších než* 1, *nechť* $X \subseteq B$. *Pak číslo* $k = \prod_{i \in X} b_i$ *není dělitelné žádným* $b \in B - X$.

Fakt 2 *Je-li* $m \neq 0$ *dělitelné čísly* $2, 3, \ldots, r$, *pak čísla* $1+m, 1+2m, \ldots, 1+(r+1)m$ *jsou po dvou nesoudělná.*

Ve formulaci faktu 2 jsme ovšem užili stejný postup jako při důkazu existence nekonečně mnoha prvočísel: protože jsme se zařekli, že nebudeme užívat faktoriál, mluvíme o číslu m dělitelném všemi čísly $2, 3, \ldots, r$.

Fakty 1 a 2 zatím nedokazujme. Chceme nalézt takové reformulace, které budeme schopni dokázat v Peanově aritmetice. Kromě faktů 1 a 2 budeme potřebovat také párovací funkci. *Párovací funkce* je libovolná vzájemně jednoznačná funkce z N^2 na N. Jedna z párovacích funkcí je dána touto tabulkou:

0	1	3	6	10	...
2	4	7	11		...
5	8				
9					
⋮					

Označme tuto funkci c. Platí například $c(2,0) = 5$, $c(2,2) = 12$ a $c(3,1) = 13$. Nechť na chvíli d označuje funkci jedné proměnné, jejíž hodnoty jsou uvedeny v nultém řádku tabulky, tj. funkci definovanou předpisem $d(y) = c(0,y)$. Pro každé y platí $d(y) = 1+2+\ldots+y$, tedy $d(y) = \frac{1}{2}y(y+1)$. Dále platí $c(x,y) = d(x+y)+x$. Tím jsme odvodili předpis pro výpočet funkce c:

$$c(x,y) = \frac{1}{2}(x+y)(x+y+1) + x.$$

V dalším pišme (x,y) místo $c(x,y)$ a číslu (x,y) říkejme *kód dvojice* $[x,y]$.

Kódování množin a posloupností založené na faktech 1 a 2 definujeme následovně. Máme-li zjistit, zda číslo j je prvkem čísla q, nalezneme nejprve čísla m a k taková, že $q = (m,k)$. Pak ověříme, zda všechna čísla $2, 3, \ldots, j$ dělí m. Pokud ne, nebo pokud m nebo k je nula, j není prvkem čísla q. Pokud ano, zjistíme, zda $1 + (1+j) \cdot m$ dělí k. To znamená, že j *je prvkem čísla* $q = (m,k)$, je-li splněna podmínka

$$m \neq 0 \ \&\ k \neq 0 \ \&\ \forall i \leq j\,(i \neq 0 \Rightarrow i \text{ dělí } m) \ \&\ 1 + (j+1) \cdot m \text{ dělí } k.$$

Máme-li naopak k dané konečné množině F přirozených čísel nalézt q, jehož prvky jsou prvky množiny F a nic jiného, nejprve zvolíme $r \geq \max F$ a nenulové m dělitelné všemi čísly $2, 3, \ldots, r$. Pak utvoříme součin $k = \prod_{j \in F}(1 + (j+1) \cdot m)$ a stanovíme číslo $q = (m, k)$. Řekneme, že číslo q *je množinou* (neboli je kódem nějaké množiny), a píšeme $\mathrm{Set}(q)$, jestliže žádné $q' < q$ nemá stejné prvky jako q. Dále definujeme, že číslo q je *kódem posloupnosti* $a_0, \ldots, a_{n-1}$, a píšeme $q = \langle a_0, \ldots, a_{n-1} \rangle$, jestliže q je kódem množiny $\{(0, a_0), \ldots, (n-1, a_{n-1})\}$. Řekneme, že číslo q *je posloupností* (je kódem nějaké posloupnosti), a píšeme $\mathrm{Seq}(q)$, jestliže levé členy všech jeho prvků tvoří „souvislou“ množinu tvaru $\{0, \ldots, n-1\}$. *Délka* $\mathrm{Lh}(q)$ *posloupnosti* q je nejmenší číslo n takové, že $(n, k) \notin q$ pro žádné k.

Příklad 4.2.1 Předpokládejme, že máme číslo $q = 86\,435\,497\,642\,921$ a máme určit všechny jeho prvky. S určitým úsilím a užitím vhodných prostředků nejprve rozložíme q na dvojici: $q = (60, 13\,147\,981)$. Číslo $m = 60$ je dělitelné čísly 2 až 6, není dělitelné sedmi. Tedy j je prvkem q, pokud $j \leq 6$, a navíc $1 + (j+1) \cdot 60$ dělí $k = 13\,147\,981$. Snadno lze ověřit, že pro $j \in \{1, 4, 5\}$ číslo $1 + (j+1) \cdot 60$ dělí, pro $j \in \{0, 2, 3, 6\}$ nedělí k. Prvky čísla q jsou tedy všechny tři prvky množiny $F = \{1, 4, 5\}$, a nic jiného. Lze ověřit, že m je nejmenší číslo dělitelné všemi čísly $2, 3, \ldots, \max F$ a že k je nejmenší číslo dělitelné všemi čísly tvaru $1 + (j+1) \cdot m$, kde $j \in F$. Protože funkce $[m, k] \mapsto (m, k)$ je monotonní v obou proměnných (cvičení), číslo q je nejmenší číslo s prvky 1, 4 a 5. Platí tedy $\mathrm{Set}(q)$. Protože $1 = (0, 1)$, $4 = (1, 1)$ a $5 = (2, 0)$, číslo q je kódem posloupnosti, neboli $\mathrm{Seq}(q)$, a platí $q = \langle 1, 1, 0 \rangle$ a $\mathrm{Lh}(q) = 3$.

Při vývoji větších programových celků se často uplatňují knihovny podprogramů. Jsou-li často užívané podprogramy umístěny v takové knihovně, mohou být užity při sestavení více různých programů. A jsou-li v takové knihovně umístěny strojově závislé podprogramy, někdy lze hlavní program přizpůsobit jinému hardwaru pouhým novým sestavením při použití jiné knihovny podprogramů. V tom případě není nutné hlavní program nijak měnit, jiná knihovna obsahuje jiné, ale stejně pojmenované podprogramy. Tím chceme říci, že užití symbolů Seq, Lh atd. v jiném významu než v kapitole 2, kde jsme se s nimi již setkali, nepokládáme za nedbalost, ale za užitečnou praxi.

Nyní jsme schopni postupně zapsat právě popsané kódování aritmetickými formulemi a dokázat jejich vlastnosti. Nejprve definujme formule $\mathsf{Pair}(z, t, w)$, $x \in w$ a $\mathsf{Set}(w)$:

$$\begin{aligned}
\mathsf{Pair}(z,t,w) &\equiv \overline{2} \cdot w = (z+t) \cdot (z+t+\overline{1}) + \overline{2} \cdot z, \\
x \in w &\equiv \exists z \exists t (z \neq 0 \ \&\ t \neq 0 \ \&\ \mathsf{Pair}(z,t,w) \ \& \\
&\qquad \& \ \forall v \leq x (v \neq 0 \ \rightarrow \ v \mid z) \ \&\ \overline{1} + (x+\overline{1}) \cdot z \mid t), \\
\mathsf{Set}(w) &\equiv \neg \exists w' < w \forall v (v \in w' \ \equiv \ v \in w).
\end{aligned}$$

Formule $\mathsf{Pair}(z, t, w)$ v aritmetickém jazyce popisuje párovací funkci, formule $x \in w$ a $\mathsf{Set}(w)$ vyjadřují podmínku číslo x je prvkem čísla w resp. číslo w je množina.

Lemma 4.2.2 *(a) V* PA *lze dokázat sentenci* pro každou dvojici $[z,t]$ existuje právě jedno w takové, že $\mathsf{Pair}(z,t,w)$, *a také sentenci* pro každé w existuje právě jedna dvojice [z,t] taková, že $\mathsf{Pair}(z,t,w)$.
(b) $\mathsf{PA} \vdash \forall z \forall t \forall w (\mathsf{Pair}(z,t,w) \rightarrow z \leq w \ \& \ t \leq w)$.
(c) $\mathbf{N} \models \mathsf{Pair}(\overline{m}, \overline{k}, \overline{q})$, *právě když* $(m,k) = q$.

Důkaz Uvažujme v PA.

Nechť w je dáno. Nalezněme maximální y takové, že $y \cdot (y + \overline{1}) \leq \overline{2} \cdot w$. To lze, neboť y je zároveň minimální takové, že $(y + \overline{1}) \cdot (y + \overline{2}) > \overline{2} \cdot w$. Obě čísla $\overline{2} \cdot w$ a $y \cdot (y + \overline{1})$ jsou sudá, a jejich rozdíl lze tedy psát jako $\overline{2} \cdot z$. Platí tedy

$$y \cdot (y + \overline{1}) + \overline{2} \cdot z = \overline{2} \cdot w < (y + \overline{1}) \cdot (y + \overline{2}) = y \cdot (y + \overline{1}) + \overline{2} \cdot (y + \overline{1}).$$

Z toho plyne $\overline{2} \cdot z < \overline{2} \cdot (y + \overline{1})$ a $z \leq y$. Číslo y tedy lze psát jako součet $y = z + t$, a z a t jsou hledaná čísla splňující $\mathsf{Pair}(z,t,w)$.

Zbývající úvahy ponecháváme za cvičení. QED

Lemma 4.2.3 *(a)* $\mathsf{PA} \vdash \forall x \forall w (x \in w \rightarrow x < w)$.
(b) $\mathbf{N} \models \overline{j} \in \overline{q}$, *právě když číslo* j *je prvek čísla* q.

Důkaz Tvrzení (a) lze dokázat takto:

Je-li $z \neq 0$, pak $x < \overline{1} + (x + \overline{1}) \cdot z$. Je-li $t \neq 0$, pak z $\overline{1} + (x + \overline{1}) \cdot z \mid t$ plyne $\overline{1} + (x + \overline{1}) \cdot z \leq t$. Vezmeme-li v úvahu ještě (b) lemmatu 4.2.2 a tranzitivitu uspořádání, máme (a).

Důkaz tvrzení (b) ponecháváme na čtenáři, užije se 4.2.2(c). QED

Tvrzení 4.2.3(a) zdaleka není všechno, co hodláme v PA dokázat o náležení. Potřebujeme ještě tvrzení, které bychom mohli interpretovat jako každá konečná množina má nějaký kód. To uděláme v podstatě formalizací (důkazů) faktů 1 a 2. Ve znění faktů 1 a 2 je řeč o nesoudělných číslech. Relaci nesoudělnosti lze definovat dvěma způsoby:

(i) Čísla a a b jsou nesoudělná, jestliže nemají společného dělitele většího než 1.

(ii) Čísla a a b jsou nesoudělná, jestliže a dělí každé číslo x takové, že a dělí $b \cdot x$.

Obě definice jsou (v případě, kdy $a \neq 0$) ekvivalentní. Důkaz (v PA) lze získat modifikací důkazu tvrzení 4.1.7(c) z předchozího oddílu. Ponecháváme jej za cvičení, protože v dalším výkladu plně vystačíme s definicí (ii):

$$\mathsf{RPrime}(x,y) \equiv \forall v (x \mid y \cdot v \rightarrow x \mid v).$$

Formuli $\mathsf{RPrime}(x,y)$ lze číst číslo x je nesoudělné s číslem y. Následující lemma je téměř doslova převzato z [75].

Lemma 4.2.4 *Následující sentence jsou dokazatelné v* PA*:*
(a) $\forall x \forall y (x \neq 0 \ \& \ \mathsf{RPrime}(x,y) \rightarrow \mathsf{RPrime}(y,x))$,
(b) $\forall z \forall x \mathsf{RPrime}(z, \overline{1} + x \cdot z)$,
(c) $\forall u \forall z \forall x (u \mid z \rightarrow \mathsf{RPrime}(\overline{1} + x \cdot z, \overline{1} + (x+u) \cdot z))$.

Důkaz (v PA**)** (a) Nechť platí oba předpoklady a nechť $y \mid x \cdot v$. Pak existuje u_1 takové, že $y \cdot u_1 = x \cdot v$. Tedy $x \mid y \cdot u_1$. Protože $\mathsf{RPrime}(x,y)$, platí $x \mid u_1$. Tedy $x \cdot u_2 = u_1$ pro vhodné u_2. Tedy $y \cdot x \cdot u_2 = x \cdot v$. Protože $x \neq 0$, máme $y \cdot u_2 = v$ a $y \mid v$.

(b) Nechť $z \mid (\overline{1} + x \cdot z) \cdot v$. Pak $z \mid v + x \cdot z \cdot v$. Z 4.1.5(j) plyne $z \mid v$.

(c) Uvažujme za předpokladu $\overline{1} + x \cdot z \mid (\overline{1} + (x+u) \cdot z) \cdot v$:

1: $\overline{1} + x \cdot z \mid (\overline{1} + (x+u) \cdot z) \cdot v$

2: $\overline{1} + x \cdot z \mid v + x \cdot z \cdot v + u \cdot z \cdot v$

3: $\overline{1} + x \cdot z \mid (\overline{1} + x \cdot z) \cdot v + u \cdot z \cdot v$

4: $\overline{1} + x \cdot z \mid u \cdot z \cdot v$; 4.1.5(j)

5: $\overline{1} + x \cdot z \mid u \cdot v$; (a), (b)

6: $\overline{1} + x \cdot z \mid z \cdot v$; $u \mid z$

7: $\overline{1} + x \cdot z \mid v$; (a), (b).

QED

Následující věta říká, že pro naše náležení platí *schéma vydělení*: vždy existuje množina všech čísel, která mají takovou a takovou vlastnost.

Věta 4.2.5 *Každá sentence* $\forall \underline{u} \forall y \exists w (\mathsf{Set}(w) \ \& \ \forall v (v \in w \equiv v < y \ \& \ \varphi(v, \underline{u})))$ *je v* PA *dokazatelná.*

Důkaz Budeme postupovat v podstatě tak, jak naznačují fakty 1 a 2 a naše definice náležení. Protože ale obrat „označme t součin všech čísel tvaru $\overline{1} + (v + \overline{1}) \cdot z$ takových, že $v < y$ a $\varphi(v, \underline{u})$“ není (alespoň zatím) v aritmetickém jazyce zcela korektní, obejdeme jej pomocí indukce. Uvažujme v PA:

> Nechť čísla $u_1, \ldots, u_n$ a y jsou dána. Zvolme nenulové z dělitelné všemi čísly $\overline{2}, \overline{3}, \ldots, y - \overline{1}$. Indukcí podle x dokážeme, že
>
> $$\forall x (x \leq y \rightarrow \exists t \forall v (v \in (z,t) \equiv v < x \ \& \ \varphi(v, \underline{u}))), \tag{1}$$
>
> kde $v \in (z,t)$ je zkratka pro formuli $\forall w (\mathsf{Pair}(z,t,w) \rightarrow v \in w)$ nebo pro formuli $\exists w (\mathsf{Pair}(z,t,w) \ \& \ v \in w)$. Z (1) dostaneme tvrzení věty volbou $x := y$. Protože z je dělitelné všemi nenulovými čísly menšími než y, podmínka $v \in (z,t)$ je pro $v < y$ ekvivalentní s podmínkou $\overline{1} + (v + \overline{1}) \cdot z \mid t$, viz definice náležení. Pro $v \geq y$ platí alespoň implikace $v \in (z,t) \rightarrow \overline{1} + (v + \overline{1}) \cdot z \mid t$. Z toho plyne, že místo (1) stačí dokázat
>
> $$\forall x (x \leq y \rightarrow \exists t \forall v (\overline{1} + (v + \overline{1}) \cdot z \mid t \equiv v < x \ \& \ \varphi(v, \underline{u}))). \tag{2}$$

Je-li $x = 0$, pak $t = \overline{1}$ vyhovuje, protože $\overline{1}+(v+\overline{1})\cdot z$ je alespoň $\overline{2}$ pro libovolné v, a tedy $\overline{1} + (v + \overline{1}) \cdot z$ nedělí t. Nechť tedy t vyhovuje pro x, tj. platí

$$\forall v(\overline{1} + (v + \overline{1}) \cdot z \mid t \equiv v < x \ \& \ \varphi(v, \underline{u})), \tag{3}$$

a nechť navíc $x + \overline{1} \leq y$. Když $\neg\varphi(x, \underline{u})$, pak $t' = t$ vyhovuje i pro $x + \overline{1}$. Když naopak $\varphi(x, \underline{u})$, zvolme $t' = t \cdot (\overline{1} + (x + \overline{1}) \cdot z)$. V ekvivalenci

$$\forall v(\overline{1} + (v + \overline{1}) \cdot z \mid t \cdot (\overline{1} + (x + \overline{1}) \cdot z) \equiv v < x + \overline{1} \ \& \ \varphi(v, \underline{u}))$$

jistě platí implikace $\leftarrow$. Ověříme implikaci $\rightarrow$. Nechť

$$\overline{1} + (v + \overline{1}) \cdot z \mid t \cdot (\overline{1} + (x + \overline{1}) \cdot z).$$

Když $v \neq x$, pak, díky 4.2.4(c), $\overline{1} + (v + \overline{1}) \cdot z$ a $\overline{1} + (x + \overline{1}) \cdot z$ jsou nesoudělná čísla. Tedy $\overline{1} + (v + \overline{1}) \cdot z \mid t$. Zbytek plyne z (3).

Máme tedy dokázánu podmínku (1). Vezměme t, jehož existence je v (1) zaručena pro $x := y$. Pro w takové, že $\mathsf{Pair}(z, t, w)$, platí

$$\forall v(v \in w \equiv v < y \ \& \ \varphi(v, \underline{u})). \tag{4}$$

Díky principu LNP můžeme vzít nejmenší w splňující podmínku (4). Pro takové w platí navíc $\mathsf{Set}(w)$.

QED

V důkazu předchozí věty jsme si dovolili zápis $v \in (z, t)$, jehož význam byl číslo v je prvkem některého neboli každého w takového, že $\mathsf{Pair}(z, t, w)$. Takto budeme postupovat i v budoucnu, čili budeme někdy v symbolických zápisech užívat funkční symboly, jejichž význam je zřejmý, ale jejichž definici (ve smyslu tvrzení (b) věty 3.5.3) jsme nevyslovili, protože aritmetický jazyk rozšiřovat nechceme. Díky tvrzení věty 4.2.5 můžeme v Peanově aritmetice mluvit o množině $\{ v < y; \varphi(v, \underline{u}) \}$. Zápis $\{ \, v < y \, ; \, \varphi(v, \underline{u}) \, \}$ lze také počítat k nedefinovaným funkčním symbolům, jejichž význam je zřejmý a jejichž užití bychom se snadno mohli vyhnout za cenu méně přehledných zápisů.

Za formuli $\varphi(v, \underline{u})$ můžeme například zvolit formuli $v = u_1 \vee v = u_2$. Protože uvnitř PA můžeme říci, že „mez“ y volíme dostatečně velkou, můžeme v PA mluvit o dvouprvkové množině $\{u_1, u_2\}$. Stejným právem můžeme mluvit i o tříprvkových, čtyřprvkových atd. množinách (formálních) přirozených čísel, a také užívat zápisy tvaru $w \cup \{x\}$. Pišme $w_1 \subseteq w_2$ místo $\forall v(v \in w_1 \rightarrow v \in w_2)$.

Lemma 4.2.6 *V* PA *lze dokázat sentence:*
(a) $\forall w_1 \forall w_2(\mathsf{Set}(w_1) \ \& \ \mathsf{Set}(w_2) \ \& \ w_1 \subseteq w_2 \ \& \ w_2 \subseteq w_1 \rightarrow w_1 = w_2)$,
(b) $\forall w_1 \forall w_2(\mathsf{Set}(w_1) \ \& \ \mathsf{Set}(w_2) \ \& \ w_1 \subseteq w_2 \rightarrow w_1 \leq w_2)$,
(c) $\forall w \forall x \forall y(\mathsf{Set}(w) \ \& \ y \notin w \ \& \ x \leq y \rightarrow w \cup \{x\} \leq w \cup \{y\})$.

Důkaz Dokažme například tvrzení (c):

Vezměme čísla z a t taková, že $(z, t) = w \cup \{y\}$. Čísla z a t jsou obě nenulová, z je dělitelné všemi prvky množiny w i číslem y a platí $\overline{1}+(y+\overline{1})\cdot z \mid t$. Vezměme t_1 takové, že $t_1 \cdot (\overline{1} + (y + \overline{1}) \cdot z) = t$. Když $x \notin w$, volme $t' = t_1 \cdot (\overline{1} + (x + \overline{1}) \cdot z)$,

jinak volme $t' = t_1$. V obou případech platí $t' \leq t$, tedy $(z,t') \leq (z,t)$. Úvahami podobnými jako v důkazu věty 4.2.5 lze ověřit, že (z,t') je číslo, jehož prvky jsou všechny prvky množiny w, číslo x, a nic jiného. Protože množina $w \cup \{x\}$ je definována jako nejmenší číslo, jehož prvky jsou všechny prvky množiny w, číslo x, a nic jiného, máme $w \cup \{x\} \leq w \cup \{y\}$.

QED

Tvrzení (b) a (c) předchozího lemmatu říkají, že odstraníme-li z množiny některé prvky nebo nahradíme-li některé prvky menšími čísly, kód výsledné množiny není větší. Vzhledem k tvrzení (a), tj. vzhledem k platnosti axiomu extenzionality, můžeme tvrdit, že kód výsledné množiny je dokonce ostře menší.

Tím jsme dospěli ke kódování konečných *posloupností*:

$$\begin{aligned}
\mathsf{B}(w,u,v) &\equiv \exists x(\mathsf{Pair}(u,v,x) \ \&\ x \in w),\\
\mathsf{Lh}(w,y) &\equiv \neg\exists v\mathsf{B}(w,y,v) \ \&\ \forall u{<}y\,\exists v\mathsf{B}(w,u,v),\\
\mathsf{Seq}(w) &\equiv \mathsf{Set}(w) \ \&\ \exists y(\mathsf{Lh}(w,y) \ \&\ \forall u\forall v(\mathsf{B}(w,u,v) \to u < y) \ \&\\
&\qquad\qquad \&\ \forall u{<}y\,\exists!\, v\mathsf{B}(w,u,v)).
\end{aligned}$$

Formule $\mathsf{Seq}(w)$, $\mathsf{Lh}(w,y)$ a $\mathsf{B}(w,u,v)$ čteme číslo w je posloupnost, číslo y je délka čísla w a číslo v je u-tý člen čísla w. Formule jsme pro jednoduchost definovali tak, že o délce a o u-tém členu čísla w dovolují mluvit i v případě, kdy w není posloupností (dokonce i když není množinou). Všimněme si ještě, že formule Pair se ve formuli B vyskytuje na dvou místech: abychom určili, zda $\mathsf{B}(w,u,v)$, musíme w rozložit na *dvojici* z,t a pak se mimo jiné ptát, zda pro *dvojici* x utvořenou z u a v platí $\overline{1}+(x+\overline{1})\cdot z \mid t$. Za zápisem $\mathsf{B}(w,u,v)$ si můžeme představit názornější zápis $(u,v) \in w$.

Písmeno B odkazuje k řeckému „β“; funkci, která číslům w a u přiřazuje u-tý člen posloupnosti s kódem w, se často říká *Gödelova β-funkce*. „Lh“ a „Seq“ jsou samozřejmě zkratky anglických slov *length* a *sequence*.

Lemma 4.2.7 *Formule* Seq, Lh *a* B *definují příslušné pojmy v* $\mathbf{N}$. *To znamená, že pro libovolná čísla j, k, q a n platí:* $\mathbf{N} \models \mathsf{Seq}(\overline{q})$, *právě když* $\mathrm{Seq}(q)$ *(tj. právě když q je posloupnost),* $\mathbf{N} \models \mathsf{Lh}(\overline{q},\overline{n})$, *právě když* $\mathrm{Lh}(q) = n$, *a* $\mathbf{N} \models \mathsf{B}(\overline{q},\overline{j},\overline{k})$, *právě když* $(q)_j = k$.

Důkaz je podobný jako v 4.2.3(b), 4.2.2(c) a předtím v 4.1.8.

Zdůrazněme ještě jednou, že zápisy $\mathrm{Seq}(q)$, $\mathrm{Lh}(q)$ a $(q)_j = k$ užíváme ve významu, který byl definován v příkladu 4.2.1 a před ním, nikoliv ve významu z kapitoly 2.

Rozmysleme si, že v Peanově aritmetice lze dokázat, že naše kódování posloupností má očekávané vlastnosti: prvky ani délka posloupnosti w nepřevyšují (číslo) w, členy posloupnosti jsou určeny jednoznačně, existuje posloupnost, která nemá žádné členy, z libovolného čísla lze utvořit jednoprvkovou posloupnost, ke každým dvěma

posloupnostem w_1 a w_2 existuje posloupnost w, která je slepením (konkatenací) posloupností w_1 a w_2.

Věta 4.2.8 *Následující sentence jsou dokazatelné v* PA*:*

(a) $\forall w \forall u \forall v (\mathsf{B}(w,u,v) \to u < w \ \&\ v < w)$,

(b) $\forall w \exists ! y\, \mathsf{Lh}(w,y) \ \&\ \forall w \forall y (\mathsf{Lh}(w,y) \to y \leq w)$,

(c) $\forall w \forall u \forall v_1 \forall v_2 (\mathsf{Seq}(w) \ \&\ \mathsf{B}(w,u,v_1) \ \&\ \mathsf{B}(w,u,v_2) \to v_1 = v_2)$,

(d) $\exists w (\mathsf{Seq}(w) \ \&\ \mathsf{Lh}(w,0))$,

(e) $\forall v \exists w (\mathsf{Seq}(w) \ \&\ \mathsf{Lh}(w,\overline{1}) \ \&\ \mathsf{B}(w,0,v))$,

(f) $\forall w_1 \forall w_2 \forall y_1 \forall y_2 \exists w (\mathsf{Seq}(w_1) \ \&\ \mathsf{Seq}(w_2) \ \&\ \mathsf{Lh}(w_1,y_1) \ \&\ \mathsf{Lh}(w_2,y_2) \to$
$\to \mathsf{Seq}(w) \ \&\ \mathsf{Lh}(w, y_1+y_2) \ \&\ \forall u{<}y_1 \forall v (\mathsf{B}(w,u,v) \equiv \mathsf{B}(w_1,u,v)) \ \&$
$\&\ \forall u{<}y_2 \forall v (\mathsf{B}(w, y_1+u, v) \equiv \mathsf{B}(w_2,u,v)))$.

Důkaz Tvrzení (a) plyne z 4.2.3(a) a z 4.2.2(b). Ukažme si důkaz tvrzení (f), ostatní úvahy jsou podobné nebo lehké. V (f) máme zdůvodnit, že existuje množina $w_1 \cup \{\, (y_1+u, v)\,;\, (u,v) \in w_2 \,\}$. Uvažujme v PA:

> Nechť čísla w_1, w_2, y_1 a y_2 splňující předpoklady $\mathsf{Seq}(w_1)$, $\mathsf{Seq}(w_2)$, $\mathsf{Lh}(w_1,y_1)$ a $\mathsf{Lh}(w_2,y_2)$ jsou dána. Zvolme číslo v_0 větší než všechny prvky obou posloupností w_1 a w_2. To lze díky již dokázanému tvrzení (a). Zvolme číslo z takové, že $\mathsf{Pair}(y_1+y_2, v_0, z)$. Podle věty 4.2.5 existuje množina w všech $x < z$, pro která platí
>
> $$x \in w_1 \ \vee\ \exists u \exists v (\mathsf{Pair}(y_1+u, v, x) \ \&\ \mathsf{B}(w_2,u,v)).$$
>
> Je jasné, že když $\mathsf{Pair}(u,v,x)$ a $\mathsf{B}(w_1,u,v)$, nebo $\mathsf{Pair}(y_1{+}u,v,x)$ a $\mathsf{B}(w_2,u,v)$, pak $x < z$. Číslo z tedy bylo zvoleno dostatečně velké, a tudíž w je opravdu hledaným slepením obou posloupností w_1 a w_2.

QED

Díky tvrzením (e) a (f) věty 4.2.8 můžeme rozšířit naši úmluvu o užívání nedefinovaných funkčních symbolů se zřejmým významem: $w_1 * w_2$ označuje ono (jednoznačně určené) číslo, které je konkatenací posloupností w_1 a w_2, dále například $w * \langle x \rangle$ označuje prodloužení posloupnosti w o člen x (čili množinu $w \cup \{(y,x)\}$, kde $\mathsf{Lh}(w,y)$), a podobně.

Lemma 4.2.9 *V* PA *lze dokázat sentenci* $\forall w_1 \forall w_2 (w_1 \leq w_1 * w_2 \ \&\ w_2 \leq w_1 * w_2)$.

Toto tvrzení plyne téměř bezprostředně z tvrzení (b) lemmatu 4.2.6. Z tvrzení (a) téhož lemmatu navíc plyne, že konkatenace dvou posloupností w_1 a w_2 nenulové délky je dokonce ostře větší než kterékoliv z čísel w_1 a w_2.

Raději připomeňme, že kódy a prvky (formalizovaných) množin a posloupností či délky posloupností jsou *formální přirozená čísla*, tj. čísla, jejichž vlastnosti vyjadřujeme uvnitř Peanovy aritmetiky aritmetickým jazykem a která je vhodné si

představovat jako libovolné, čili standardní nebo nestandardní, prvky nějakého modelu Peanovy aritmetiky. Každý prvek takového modelu $\mathbf{M}$ je v $\mathbf{M}$ délkou nějakých posloupností, tj. prvků $a \in M$, které v $\mathbf{M}$ splňují formuli $\mathsf{Seq}(w)$!

Můžeme-li mluvit o posloupnostech, lze přikročit k úvahám o tom, jak v aritmetickém jazyce definovat termy, formule a další syntaktické pojmy a jak v Peanově aritmetice dokázat jejich vlastnosti. Můžeme tedy přikročit k *aritmetizaci logické syntaxe*. Postupujeme podobně jako v důkazu věty 3.6.6. Tam jsme postupně mimo jiné zdůvodnili, že podmínka $\mathrm{Proof}_T(\varphi, d)$, čili podmínka „$d$ je důkaz formule φ v teorii T“, je rekurzívní, je-li T rekurzívní. Tady chceme také mluvit o proměnných, termech a řadě dalších syntaktických pojmů. Pro každý z těchto pojmů chceme sestrojit aritmetickou formuli, která jej popisuje (definuje v $\mathbf{N}$), a zmínit se o jejích vlastnostech. Někdy konstrukci příslušné formule jen naznačíme. Tím dospějeme k formuli $\mathsf{Proof}_\tau(x, y)$, která za přirozených předpokladů o teorii T a formuli τ definuje v $\mathbf{N}$ podmínku $\mathrm{Proof}_T(\varphi, d)$ a má ještě další užitečné vlastnosti. Až budeme mít formuli $\mathsf{Proof}_\tau(x, y)$, budeme v aritmetickém jazyce moci mluvit o formálních důkazech, o dokazatelnosti a o bezespornosti.

Stejně jako v důkazu věty 3.6.6 předpokládáme, že indexy u proměnných jsme se rozhodli zapisovat binárně a že jazyk, který formalizujeme, je aritmetický.

Nejprve si vzpomeňme, že *proměnná* je posloupnost, ve které za jedním znakem „v“ následuje zápis přirozeného čísla, a definujme formuli $\mathsf{Var}(v)$:

$$\begin{aligned}\mathsf{Var}(v) \equiv\ & \mathsf{Seq}(v)\ \&\ \neg\mathsf{Lh}(v,0)\ \&\ \neg\mathsf{Lh}(v,\overline{1})\ \&\ \mathsf{B}(v,0,\overline{\text{`v}})\ \&\\ & \&\ (\mathsf{B}(v,\overline{1},\overline{\text{`0}})\ \to\ \mathsf{Lh}(v,\overline{2}))\ \&\\ & \&\ \forall u\forall z(\mathsf{B}(v,u,z)\ \&\ u\neq 0\ \to\ z=\overline{\text{`0}}\ \vee\ z=\overline{\text{`1}}).\end{aligned}$$

Stejně jako v kapitole 2, levý apostrof následovaný znakem označuje číselný kód, který naše kódová tabulka přiřazuje onomu znaku. Například protože číselným kódem znaku 0 je číslo 32, zápisy $\overline{\text{`0}}$ a $\overline{32}$ představují tytéž termy.

Term je posloupnost symbolů, která je buď proměnná, nebo je jednočlennou posloupností sestávající jen ze symbolu 0, nebo vznikla z nějakých termů pomocí jednoho ze symbolů $+$, $\cdot$, S a závorek:

$$\begin{aligned}\mathsf{Term}(x) \equiv\ & \exists w(\mathsf{Seq}(w)\ \&\ \mathsf{Lh}(w,x+\overline{1})\ \&\ \mathsf{B}(w,x,\overline{1})\ \&\\ & \forall u\forall v(\mathsf{B}(w,u,v)\ \to\ v\le\overline{1})\ \&\\ & \forall u(\mathsf{B}(w,u,\overline{1})\ \equiv\ (\mathsf{Var}(u)\ \vee\ u=\langle\overline{\text{`0}}\rangle\ \vee\\ & \qquad \vee\ \exists u_1{<}u\exists u_2{<}u(\mathsf{B}(w,u_1,\overline{1})\ \&\ \mathsf{B}(w,u_2,\overline{1})\ \&\\ & \qquad\qquad \&\ u=\langle\overline{\text{`(}}\rangle * u_1 * \langle\overline{\text{`+}}\rangle * u_2 * \langle\overline{\text{`)}}\rangle\,)\\ & \qquad \vee\ (\ldots\text{ podobně pro symbol „}\cdot\text{“ }\ldots\,)\\ & \qquad \vee\ (\ldots\text{ a symbol „S“ }\ldots\,)\,))).\end{aligned}$$

Posloupnost w ve formuli Term je posloupnost nul a jedniček, která o každém čísle nepřevyšujícím x říká, zda je kódem termu. Jednička znamená ano, nula ne. Posloupnost w je tedy počátečním úsekem charakteristické funkce množiny

všech termů. S její pomocí se nám podařilo simulovat v aritmetickém jazyce primitivní rekurzi. Vzpomeňme si, že stejně jsme postupovali v důkazu věty 3.6.9. Posloupnosti w můžeme říkat *dosvědčující posloupnost*.

Zápis $u = \langle \overline{\text{`(}} \rangle * u_1 * \langle \overline{\text{`+}} \rangle * u_2 * \langle \overline{\text{`)}} \rangle$ ve formuli $\mathsf{Term}$ je zkratka pro číslo $u$ je posloupnost, jejíž nejlevější člen je $\overline{\text{`(}}$, pak následují členy totožné s členy posloupnosti u_1, pak člen $\overline{\text{`+}}$ a členy posloupnosti $u_2$, nakonec člen $\overline{\text{`)}}$. Čtyři hvězdičky naznačují, že u je konkatenací pěti posloupností, z nichž tři jsou jednoprvkové sestávající pouze z číselného kódu přiřazeného levé závorce, symbolu + resp. pravé závorce. Domluvme se, že v této situaci budeme nadále psát $u = \ulcorner (u_1 \text{+} u_2) \urcorner$, formální výraz u vznikl z formálních výrazů u_1 a u_2 a tří jednotlivých symbolů. Podobně budeme psát například $u = \ulcorner \forall x z \urcorner$, jestliže formální výraz u je posloupnost, která je utvořena konkatenací posloupností x a z a připojením (na začátek) ještě jednoho členu $\overline{\text{`}\forall}$. Zápisy tvaru $\ulcorner . . \urcorner$, tj. výrazy vymezené „horními růžky“, umožňují vypustit hvězdičky, levé apostrofy a pruhy nad ciframi. K typu písma ještě poznamenejme, že například +, $\cdot$ a S jsou tytéž symboly jako $\mathtt{+}$, $\mathtt{\cdot}$ a $\mathtt{S}$. Strojopisnou verzi užíváme stejně jako v kapitole 2 tehdy, chceme-li zdůraznit, že opravdu jde o symboly. V zápisech typu $\ulcorner (u_1 \text{+} u_2) \urcorner$ a $\ulcorner \forall x z \urcorner$ umožňuje strojopisné písmo odlišit jednotlivé symboly od zkratek zastupujících posloupnosti symbolů.

Lemma 4.2.10 *(a)* $\mathbf{N} \models \mathsf{Var}(\overline{m})$*, právě když m je (ve smyslu kódování z tohoto oddílu) kódem nějaké proměnné.*

(b) $\mathbf{N} \models \mathsf{Term}(\overline{m})$*, právě když m je kódem nějakého termu.*

(c) $\mathsf{PA} \vdash \forall x_1 \forall x_2 (\mathsf{Term}(x_1) \;\&\; \mathsf{Term}(x_2) \to \mathsf{Term}(\ulcorner (x_1 \text{+} x_2) \urcorner) \;\&$
$\&\; \mathsf{Term}(\ulcorner (x_1 \cdot x_2) \urcorner) \;\&\; \mathsf{Term}(\ulcorner \mathtt{S}(x_1) \urcorner))$.

(d) $\mathsf{PA} \vdash \forall x (\mathsf{Term}(x) \to \mathsf{Var}(x) \vee x = \ulcorner \mathtt{0} \urcorner \vee \exists x_1 (\mathsf{Term}(x_1) \;\&\; x = \ulcorner \mathtt{S}(x_1) \urcorner) \vee$
$\vee \exists x_1 \exists x_2 (\mathsf{Term}(x_1) \;\&\; \mathsf{Term}(x_2) \;\&\; x = \ulcorner (x_1 \text{+} x_2) \urcorner \vee x = \ulcorner (x_1 \cdot x_2) \urcorner))$.

Důkaz Tvrzení (a) plyne z lemmatu 4.2.7, tj. z faktu, že všechny tři formule Seq, Lh a B použité k sestavení formule $\mathsf{Var}(v)$ definují v $\mathbf{N}$ to, co mají definovat.

Podívejme se na (c). Označme $\alpha(x, w)$ formuli $\mathsf{Seq}(w) \;\&\; \mathsf{Lh}(w, x + \overline{1}) \;\&\; (\ldots)$, kde závorka s tečkami označuje druhý až sedmý řádek ve formuli $\mathsf{Term}(x)$. Formule $\mathsf{Term}(x)$ je tedy ekvivalentní s $\exists w (\alpha(x, w) \;\&\; \mathsf{B}(w, x, \overline{1}))$. Formuli $\alpha(x, w)$ lze číst číslo w je dosvědčující posloupnost délky $x + \overline{1}$. Platí

$$\mathsf{PA} \vdash \exists w \alpha(0, w) \quad \text{a} \quad \mathsf{PA} \vdash \forall x (\exists w \alpha(x, w) \to \exists w' \alpha(x + \overline{1}, w')).$$

Přitom se uplatní 4.2.8(d)–(f) (viz též cvičení 9). Indukce dává

$$\mathsf{PA} \vdash \forall x \exists w \alpha(x, w). \tag{1}$$

Dále platí

$$\mathsf{PA} \vdash \forall x_1 \forall x_2 \forall w_1 \forall w_1 \forall y (y \le x_1 \;\&\; y \le x_2 \;\&\; \alpha(x_1, w_1) \;\&\; \alpha(x_2, w_2) \to$$
$$\to \forall u \le y (\mathsf{B}(w_1, u, \overline{1}) \equiv \mathsf{B}(w_2, u, \overline{1})). \tag{2}$$

Toto se rovněž dokáže indukcí (podle y s parametry x_1, x_2, w_1 a w_2). Z (2) plyne, že v každé dvojici dosvědčujících posloupností je některá z nich počátečním úsekem druhé. Uvažujme v PA:

> Nechť $\mathsf{Term}(x_1)$ a $\mathsf{Term}(x_2)$. Tedy existují čísla w_1 a w_2 taková, že $\alpha(x_1, w_1)$, $\alpha(x_2, w_2)$, $\mathsf{B}(w_1, x_1, \overline{1})$ a $\mathsf{B}(w_2, x_2, \overline{1})$. Vezměme posloupnost w takovou, že $\alpha(\ulcorner(x_1{+}x_2)\urcorner, w)$, tj. vezměme dosvědčující posloupnost délky $\ulcorner(x_1{+}x_2)\urcorner + \overline{1}$. Taková existuje dle (1). Z lemmatu 4.2.9 a z poznámky uvedené za tímto lemmatem plyne $x_1 < \ulcorner(x_1{+}x_2)\urcorner$ a $x_2 < \ulcorner(x_1{+}x_2)\urcorner$. Posloupnost w tedy přiřazuje nějaké hodnoty číslům x_1 a x_2. Dle (2) se w až do x_1 shoduje s w_1 a až do x_2 s w_2. Tedy $\mathsf{B}(w, x_1, \overline{1})$ a $\mathsf{B}(w, x_2, \overline{1})$. Užití poslední části formule α, začínající kvantifikátorem $\forall u$, na $u = \ulcorner(x_1{+}x_2)\urcorner$ dává $\mathsf{B}(w, \ulcorner(x_1{+}x_2)\urcorner, \overline{1})$. Tím jsme ověřili, že $\mathsf{Term}(\ulcorner(x_1{+}x_2)\urcorner)$.

Zbývající úvahy v (c) a (d) jsou podobné.

Vraťme se ještě krátce k tvrzení (b). Je-li m term, můžeme vzít posloupnost q délky $m+1$, která každému $j \leq m$ přiřazuje hodnotu 1 nebo 0 podle toho, je-li j termem. Musí platit $\mathbf{N} \models \alpha(\overline{m}, \overline{q})$ a $\mathbf{N} \models \mathsf{B}(\overline{m}, \overline{q}, \overline{1})$. Tedy $\mathbf{N} \models \mathsf{Term}(\overline{q})$. Když naopak q je takové, že $\mathbf{N} \models \alpha(\overline{m}, \overline{q})$ a $\mathbf{N} \models \mathsf{B}(\overline{m}, \overline{q}, \overline{1})$, pak ve skutečnosti (tj. na metamatematické úrovni) q je počátečním úsekem charakteristické funkce množiny všech termů přiřazující hodnotu 1 číslu m. Tedy m je term. QED

Podobně jako se to podařilo u proměnných a termů, můžeme zavést formule definující ostatní syntaktické pojmy a podmínky:

$\mathsf{Numeral}(x, y)$	y je x-tý numerál,
$\mathsf{FmAt}(z)$	z je atomická formule,
$\mathsf{Fm}(z)$	z je formule,
$\mathsf{SubT}(v, x, t, y)$	y je výsledek substituce termu t za proměnnou v v termu x,
$\mathsf{SubF}(v, z, t, y)$	y je výsledek substituce termu t za proměnnou v ve formuli z,
$\mathsf{OccT}(v, t)$	proměnná v se vyskytuje v termu t,
$\mathsf{OccF}(v, z)$	proměnná v má volné výskyty ve formuli z,
$\mathsf{Sent}(z)$	z je sentence,
$\mathsf{FreeSub}(v, z, t)$	t je term substituovatelný za v ve formuli z,
$\mathsf{LogAx}(z)$	z je logický axiom,
$\mathsf{UnivClo}(z, y)$	z je formule a y je její univerzální uzávěr.

Předpokládáme, že čtenář je schopen kteroukoliv z těchto deseti formulí zapsat pomocí formulí popisujících kódování posloupností a případně s užitím formulí, které se na seznamu vyskytují dříve. Například $\mathsf{Numeral}(x, y)$ je formule term y je onen term, který vznikne x-násobnou aplikací operace $v \mapsto \ulcorner\mathsf{S}(v)\urcorner$ z termu $\ulcorner\mathsf{0}\urcorner$, kdežto $\mathsf{UnivClo}(z, y)$ je formule číslo z je formule, číslo y je tvaru $\ulcorner u\overline{z}\urcorner$, kde u je posloupnost, která začíná kvantifikátorem a která má navíc vlastnost, že každá její podposloupnost

umístěná mezi dvěma kvantifikátory nebo za posledním kvantifikátorem je proměnná, která má volné výskyty v z.

Můžeme-li mluvit o substituovatelnosti termů, snadno aritmetickou formulí vyjádříme, že formule z je logickým axiomem tvaru B1:

$$\exists v \exists x \exists t \exists y (\mathsf{FreeSub}(v,x,t) \ \&\ \mathsf{SubF}(v,x,t,y) \ \&\ z = \ulcorner (\forall v x \to y) \urcorner).$$

Naprosto analogicky popíšeme schéma B2. Pak už snadno zapíšeme formulí, že z je logickým axiomem: $\mathsf{LogAx}(z)$, jestliže z má jeden z tvarů B1, B2, A1–A7, E1–E5.

Věta 4.2.11 *(a) Všechny dosud utvořené formule definují příslušné pojmy v* $\mathbf{N}$. *Například* $\mathbf{N} \models \mathsf{Fm}(\overline{\varphi})$, *právě když* φ *je (číselný kód) formule, a* $\mathbf{N} \models \mathsf{LogAx}(\overline{\varphi})$, *právě když* φ *je logický axiom (jazyka aritmetiky).*

(b) Triviální fakty o syntaktických objektech analogické tvrzením 4.2.10 (c) a (d) jsou dokazatelné v PA. *Například:*

- Konjunkcí, disjunkcí, implikací, negací a kvantifikací z formulí vzniknou opět formule.
- Každá formule je atomická, nebo má některý z tvarů $\ulcorner \neg z_1 \urcorner$, $\ulcorner \forall v z_1 \urcorner$, $\ulcorner \exists v z_1 \urcorner$, $\ulcorner (z_1 \to z_2) \urcorner$, $\ulcorner (z_1 \& z_2) \urcorner$, nebo $\ulcorner (z_1 \vee z_2) \urcorner$, kde z_1 je formule resp. z_1 a z_2 jsou formule.

(c) U těch formulí, které definují graf funkce, lze i v PA *dokázat, že definují graf funkce:*

- $\mathsf{PA} \vdash \forall x \exists ! y \mathsf{Numeral}(x,y)$,
- $\mathsf{PA} \vdash \forall v \forall x \forall t \exists ! y \mathsf{SubT}(v,x,t,y)$,
- $\mathsf{PA} \vdash \forall v \forall z \forall t \exists ! y \mathsf{SubF}(v,z,t,y)$,
- $\mathsf{PA} \vdash \forall z \exists ! y \mathsf{UnivClo}(z,y)$.

Důkaz Formulí Term jsme se dost podrobně zabývali v 4.2.10. Všechna tvrzení v (a) se dokáží víceméně stejně jako v 4.2.10(b) a všechna tvrzení v (b) se dokáží víceméně stejně jako v 4.2.10 (c) a (d). Tvrzení (c) je analogické tvrzení 4.2.8(b) (o jednoznačnosti délky posloupnosti). QED

Tím jsme v aritmetizaci logické syntaxe dospěli k důkazům a dokazatelnosti. Postupujeme opět stejně jako v důkazu věty 3.6.6. Chceme vyjádřit formulí, že *důkaz* je číslo tvaru $\ulcorner z_1 \# z_2 \# \ldots \# z_t \urcorner$, kde každá podposloupnost z_v je formule, která je z některých předchozích formulí odvozena tak, jak se požaduje v definici hilbertovského kalkulu, přičemž počet t formulí v důkazu w může být libovolné (formální!) číslo. Formule $\mathsf{Beg}(w_1, w)$ říká, že posloupnosti w_1 a w jsou totožné, nebo posloupnost w_1 lze z w získat odstraněním všech členů od některého členu $\overline{\#}$ do konce. Formule $\mathsf{Ends}(w,x)$ říká, že posloupnost x neobsahuje člen $\overline{\#}$, a je buď rovna posloupnosti w, nebo ji lze z w získat odstraněním počátečních členů až do některého členu $\overline{\#}$. Je-li w důkazem, pak formuli $\mathsf{Beg}(w_1, w)$ lze číst důkaz w_1 je počátečním úsekem důkazu w, kdežto formuli $\mathsf{Ends}(w,x)$ lze číst formule x je poslední formulí důkazu w.

Nechť nyní $\tau(z)$ je formule s jednou volnou proměnnou. S pomocí formulí $\mathsf{Beg}(w_1, w)$ a $\mathsf{Ends}(w, x)$ definujme formuli $\mathsf{Proof}_\tau(x, w)$:

$$\begin{aligned}&\mathsf{Ends}(w,x)\ \&\ \forall w_1\forall z(\mathsf{Beg}(w_1,w)\ \&\ \mathsf{Ends}(w_1,z)\ \to\ \mathsf{Fm}(z)\ \&\\ &\quad\&\ (\exists w_2\exists z_1\exists z_2\exists v(\mathsf{Fm}(z_1)\ \&\ \mathsf{Fm}(z_2)\ \&\ \mathsf{Var}(v)\ \&\\ &\qquad\qquad\&\ \mathsf{Beg}(w_2,w_1)\ \&\ \mathsf{Ends}(w_2,\ulcorner(z_1\to z_2)\urcorner)\ \&\ \neg\mathsf{OccF}(v,z_1)\ \&\\ &\qquad\qquad\&\ z=\ulcorner(z_1\to\forall v z_2)\urcorner)\ \vee\\ &\qquad\vee\ (\ldots\text{ podobně pro pravidla Gen-E a MP }\ldots)\ \vee\\ &\qquad\vee\ \mathsf{LogAx}(z)\ \vee\ (\tau(z)\ \&\ \mathsf{Sent}(z)))).\end{aligned}$$

Formule τ vystupuje ve formuli $\mathsf{Proof}_\tau(x, w)$ jako podformule, která popisuje množinu předpokladů. Formuli $\mathsf{Proof}_\tau(x, w)$ čteme číslo w je důkaz formule x, případně podrobněji číslo w je důkaz formule x z množiny předpokladů $\{\, z\,;\, \tau(z)\ \&\ \mathsf{Sent}(z)\,\}$.

Věta 4.2.12 *Nechť formule τ definuje v $\mathbf{N}$ množinu axiomů teorie T. Pak formule $\mathsf{Proof}_\tau(x, w)$ definuje v $\mathbf{N}$ relaci $\{\,[\varphi, d]\,;\, d$ je důkaz formule φ v $T\,\}$, tj. podmínku* $\mathrm{Proof}(\varphi, d)$.

E

Důkaz je analogický jako v 4.2.11(a), 4.2.10 (a) a (b) a v řadě podobných tvrzení uvedených dříve.

Máme-li pojem důkazu, můžeme v aritmetickém jazyce mluvit i o *dokazatelnosti* a *bezespornosti*:

$$\mathsf{Pr}_\tau(x)\ \equiv\ \exists w\mathsf{Proof}_\tau(x,w),\qquad \mathsf{Con}(\tau)\ \equiv\ \neg\mathsf{Pr}_\tau(\overline{0=\mathrm{S}(0)}).$$

Formule x je dokazatelná, má-li nějaký důkaz, a množina $\{\, z\,;\, \tau(z)\ \&\ \mathsf{Sent}(z)\,\}$ je bezesporná, není-li z ní dokazatelná sentence $0 = \mathrm{S}(0)$, o které jsme se tedy tímto rozhodli, že reprezentuje spor.

Dále se domluvme na tom, jak popíšeme rozšíření teorie přidáním jednoho axiomu a jak aritmetickými formulemi popíšeme axiomatiku teorií Q a PA.

Nechť $\tau(z)$ je formule s jednou volnou proměnnou z. Označme $(\tau + y)$ formuli $\tau(z)\ \vee\ z = y$. Formule $\mathsf{Proof}_{(\tau+y)}(x, w)$, $\mathsf{Pr}_{(\tau+y)}(x)$ a $\mathsf{Con}(\tau + y)$ (zde jeden pár závorek vynecháváme) připouštějí jako axiomy kromě formálních sentencí s vlastností τ i předpoklad y, pokud ovšem y je také (formální) sentencí.

Je-li F konečná množina aritmetických sentencí, $F = \{\varphi_1, .., \varphi_n\}$, pak $[F](z)$ označuje formuli $z = \overline{\varphi_1} \vee .. \vee z = \overline{\varphi_n}$. Domluvme se, že je-li $[F]$ v indexu u formule Proof nebo Pr nebo v závorce u sentence Con, vynecháváme hranaté závorky. Formule $\mathsf{Proof}_{\mathsf{Q}}(x, w)$ tedy vyjadřuje, že číslo w je důkazem formule x v Robinsonově aritmetice. Axiomy Peanovy aritmetiky popišme následující formulí, kterou označme $\pi(z)$:

$$\begin{aligned}&[\mathsf{Q}](z)\ \vee\ \exists u\exists u_1\exists u_2\exists y\exists v\exists t_1\exists t_2(\mathsf{Var}(v)\ \&\ t_1=\ulcorner\mathsf{0}\urcorner\ \&\ t_2=\ulcorner\mathsf{S}(v)\urcorner\ \&\\ &\qquad\qquad\&\ \mathsf{SubF}(v,u,t_1,u_1)\ \&\ \mathsf{SubF}(v,u,t_2,u_2)\ \&\\ &\qquad\qquad\&\ y=\ulcorner((u_1\&\forall v(u\to u_2))\to\forall v u)\urcorner\ \&\ \mathsf{UnivClo}(y,z)),\end{aligned}$$

formule z je axiomem Peanovy aritmetiky, je-li axiomem Robinsonovy aritmetiky nebo je-li axiomem indukce, tj. univerzálním uzávěrem nějaké formule y tvaru $\ulcorner((u_1\&\forall v(u\to u_2))\to\forall v u)\urcorner$, kde formule u_1 a u_2 jsou výsledky substituce termu $\ulcorner\mathsf{0}\urcorner$ resp. termu $\ulcorner\mathsf{S}(v)\urcorner$ za proměnnou v ve formuli u.

Věta 4.2.13 *(a) Když formule τ definuje v $\mathbf{N}$ množinu axiomů teorie T, pak formule $\mathsf{Pr}_\tau(x)$ definuje množinu $\mathrm{Thm}(T)$. Když navíc φ je libovolná sentence, pak formule $(\tau+\overline{\varphi})$ definuje množinu axiomů teorie $(T+\varphi)$ a formule $\mathsf{Pr}_{(\tau+\overline{\varphi})}(x)$ definuje množinu $\mathrm{Thm}(T+\varphi)$.*

(b) Formule $[\mathsf{Q}](z)$ a $\pi(z)$ definují množinu axiomů teorie Q resp. PA. Obecně každá formule $[F](z)$, kde F je konečná množina sentencí, definuje množinu F.

(c) Formule $\mathsf{Pr}_\mathsf{Q}(x)$ a $\mathsf{Pr}_\pi(x)$ definují množiny $\mathrm{Thm}(\mathsf{Q})$ a $\mathrm{Thm}(\mathsf{PA})$. Obecně je-li F konečná množina sentencí, pak formule $\mathsf{Pr}_F(x)$ definuje množinu $\mathrm{Thm}(F)$.

(d) $\mathbf{N}\models\mathsf{Con}(\mathsf{Q})$ a $\mathbf{N}\models\mathsf{Con}(\pi)$.

Důkaz Pro libovolnou sentenci φ platí

$$\begin{aligned} T\vdash\varphi &\Leftrightarrow \text{existuje důkaz } d \text{ formule } \varphi \text{ z předpokladů } T\\ &\Leftrightarrow \exists d(\mathbf{N}\models\mathsf{Proof}_\tau(\overline{\varphi},\overline{d}))\\ &\Leftrightarrow \mathbf{N}\models\exists w\mathsf{Proof}_\tau(\overline{\varphi},w),\end{aligned}$$

kde druhá ekvivalence plyne z 4.2.12. Tím jsme dokázali první část tvrzení (a). Druhá část a (b) jsou jasné. Tvrzení (c) plyne z (a) a (b). Protože PA je bezesporná teorie (neboť $\mathbf{N}$ je jejím modelem), žádné číslo d není důkazem sentence $0=\mathrm{S}(0)$. Protože formule $\mathsf{Proof}_\pi(x,w)$ definuje podmínku $\mathrm{Proof}_T(\varphi,d)$, máme E

$$\forall d(\mathbf{N}\models\neg\mathsf{Proof}_\pi(\overline{0=\mathrm{S}(0)},\overline{d}))\quad\text{a}\quad\mathbf{N}\models\forall w\neg\mathsf{Proof}_\pi(\overline{0=\mathrm{S}(0)},w).$$

Úvaha pro teorii Q je úplně stejná. QED

Věta 4.2.14 *(a)* $\mathsf{PA}\vdash\forall x(\mathsf{LogAx}(x)\vee(\tau(x)\,\&\,\mathsf{Sent}(x))\to\mathsf{Pr}_\tau(x))$.

(b) $\mathsf{PA}\vdash\forall x\forall y(\mathsf{Pr}_\tau(x)\,\&\,\mathsf{Pr}_\tau(\ulcorner(x\to y)\urcorner)\to\mathsf{Pr}_\tau(y))$.

(c) $\mathsf{PA}\vdash\forall x(\tau_1(x)\,\&\,\mathsf{Sent}(x)\to\mathsf{Pr}_{\tau_2}(x))\to\forall x(\mathsf{Pr}_{\tau_1}(x)\to\mathsf{Pr}_{\tau_2}(x))$.

(d) Když $\mathsf{PA}\vdash\mathsf{Pr}_\tau(\overline{\alpha_i})$ *pro každý z devíti axiomů $\alpha_1,\ldots,\alpha_9$ Robinsonovy aritmetiky, pak* $\mathsf{PA}\vdash\forall x(\mathsf{Pr}_\mathsf{Q}(x)\to\mathsf{Pr}_\tau(x))$.

(e) $\mathsf{PA}\vdash\forall x(\mathsf{Pr}_\mathsf{Q}(x)\to\mathsf{Pr}_\pi(x))$.

(f) $\mathsf{PA}\vdash\forall x\forall y(\mathsf{Sent}(y)\to(\mathsf{Pr}_{(\tau+y)}(x)\equiv\mathsf{Pr}_\tau(\ulcorner(y\to x)\urcorner)))$.

(g) $\mathsf{PA}\vdash\neg\mathsf{Con}(\tau)\equiv\forall x\mathsf{Pr}_\tau(x)$.

(h) $\mathsf{PA}\vdash\forall y(\mathsf{Sent}(y)\to(\mathsf{Con}(\tau+y)\equiv\neg\mathsf{Pr}_\tau(\ulcorner\neg y\urcorner)))$.

Důkaz Snadno lze ověřit $\mathsf{PA}\vdash\forall x(\tau(x)\,\&\,\mathsf{Sent}(x)\to\mathsf{Proof}_\tau(x,x))$:

Platí-li $\mathsf{Beg}(w_1, x)$ a $\mathsf{Ends}(w_1, z)$, tj. je-li z na konci některého počátečního úseku posloupnosti x, pak z splňuje disjunkci $(\ldots)\vee\mathsf{LogAx}(z)\vee(\tau(z)\&\mathsf{Sent}(z))$, neboť jediné takové z je x a x splňuje některý ze dvou posledních členů.

Podobně snadno se dokáže tvrzení (b):

Je-li $\mathsf{Proof}_\tau(x, w_1)$ a $\mathsf{Proof}_\tau(\ulcorner(x{\to}y)\urcorner, w_2)$, pak $\mathsf{Proof}_\tau(y, \ulcorner w_1\#w_2\#y\urcorner)$.

V (c) užijeme indukci:

Předpokládejme $\forall z(\tau_1(z)\ \&\ \mathsf{Sent}(z) \to \mathsf{Pr}_{\tau_2}(z))$ a $\mathsf{Proof}_{\tau_1}(x, w)$. Dokažme $\forall y\forall w_1\forall z(\mathsf{Beg}(w_1, w)\,\&\,\mathsf{Ends}(w_1, z)\,\&\,\mathsf{Lh}(w_1, y) \to \mathsf{Pr}_{\tau_2}(z))$ indukcí dle y. Platí-li $\tau_1(z)\,\&\,\mathsf{Sent}(z)$, pak $\mathsf{Pr}_{\tau_2}(z)$ dle předpokladu. Je-li $\mathsf{LogAx}(z)$, pak $\mathsf{Pr}_{\tau_2}(z)$ dle (a). Je-li z odvozena z předchozích členů $\ulcorner(z_1{\to}z)\urcorner$ a z_1 pomocí pravidla MP, pak počáteční úseky důkazu w_1 končící formulemi $\ulcorner(z_1{\to}z)\urcorner$ a z_1 mají délku menší než y, takže na ně lze užít indukční předpoklad. Tedy $\mathsf{Pr}_{\tau_2}(z_1)$ a $\mathsf{Pr}_{\tau_2}(\ulcorner(z_1{\to}z)\urcorner)$. Z toho plyne $\mathsf{Pr}_{\tau_2}(z)$ díky již dokázanému tvrzení (b). Zbývající dva případy, kdy z je odvozena z předchozích členů pomocí pravidla Gen-A nebo Gen-E, jsou analogické.

Všimněme si, že tvrzení (b) je formalizací pravidla MP. Dvě analogická tvrzení týkající se pravidel Gen-A a Gen-E jsme pro stručnost vynechali, ale v předchozím důkazu tvrzení (c) jsme je použili. Tvrzení (f) lze označit jako formalizovanou větu o dedukci a lze je dokázat podobně jako tvrzení (c), tj. formalizací běžného důkazu věty o dedukci známého z kapitoly 3. Jsou-li $\alpha_1, \ldots, \alpha_9$ axiomy Robinsonovy aritmetiky, pak $\mathsf{PA} \vdash \forall x([\mathsf{Q}](x)\ \&\ \mathsf{Sent}(x) \to x = \overline{\alpha_1} \vee \ldots \vee x = \overline{\alpha_9})$. Z toho a z (c) plyne (d). Tvrzení (e) plyne z (d) volbou $\tau := \pi$. Tvrzení (g) a (h) lze dokázat „přeříkáním v PA“ příslušných důkazů z 3.2.7. QED

Peanova aritmetika tedy ví o platnosti nejzákladnějších faktů z predikátové logiky, jako je věta o dedukci nebo fakt, že PA není slabší teorií než Q. A ví to proto, že příslušné důkazy v ní lze formalizovat.

V tomto oddílu se vyskytla také dvě tvrzení, která lze celkem lehko dokázat, ale jejichž běžné důkazy nejsou čistě syntaktické. Jde o tvrzení Robinsonova aritmetika je bezesporná a o tvrzení Peanova aritmetika je bezesporná vyjádřená sentencemi $\mathsf{Con}(\mathsf{Q})$ a $\mathsf{Con}(\pi)$. Vypadá to, že k jejich formalizaci uvnitř PA bychom potřebovali formalizovat v PA také logickou sémantiku. Formalizovat v PA logickou sémantiku nebo alespoň její vhodnou část a dokázat tak v PA bezespornost teorií Q a PA — je to rozumný plán, který poskytne žádoucí a očekávané výsledky? Varujeme čtenáře před ukvapenou odpovědí. S „ano“ se celkem dá souhlasit a něco v tomto směru v příštích oddílech uděláme. Ale případný důkaz, že některá ze sentencí $\mathsf{Con}(\mathsf{Q})$ a $\mathsf{Con}(\pi)$ je v PA nedokazatelná, by také byl žádoucím výsledkem, protože by znamenal (negativní) odpověď na otázku, zda PA je úplná. Z věty 4.2.13(d) víme, že obě sentence $\mathsf{Con}(\mathsf{Q})$ a $\mathsf{Con}(\pi)$ platí v $\mathbf{N}$. Položme si tedy otázky:

- *Platí* $\mathsf{PA} \vdash \mathsf{Con}(\mathsf{Q})$ *nebo* $\mathsf{PA} \vdash \mathsf{Con}(\pi)$*?*

Podobně jako jsme to udělali pro aritmetický jazyk a teorie Q a PA, lze v PA formalizovat i dokazatelnost v jakékoliv jiné teorii (s konečným jazykem), například v teorii množin. O tom a o dokazatelnosti bezespornosti teorie množin v Peanově aritmetice nebo v samotné teorii množin se v dalším výkladu ještě zmíníme.

Neklademe si otázku, zda nějaké tvrzení vyjadřující bezespornost je dokazatelné už v Q. Logickou syntax jsme se rozhodli formalizovat v Peanově aritmetice, ačkoliv je známo, že to není poslední slovo. Všude, kde ve větě 4.2.14 stojí „PA“ vlevo od znaku „$\vdash$“, by mohla stát mnohem slabší teorie než PA. A po určitých (spíše značných) modifikacích dokazovaných sentencí by tam dokonce mohlo stát „Q“. O tom jsou například Pudlákovy články [68] a [67] nebo článek Wilkieho a Parise [98]. Ale dokud to není učiněno, tj. dokud uvnitř nějaké teorie T není dokázáno, že dokazatelnost má obvyklé vlastnosti, nemá asi smysl se ptát, zda v T je dokazatelné jakékoliv tvrzení vyjadřující bezespornost.

Zalistujeme-li ještě jednou v tomto oddílu, můžeme si všimnout, že všechna tvrzení lze rozdělit do dvou skupin. Tvrzení 4.2.14 a předtím 4.2.2 (a) a (b), 4.2.3(a), 4.2.4, 4.2.5, 4.2.6, 4.2.8, 4.2.9, 4.2.10 (c) a (d) a 4.2.11 (b) a (c) se týkají *dokazatelnosti obecných faktů* o množinách, posloupnostech a syntaktických objektech. A tvrzení 4.2.12 a 4.2.13 a předtím 4.2.2(c), 4.2.3(b), 4.2.7, 4.2.10 (a) a (b) a 4.2.11(a) se týkají *platnosti numerických instancí* různých formulí ve struktuře $\mathbf{N}$. Víme například, kdy v $\mathbf{N}$ platí sentence $\mathsf{Pr}_\pi(\overline{n})$: právě tehdy, když n je (numerickým kódem) formule, která je ve skutečnosti dokazatelná v PA. Nezabývali jsme se ale dokazatelností numerických instancí. Víme-li například $\mathsf{PA} \nvdash \overline{3}+\overline{2}=\overline{4}$ (což víme), znamená to, že platí také $\mathsf{PA} \vdash \neg\mathsf{Pr}_\pi(\overline{\overline{3}+\overline{2}=\overline{4}})$? A víme-li, že $\mathsf{PA} \vdash \overline{3}+\overline{2}=\overline{5}$ (což ponecháváme jako cvičení), znamená to, že platí i $\mathsf{PA} \vdash \mathsf{Pr}_\pi(\overline{\overline{3}+\overline{2}=\overline{5}})$? Tyto otázky lze zobecnit:

- *Když $\tau(z)$ definuje v $\mathbf{N}$ množinu axiomů teorie T, jaký je vztah mezi podmínkami $T \vdash \varphi$ a $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi})$?*
- *Když $\tau(z)$ definuje v $\mathbf{N}$ množinu axiomů teorie T, jaký je vztah mezi podmínkami $T \nvdash \varphi$, $\mathsf{PA} \nvdash \mathsf{Pr}_\tau(\overline{\varphi})$ a $\mathsf{PA} \vdash \neg\mathsf{Pr}_\tau(\overline{\varphi})$?*

Některé odpovědi jsou zřejmé. Například když $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi})$, pak sentence $\mathsf{Pr}_\tau(\overline{\varphi})$ platí v každém modelu teorie PA, tedy i v $\mathbf{N}$. Věta 4.2.13(a) říká, že platí-li sentence $\mathsf{Pr}_\tau(\overline{\varphi})$ v $\mathbf{N}$, pak $T \vdash \varphi$. Další odpovědi se dozvíme v následujících oddílech. Je také zřejmé, že otázky, zda $\mathsf{PA} \vdash \neg\mathsf{Pr}_\pi(\overline{\varphi})$ pro určitou sentenci φ, souvisejí s výše zmíněnou otázkou, zda $\mathsf{PA} \vdash \mathsf{Con}(\pi)$. Z tvrzení 4.2.14(h) totiž plyne, že $\mathsf{PA} \vdash \neg\mathsf{Pr}_\pi(\overline{\varphi}) \to \mathsf{Con}(\pi)$ pro každou aritmetickou sentenci φ.

Cvičení

1. Formuli $\forall x \forall y(x \cdot x = \overline{2} \cdot y \cdot y \to x = 0 \ \&\ y = 0)$ lze číst číslo $\sqrt{2}$ je iracionální. Dokažte ji v PA.
2. Nalezněte všechny prvky čísla $q = (24, 29\,341)$. Je q kódem množiny či posloupnosti?

3. Dokažte zbývající případy v 4.2.2(a): levý člen konjunkce a jednoznačnost v pravém členu.

4. Dokažte v PA, že podmínky $\mathsf{RPrime}(a,b)$ a $\forall x(x \mid a \ \&\ x \mid b \to x = \overline{1})$ jsou za předpokladu $a \neq 0$ ekvivalentní.

   Návod. Při důkazu implikace $\Leftarrow$ (v němž se předpoklad $a \neq 0$ neuplatní) užijte Bezoutovu větu na dvojici $[a,b]$.

5. Definujte v PA největšího společného dělitele $\mathsf{D}(a,b)$ čísel a a b:

$$\mathsf{D}(a,b) = c \equiv c \mid a \ \&\ c \mid b \ \&\ \forall v(v \mid a \ \&\ v \mid b \to v \mid c).$$

   Dokažte v PA, že tato definice je korektní, tj. že ke každé dvojici a, b existuje právě jedno c splňující podmínku na pravé straně ekvivalence. Dokažte dále, že nahradíme-li ve formulích Ax1–Ax5 v Úvodu na str. 9 symboly $\leq$, $\cdot$ a $+$ symboly $|$, D a $\cdot$, pak v PA lze dokázat, že výsledné formule pro nenulová čísla platí. Zdůvodněte, že distributivní pravidlo $\mathsf{D}(a \cdot c, b \cdot c) = \mathsf{D}(a,b) \cdot c$ je v PA dokazatelné pro všechna a, b a c.

6. Na předchozím cvičení lze založit alternativní důkaz tvrzení z cvičení 4:

   Nechť $a \mid b \cdot x$, $a \neq 0$, $x \neq 0$. Vezměme d takové, že $d = \mathsf{D}(a,x)$, a vezměme v takové, že $d \cdot v = a$. Platí $\mathsf{D}(a \cdot b, b \cdot x) = d \cdot b$. Tedy $a \mid d \cdot b$. Z toho a z podmínek $d \cdot v = a$ a $D(a,b) = \overline{1}$ plyne $v = \overline{1}$. Tedy $d = a$ a $a = \mathsf{D}(a,x)$. Takže $a \mid x$.

   Domyslete a dokončete!

7. Dokažte v PA formuli $\forall x \forall y \forall z(\mathsf{RPrime}(x,y) \ \&\ x \mid z \ \&\ y \mid z \to x \cdot y \mid z)$.

8. Zdůvodněte, že číslo q z příkladu 4.2.1 je nejmenším přirozeným číslem, jehož prvky jsou 1, 4 a 5, a že tedy q je množinou.

9. Dokažte v PA formuli

$$\forall w \forall x \forall y \exists w'(\mathsf{Seq}(w) \ \&\ \mathsf{Lh}(w,y) \to \mathsf{Seq}(w') \ \&\ \mathsf{Lh}(w', y+\overline{1}) \\ \&\ \forall u{<}y \forall v(\mathsf{B}(w,u,v) \equiv \mathsf{B}(w',u,v)) \ \&\ \mathsf{B}(w',y,x)).$$

10. Zdůvodněte, že pro každý z axiomů $\alpha_1, \ldots, \alpha_9$ Robinsonovy aritmetiky platí $\mathsf{PA} \vdash \mathsf{Pr}_\pi(\overline{\alpha_i})$. Ukažte na místo v důkazu věty 4.2.14, kde bylo toto tvrzení použito.

11. Jestliže sentence $\mathsf{Con}(\pi)$ je v PA dokazatelná, pak i sentence $\mathsf{Con}(\mathsf{Q})$ je v PA dokazatelná, a to proto, že $\mathsf{PA} \vdash \mathsf{Con}(\pi) \to \mathsf{Con}(\mathsf{Q})$. Dokažte.

12. Nechť formule $\tau(z)$ definuje množinu axiomů teorie T v $\mathbf{N}$. Zdůvodněte implikace $\mathsf{PA} \vdash \neg\mathsf{Pr}_\tau(\overline{\varphi}) \Rightarrow T \not\vdash \varphi$ a $T \not\vdash \varphi \Rightarrow \mathsf{PA} \not\vdash \mathsf{Pr}_\tau(\overline{\varphi})$.

4.3 Hierarchie aritmetických formulí

V tomto oddílu se budeme zabývat otázkami, jaké množiny přirozených čísel jsou definovatelné ve struktuře **N** a jak složité jsou formule, které je definují. Nejprve uvažujme o syntaktické složitosti aritmetických formulí. Stejně jako v kapitole 2 přijímáme hledisko, že syntaktická složitost formule je především dána střídáním kvantifikátorů.

Definice 4.3.1 *Řekneme, že aritmetická formule φ je utvořena z formule ψ* omezenou kvantifikací*, jestliže φ má jeden z tvarů*

$$\forall v(v < x \to \psi), \quad \exists v(v < x \ \&\ \psi), \quad \forall v(v \leq x \to \psi), \quad \exists v(v \leq x \ \&\ \psi), \qquad (*)$$

kde v a x jsou různé *proměnné. Formule $(*)$ zapisujeme $\forall v{<}x\,\psi$, $\exists v{<}x\,\psi$, $\forall v{\leq}x\,\psi$ resp. $\exists v{\leq}x\,\psi$. Zápisy „$\forall v{<}x$“, „$\exists v{<}x$“, „$\forall v{\leq}x$“ a „$\exists v{\leq}x$“ nazýváme* omezené kvantifikátory*. Aritmetická formule je* omezená*, jestliže obsahuje pouze omezené kvantifikátory. Množinu všech omezených formulí značíme Δ_0. Místo omezená formule říkáme také* Δ_0-formule*.*

Netvrdí se, že omezená formule obsahuje nějaké (omezené) kvantifikátory. Tvrdí se ale, že neobsahuje žádné jiné kvantifikátory než omezené, čili že neobsahuje neomezené kvantifikátory. Například formule $\mathsf{Pair}(z,t,w)$ je omezená, protože neobsahuje vůbec žádné kvantifikátory. Formule $\exists v(v \cdot x = y)$, kterou zkráceně zapisujeme $x \mid y$, omezená není. Je ale v PA ekvivalentní s formulí $\exists v{\leq}y\,(v \cdot x = y)$, která omezená je. U formule tvaru například $\forall v{\leq}x\,\psi$, která vznikla z ψ omezenou kvantifikací, je samozřejmě přípustné, aby proměnné v a x měly volné výskyty ve formuli ψ. Formuli tvaru $\forall v(v \leq v \to \psi)$ pochopitelně neuznáváme za formuli, která vznikla z ψ pomocí omezené kvantifikace. Všimněme si dále, že omezené kvantifikátory očekávaným způsobem interagují s negací: například formule $\neg\forall v{\leq}x\,\psi$ je v PA (a dokonce už v predikátové logice) ekvivalentní s $\exists v{\leq}x\,\neg\psi$ atd. Význam omezených formulí je zejména v tom, že úloha, zda daná omezená formule je v **N** splněna daným ohodnocením proměnných, je algoritmicky rozhodnutelná. K tomu se ještě vrátíme.

Definice 4.3.2 *Řekneme, že formule φ je* Σ-formule*, jestliže φ je sestavena z omezených formulí pomocí konjunkce, disjunkce, existenční kvantifikace a libovolné omezené kvantifikace. Formule φ je Σ_n, kde $n \geq 0$, je-li je tvaru $\exists v_1 \forall v_2 \exists \ldots v_n \theta$, kde $\theta \in \Delta_0$. Formule φ je Π_n, kde $n \geq 0$, je-li naopak tvaru $\forall v_1 \exists v_2 \forall \ldots v_n \theta$, kde $\theta \in \Delta_0$. Nechť T je teorie s (alespoň) aritmetickým jazykem a nechť Γ je některá z množin Δ_0, Σ, Σ_n nebo Π_n. Řekneme, že φ* je Γ-formule v T*, jestliže existuje formule $\psi \in \Gamma$ taková, že $T \vdash \varphi \equiv \psi$. Řekneme, že φ je Δ_n-formule v T, jestliže φ je zároveň Σ_n i Π_n v T. Množinu všech formulí, které jsou Γ-formulemi v T, kde Γ je Δ_0, Σ, Σ_n, Π_n nebo Δ_n, značíme $\Gamma(T)$.*

Takže Σ_n-formule či Π_n-formule je taková formule, která je utvořena z Δ_0-formule pomocí n střídajících se kvantifikátorů, z nichž první zleva je existenční resp.

univerzální a poslední (úplně vnitřní) je takový nebo onaký podle toho, je-li n sudé nebo liché. Platí $\Sigma_0 = \Pi_0 = \Delta_0$. Dále Σ_{n+1}-formule (Π_{n+1}-formule) jsou přesně ty, které vznikly pomocí jednoho existenčního (univerzálního) kvantifikátoru z Π_n-formulí resp. ze Σ_n-formulí. Formule $x \mid y$ je Δ_0 v PA. Rovněž formule $\mathsf{Prime}(x)$ je Δ_0 v PA, neboť je ekvivalentní s formulí

$$x > \overline{1} \;\&\; \forall u{\leq}x \forall v{<}x\,(u \cdot v = x \;\rightarrow\; v = \overline{1}),$$

která je omezená. Všimněme si také, že množina $\Delta_0(T)$ je v 4.3.2 definována dvakrát, ale shodně: $\Delta_0(T)$ v druhém významu je $\Sigma_0(T) \cap \Pi_0(T)$, ale $\Sigma_0(T)$- i $\Pi_0(T)$-formule jsou formule vzniklé z $\Delta_0(T)$-formulí (v prvním významu) pomocí nulového počtu střídajících se kvantifikátorů.

Je jasné, že když teorie T obsahuje PA (tj. když PA je podteorií teorie T), pak $\Gamma(\mathsf{PA}) \subseteq \Gamma(T)$, neboli každá formule, která je Γ-formulí v PA, je zároveň Γ-formulí v T. Vzhledem k tomuto faktu formulujeme lemma 4.3.4 pouze pro množiny formulí tvaru $\Gamma(\mathsf{PA})$. V důkazu lemmatu 4.3.4 budeme potřebovat následující tvrzení o dokazatelnosti schématu B, které se nazývá *schématem kolekce*.

Lemma 4.3.3 *Každá instance schématu*

B: $\quad \forall \underline{y} \forall z(\forall u{<}z\, \exists v \varphi(u, v, \underline{y}) \;\rightarrow\; \exists w \forall u{<}z\, \exists v{<}w\, \varphi(u, v, \underline{y}))$

je dokazatelná v PA.

Důkaz Následující důkaz je možná čtenáři velice povědomý, protože schéma B se již vyskytlo ve cvičeních oddílu 4.1.

> Postupujme indukcí podle z. Je-li $z = 0$, pak podmínka $\forall u{<}z\, \exists v{<}w\, \varphi(u, v, \underline{y})$ platí bez ohledu na w. Nechť $\forall u{<}(z{+}\overline{1})\, \exists v \varphi(u, v, \underline{y})$. Pak $\forall u{<}z\, \exists v \varphi(u, v, \underline{y})$ a zároveň $\exists v \varphi(z, v, \underline{y})$. Zvolme w_0 takové, že $\forall u{<}z\, \exists v{<}w_0\, \varphi(u, v, \underline{y})$. Takové w_0 existuje dle indukčního předpokladu. Zvolme v_0 takové, že $\varphi(z, v_0, \underline{y})$. Pak pro libovolné číslo w takové, že $w \geq w_0$ a $w > v_0$, platí $\forall u{<}(z{+}\overline{1})\, \exists v{<}w\, \varphi(u, v, \underline{y})$.

QED

Lemma 4.3.4 *(a)* $\Sigma_n(\mathsf{PA}) \cup \Pi_n(\mathsf{PA}) \subseteq \Sigma_{n+1}(\mathsf{PA}) \cap \Pi_{n+1}(\mathsf{PA})$

(b) Když $\varphi \in \Sigma_n(\mathsf{PA})$*, pak* $\neg\varphi \in \Pi_n(\mathsf{PA})$*. Když* $\varphi \in \Pi_n(\mathsf{PA})$*, pak* $\neg\varphi \in \Sigma_n(\mathsf{PA})$*.*

(c) Konjunkce, disjunkce a omezená kvantifikace užitá na $\Sigma_n(\mathsf{PA})$*-formule nebo na* $\Pi_n(\mathsf{PA})$*-formule dává formuli, která je* PA*-ekvivalentní se* Σ_n*- resp. s* Π_n*-formulí. Jinými slovy, každá z množin* $\Sigma_n(\mathsf{PA})$ *i* $\Pi_n(\mathsf{PA})$ *je uzavřena na konjunkci, disjunkci a omezenou kvantifikaci.*

(d) Je-li $n \geq 1$*, pak množina* $\Sigma_n(\mathsf{PA})$ *je uzavřena na existenční kvantifikaci a množina* $\Pi_n(\mathsf{PA})$ *je uzavřena na univerzální kvantifikaci.*

(e) Všechny množiny $\Delta_n(\mathsf{PA})$ *jsou uzavřeny na logické spojky a na omezenou kvantifikaci.*

(f) Každá Σ*-formule je zároveň v* $\Sigma_1(\mathsf{PA})$*.*

Důkaz Postupujeme víceméně stejně jako v lemmatu 2.2.35. Tvrzení (a) je jasné: přidáme-li ke kvantifikátorům formule φ další jalové kvantifikátory, které vážou nové proměnné (tj. proměnné nevyskytující se ve φ), dostaneme formuli ekvivalentní s φ.

(b) Když φ je ekvivalentní s formulí tvaru $\exists v_1 \forall v_2 \exists \ldots v_n \theta$, pak $\neg\varphi$ je ekvivalentní s $\forall v_1 \exists v_2 \forall \ldots v_n \neg\theta$. Je-li $\theta \in \Delta_0$, pak i $\neg\theta \in \Delta_0$ a $\forall v_1 \exists v_2 \forall \ldots v_n \neg\theta$ je Π_n. Druhý případ je úplně stejný.

Tvrzení (c) a (d) lze dokázat najednou indukcí podle n. Množiny $\Sigma_0(\mathsf{PA})$ a $\Pi_0(\mathsf{PA})$ jsou očividně uzavřeny na konjunkci, disjunkci a omezenou kvantifikaci. Ze všech případů (tvrzení (d) a uzavřenost třídy $\Sigma_{n+1}(\mathsf{PA})$ a $\Pi_{n+1}(\mathsf{PA})$ na konjunkci, disjunkci a na čtyři tvary omezené kvantifikace) dokažme jen jeden nejdůležitější: množina $\Sigma_{n+1}(\mathsf{PA})$ je uzavřena na omezený kvantifikátor tvaru $\forall u{<}z$. Nechť φ je $\Sigma_{n+1}(\mathsf{PA})$. To znamená, že φ je ekvivalentní s formulí tvaru $\exists v \psi$, kde $\psi \in \Pi_n$. Tři formule $\forall u{<}z\, \varphi$, $\forall u{<}z\, \exists v \psi$, $\exists w \forall u{<}z\, \exists v{<}w\, \psi$ jsou spolu ekvivalentní: jedna implikace je lemma 4.3.3 a ostatní lze snadno ověřit. Protože předpokládáme, že množina $\Pi_n(\mathsf{PA})$ je uzavřena na omezenou kvantifikaci, platí $\forall u{<}z\, \exists v{<}w\, \psi \in \Pi_n(\mathsf{PA})$, a formule $\forall u{<}z\, \varphi$ je tedy PA-ekvivalentní se Σ_{n+1}-formulí. Ostatní úvahy jsou stejné jako v 2.2.35.

(e) Nechť φ je PA-ekvivalentní s ψ i s χ, kde $\psi \in \Sigma_n$ a $\chi \in \Pi_n$. Pak $\neg\varphi$ je ekvivalentní s $\neg\psi$ i s $\neg\chi$. Tvrzení (b) dává $\neg\psi \in \Pi_n(\mathsf{PA})$ a $\neg\chi \in \Sigma_n(\mathsf{PA})$. Tedy $\neg\varphi$ je ekvivalentní se Σ_n- i s Π_n-formulí, a je tedy $\Delta_n(\mathsf{PA})$. Uzavřenost množiny $\Delta_n(\mathsf{PA})$ na konjunkci, disjunkci a omezenou kvantifikaci plyne z (d). Implikaci lze vyjádřit pomocí negace a disjunkce.

(f) V (c) a (d) je řečeno, že množina $\Sigma_1(\mathsf{PA})$ je uzavřena na konjunkci, disjunkci, existenční kvantifikaci a libovolnou omezenou kvantifikaci, což jsou přesně ty operace, které se vyskytují v definici Σ-formule. QED

Lemma 4.3.5 *(a) Formule* $x \mid y$, $\mathsf{Prime}(x)$, $\mathsf{Pair}(z,t,w)$, $x \in w$, $\mathsf{RPrime}(x,y)$, $\mathsf{Set}(w)$, $\mathsf{B}(w,u,v)$, $\mathsf{Lh}(w,y)$, $\mathsf{Seq}(w)$, $\mathsf{Var}(x)$, $\mathsf{UnivClo}(z,y)$, $\mathsf{Beg}(w_1,w)$, $\mathsf{Ends}(w,z)$ *a* $[\mathsf{Q}](z)$ *jsou* Δ_0 *v* PA.

(b) Formule $\mathsf{Term}(x)$, $\mathsf{Numeral}(x,y)$, $\mathsf{FmAt}(z)$, $\mathsf{Fm}(z)$, $\mathsf{SubT}(v,x,t,y)$, $\mathsf{OccT}(v,t)$, $\mathsf{SubF}(v,z,t,y)$, $\mathsf{OccF}(v,z)$, $\mathsf{Sent}(z)$, $\mathsf{FreeSub}(v,z,t)$ *a* $\mathsf{LogAx}(z)$ *jsou* Δ_1 *v* PA.

(c) Když $\tau(z)$ *je* Δ_1 *v* PA, *pak formule* $\mathsf{Proof}_\tau(x,w)$ *je* Δ_1 *v* PA.

(d) Když $\tau(z)$ *je* Σ *v* PA, *pak* $\mathsf{Proof}_\tau(x,w)$ *a* $\mathsf{Pr}_\tau(x)$ *jsou* Σ_1 *v* PA *a* $\mathsf{Con}(\tau)$ *je* Π_1 *v* PA.

(e) Formule $\pi(z)$ *je* Δ_1 *v* PA. *Tedy* $\mathsf{Proof}_\mathsf{Q}(x,w)$ *a* $\mathsf{Proof}_\pi(x,w)$ *jsou* Δ_1 *v* PA, $\mathsf{Pr}_\mathsf{Q}(x)$ *a* $\mathsf{Pr}_\pi(x)$ *jsou* Σ_1 *v* PA *a* $\mathsf{Con}(\mathsf{Q})$ *a* $\mathsf{Con}(\pi)$ *jsou* Π_1 *v* PA.

Důkaz O formulích $x \mid y$, $\mathsf{Prime}(x)$ a $\mathsf{Pair}(z,t,w)$ jsme se již zmínili. Formule $[\mathsf{Q}](z)$ je otevřená. Podívejme se na formuli $\mathsf{RPrime}(x,y)$:

> Nechť $x \neq 0$ a nechť $x \mid y \cdot v$. Dělme v se zbytkem (viz 4.1.4) číslem x: $v = x \cdot u + v'$, $v' < x$. Z $x \mid y \cdot (x \cdot u + v')$ plyne $x \mid y \cdot v'$ dle 4.1.5(j).

Věříme, že tento argument čtenář snadno doplní na důkaz, že formule $\mathsf{RPrime}(x,y)$ je PA-ekvivalentní s formulí $\forall v{<}x(x \mid y\cdot v \;\to\; v=0)$, která je omezená v PA. Formule $x\in w$ začíná kvantifikátory $\exists z\exists t$. V PA můžeme říci, že splňují-li z a t podmínku $\mathsf{Pair}(z,t,w)$, lze dle 4.2.2(b) místo $\exists z\exists t(..)$ ekvivalentně psát $\exists z{\le}w\exists t{\le}w(..)$. V této situaci se říká, že kvantifikátory se nám podařilo „omezit do w“. Podobně lze uvažovat u všech zbývajících formulí v (a): všechny v nich se vyskytující kvantifikátory lze omezit do w (nebo, v případě formulí $\mathsf{Var}(v)$ a $\mathsf{UnivClo}(z,y)$, do v či do y).

Podívejme se nyní podrobně na formuli $\mathsf{Term}(x)$. Vraťme se k lemmatu 4.2.10(c). V jeho důkazu jsme formuli $\mathsf{Term}(x)$ zapsali ve tvaru $\exists w(\alpha(x,w)\ \&\ \mathsf{B}(w,x,\overline{1}))$. Formuli $\alpha(x,w)$ jsme četli posloupnost w je počátečním úsekem charakteristické funkce množiny všech aritmetických termů, jejíž délka je $x+\overline{1}$, nebo stručněji posloupnost w je dosvědčující posloupností délky $x+\overline{1}$. Stejnou úvahou jako v předchozím odstavci lze zdůvodnit, že $\alpha(x,w)$ je Δ_0 v PA: všechny její kvantifikátory lze omezit do w. Tím je zdůvodněno, že formule $\mathsf{Term}(x)$ je Σ_1 v PA. Podmínky (1) a (2) v důkazu tvrzení 4.2.10(c) a tvrzení 4.2.6(a) dávají $\mathsf{PA}\vdash\forall x\exists!w\alpha(x,w)$. Z toho plyne, že formule

$$\exists w(\alpha(x,w)\ \&\ \mathsf{B}(w,x,\overline{1}))\quad\text{a}\quad\forall w(\alpha(x,w)\to\mathsf{B}(w,x,\overline{1}))$$

jsou v PA ekvivalentní. Druhá z nich je Π_1 v PA. Tím je dokončen důkaz, že formule $\mathsf{Term}(x)$ je Δ_1 v PA.

Podobně lze postupovat v případě formulí Fm, SubT, SubF, OccT, OccF a FreeSub. Každou z nich lze ekvivalentně psát ve tvaru

$$\exists w(\beta(v,z,t,y,w)\ \&\ \mathsf{B}(w,z,\overline{1}))\quad\text{i}\quad\forall w(\beta(v,z,t,y,w)\to\mathsf{B}(w,z,\overline{1}))\qquad(*)$$

(s tím, že některé z proměnných y, v, t mohou chybět a z se v případě formule SubT jmenuje x). Jediný rozdíl je v tom, že formule β může obsahovat již sestrojené formule (například formuli Term), a lze o ní tedy tvrdit pouze, že je Δ_1 v PA, nikoliv, že je Δ_0 v PA. I kdyby ale byla jen Σ_1 v PA, z dvojího tvaru $(*)$ plyne, že každá z formulí Fm, SubT atd. je Δ_1 v PA.

Formule $\mathsf{FmAt}(z)$ a $\mathsf{Numeral}(x,y)$ jsou ekvivalentní s formulemi

$$\begin{aligned}&\exists x_1{<}z\,\exists x_2{<}z\,(\mathsf{Term}(x_1)\ \&\ \mathsf{Term}(x_2)\ \&\ (z=\ulcorner x_1{=}x_2\urcorner\ \vee\\ &\qquad\qquad\vee\ z=\ulcorner x_1{<}x_2\urcorner\ \vee\ z=\ulcorner x_1{\le}x_2\urcorner)),\\ &\mathsf{Term}(y)\ \&\ (\text{délka } y \text{ je } \overline{3}\cdot x+\overline{1})\ \&\ (y\ \text{neobsahuje symboly + a }\cdot).\end{aligned}$$

Obě formule jsou $\Delta_1(\mathsf{PA})$ podle 4.3.4(e). Stejně lze postupovat i v případě formulí $\mathsf{Sent}(z)$, $\mathsf{LogAx}(z)$ a $\pi(z)$. Je-li $\tau(z)\in\Delta_1(\mathsf{PA})$, pak také formule $\mathsf{Proof}_\tau(x,w)$ je sestavena z Δ_1-formulí jen pomocí logických spojek a omezených kvantifikátorů (přesněji kvantifikátorů, které lze omezit do w), a je tedy Δ_1 v PA.

Je-li τ jen Σ v PA, pak dle 4.3.4(f) je τ zároveň Σ_1 v PA. Pak dále Proof_τ je Σ_1 v PA podle 4.3.4(c) a Pr_τ je Σ_1 v PA podle 4.3.4(d). V tom případě ano, sentence $\mathsf{Con}(\tau)$ je utvořena z formule $\mathsf{Pr}_\tau(x)$ dosazením numerálu $\overline{0=\mathrm{S}(0)}$ a negací, a podle tvrzení 4.3.4(b) je to tedy $\Pi_1(\mathsf{PA})$-formule. QED

Umíme tedy klasifikovat aritmetické formule podle jejich (aritmetické) složitosti, známe nejzákladnější vlastnosti této klasifikace a přesvědčili jsme se, že všechny formule užité v minulém oddílu při aritmetizaci logické syntaxe mohou sice být dlouhé, mají ale dost nízkou pozici v aritmetické hierarchii formulí. Vraťme se nyní k otázce, jaké množiny jsou definovatelné ve struktuře $\mathbf{N}$ a jak složité jsou formule, které je definují. Připomeňme, že aritmetická formule $\varphi(x_1, .., x_k)$ definuje množinu $A \subseteq \mathrm{N}^k$, jestliže

$$A = \{\, [n_1, .., n_k] \,;\, \mathbf{N} \models \varphi(\underline{x})[n_1, .., n_k] \,\}.$$

Přitom podmínka $\mathbf{N} \models \varphi(\underline{x})[n_1, .., n_k]$, jež říká, že φ je splněna ohodnocením proměnných, které proměnným $x_1, .., x_k$ přiřazuje hodnoty $n_1, .., n_k$, je ekvivalentní s podmínkou $\mathbf{N} \models \varphi(\overline{n}_1, .., \overline{n}_k)$, protože číslo n_i je v $\mathbf{N}$ hodnotou termu $\overline{n_i}$.

Nechť Γ je množina formulí. Řekneme, že množina $A \subseteq \mathrm{N}^k$ je Γ-*definovatelná* v nějaké struktuře $\mathbf{D}$, jestliže ji v $\mathbf{D}$ definuje některá formule z množiny Γ.

Věta 4.3.6 *(a) Když A je Δ_0-definovatelná v $\mathbf{N}$, pak A je primitivně rekurzívní. (b) Když A je Σ-definovatelná v $\mathbf{N}$, pak A je rekurzívně spočetná.*

Důkaz Nechť formule φ je například tvaru $\mathrm{S}(\mathrm{S}(\mathrm{S}(x \cdot x))) \leq x + y$. Pak φ definuje v $\mathbf{N}$ relaci $\{\, [n, m] \,;\, n^2 + 3 \leq n + m \,\}$, která je PR. Toto je pravda o každé atomické formuli. Každá totiž definuje v $\mathbf{N}$ množinu tvaru $\{\, [n_1, .., n_k] \,;\, f(\underline{n})\ R\ g(\underline{n}) \,\}$, kde R je rovnost, ostré uspořádání nebo neostré uspořádání a f a g jsou primitivně rekurzívní funkce, protože jsou odvozeny ze sčítání, násobení a přičítání jedničky pomocí operace substituce (skládání funkcí). Dále postupujeme indukcí podle počtu kroků, kterými je φ utvořena z atomických formulí. Předpokládejme, že φ je utvořena z jednodušší formule pomocí omezené kvantifikace. Nechť například $\varphi(z, x_1, .., x_r)$ je tvaru $\forall v \leq z\, \psi(v, z, \underline{x})$. Pak definuje-li ψ v $\mathbf{N}$ relaci $B \subseteq \mathrm{N}^{r+2}$, formule φ definuje relaci $\{\, [m, \underline{n}] \,;\, \forall k \leq m\, B(k, m, \underline{n}) \,\}$. Ta je primitivně rekurzívní, pokud B je primitivně rekurzívní, protože třída PR je uzavřena na (metamatematickou) omezenou kvantifikaci. Ostatní případy jsou také jasné, třída PR je uzavřena i na booleovské operace.

V (b) postupujme indukcí podle počtu kroků, kterými je φ utvořena z Δ_0-formulí. Je-li tento počet nulový, pak formule φ definuje RS množinu vzhledem k (a) a inkluzi $\mathsf{PR} \subseteq \mathsf{RS}$. Jinak je φ utvořena z nějaké Σ-formule ψ pomocí existenční nebo omezené kvantifikace, nebo je utvořena ze dvou Σ-formulí ψ_1 a ψ_2 pomocí konjunkce nebo disjunkce. Pokud ψ či ψ_1 a ψ_2 definují rekurzívně spočetné podmínky B resp. B_1 a B_2, pak φ definuje podmínku, která je z B resp. z B_1 a B_2 utvořena pomocí existenční kvantifikace (tj. projekce), omezené kvantifikace, průniku nebo sjednocení, což jsou operace, na které je třída RS uzavřena. QED

Zajímavá otázka — možná zajímavější, než by čtenář na první čtení řekl — zní, zda tvrzení předchozí věty lze obrátit. Existují totiž celkem jednoduše definované množiny, o kterých lze snadno dokázat, že jsou primitivně rekurzívní, ale dosud se

nepodařilo zjistit, zda jsou Δ_0-definovatelné v $\mathbf{N}$. Příkladem takové množiny je

$$\{\, [n,m]\,;\ \text{prvočísel menších než } n \text{ je } m\,\}.$$

Nicméně sama otázka, zda tvrzení (a) lze obrátit, není otevřeným problémem. Lze dokázat, že odpověď je ne, existují PR množiny, které v $\mathbf{N}$ nejsou Δ_0-definovatelné. Naším bezprostředním cílem je dokázat, že v případě (b) platí ano, toto tvrzení lze obrátit: každou RS množinu definuje v $\mathbf{N}$ nějaká Σ-formule. Důkaz rozdělíme do několika kroků, z nichž hned první je podstatný.

Lemma 4.3.7 *Graf každé primitivně rekurzívní funkce je Σ-definovatelný v $\mathbf{N}$.*

Důkaz Nechť je dána primitivně rekurzívní funkce f, která má r proměnných. Tvrdíme, že k f existuje Σ-formule $\varphi(x_1,..,x_r,y)$, která definuje graf funkce f, tj. splňuje podmínku

$$f(n_1,..,n_r)=m \;\Leftrightarrow\; \mathbf{N}\models\varphi(\overline{n_1},..,\overline{n_r},\overline{m})$$

pro libovolnou $(r+1)$-tici $[n_1,..,n_r,m]$. Postupujme indukcí podle počtu kroků v primitivně rekurzívním odvození funkce f. Je-li f jedna z funkcí s nebo z, volme za $\varphi(x,y)$ formuli $\mathrm{S}(x)=y$ resp. $0=y$. Je-li f projekce i^r_j, volme za $\varphi(x_1,..,x_r,y)$ formuli $x_j=y$. Nechť f je odvozena z g a h primitivní rekurzí. Tedy pro všechna $n_1,..,n_r$ a k jsou splněny podmínky

$$f(0,n_1,..,n_r)=g(\underline{n}), \tag{1}$$
$$f(k+1,n_1,..,n_r)=h(f(k,\underline{n}),k,\underline{n}). \tag{2}$$

Podle indukčního předpokladu k funkcím g a h existují Σ-formule $\psi(x_1,..,x_r,y)$ a $\chi(z,v,x_1,..,x_r,y)$, které v $\mathbf{N}$ definují jejich grafy:

$$g(n_1,..,n_r)=m \;\Leftrightarrow\; \mathbf{N}\models\psi(\underline{n},\overline{m}), \tag{3}$$
$$h(j,k,n_1,..,n_r)=m \;\Leftrightarrow\; \mathbf{N}\models\chi(\overline{j},\overline{k},\underline{n},\overline{m}). \tag{4}$$

Zvolme za $\varphi(v,x_1,..,x_r,y)$ formuli

$$\begin{aligned}\exists w(&\mathsf{Seq}(w)\ \&\ \mathsf{Lh}(w,v+\overline{1})\ \&\ \mathsf{B}(w,v,y)\ \&\\ &\&\ \exists t{<}w\,(\mathsf{B}(w,0,t)\ \&\ \psi(\underline{x},t))\ \&\\ &\&\ \forall u{<}v\,\exists z{<}w\,\exists t{<}w\,(\mathsf{B}(w,u,z)\ \&\ \mathsf{B}(w,u+\overline{1},t)\ \&\ \chi(z,u,\underline{x},t))).\end{aligned}$$

Z hlediska syntaktického je vše v pořádku: φ je sestavena ze Σ-formulí (a Δ_0-formulí) ψ, χ, Seq, Lh a B pomocí konjunkce, existenční kvantifikace a omezené kvantifikace. Ověření, že φ definuje graf funkce f, je celkem přímočaré a asi by mohlo být přenecháno čtenáři. Podstatnou část ale provedeme, a to hlavně proto, aby bylo zřejmé, co z výsledků předchozího oddílu je k důkazu potřeba.

Máme ověřit, že pro každou volbu čísel $m,k,n_1,..,n_r$ platí

$$f(k,n_1,..,n_r)=m \;\Leftrightarrow\; \mathbf{N}\models\varphi(\overline{k},\underline{n},\overline{m}). \tag{5}$$

Formule φ má tvar $\exists w \alpha(v, \underline{x}, y, w)$. Předpokládejme, že $\mathbf{N} \models \varphi(\overline{k}, \underline{\overline{n}}, \overline{m})$, tj. že $\mathbf{N} \models \exists w \alpha(\overline{k}, \underline{\overline{n}}, \overline{m}, w)$. Tedy $\mathbf{N} \models \alpha(\overline{k}, \underline{\overline{n}}, \overline{m}, \overline{q})$ pro jisté číslo $q \in \mathrm{N}$. Čísla m, k, $\underline{n}$ a q tedy splňují podmínky

$$\mathbf{N} \models \mathsf{Seq}(\overline{q}) \ \&\ \mathsf{Lh}(\overline{q}, \overline{k+1}) \ \&\ \mathsf{B}(\overline{q}, \overline{k}, \overline{m}), \tag{6}$$

$$\mathbf{N} \models \exists t{<}\overline{q}\,(\mathsf{B}(\overline{q}, 0, t) \ \&\ \psi(\underline{\overline{n}}, t)), \tag{7}$$

$$\mathbf{N} \models \forall u{<}\overline{k}\,\exists z{<}\overline{q}\,\exists t{<}\overline{q}\,(\mathsf{B}(\overline{q}, u, z) \ \&\ \mathsf{B}(\overline{q}, u+\overline{1}, t) \ \&\ \chi(z, u, \underline{\overline{n}}, t)). \tag{8}$$

Z podmínky (6) díky lemmatu 4.2.7 plyne, že číslo q je (ve smyslu kódování z oddílu 4.2) kódem posloupnosti délky $k+1$, jejímž k-tým členem je m. Označme $m_0, \ldots, m_k$ všechny členy posloupnosti q. Podmínku (7) lze přepsat na disjunkci $\mathbf{N} \models \bigvee_j (\mathsf{B}(\overline{q}, 0, \overline{j}) \ \&\ \psi(\underline{\overline{n}}, \overline{j}))$. Přitom sentence $\mathsf{B}(\overline{q}, 0, \overline{j})$ v $\mathbf{N}$ platí pro jediné j, a sice pro $j = m_0$. Protože ψ definuje graf funkce g (viz (3)), sentence $\psi(\underline{\overline{n}}, \overline{j})$ platí v $\mathbf{N}$ rovněž pouze pro jediné j, a sice pro $j = g(\underline{n})$. Tedy $m_0 = g(\underline{n})$. Podobně lze z podmínky (8) a s užitím (4) usoudit, že pro každé $i < k$ platí $m_{i+1} = h(m_i, i, \underline{n})$. To vše dohromady a spolu s (1) a (2) znamená, že pro každé $i \leq k$ platí $m_i = f(i, \underline{n})$. Pro $i = k$ to spolu s $m_k = m$ dává $m = f(k, \underline{n})$. Tím jsme ověřili implikaci $\Leftarrow$ v (5). Ověření implikace $\Rightarrow$ je podobné, lemma 4.2.7 se použije opačným směrem. Všimněme si také, že podobné úvahy jsme již prováděli v důkazech tvrzení 4.2.10(b) a 4.2.11(a).

Poslední případ je ten, kdy f je odvozena z funkcí $h, g_1, \ldots, g_k$ substitucí:

$$f(n_1, \ldots, n_r) = h(g_1(\underline{n}), \ldots, g_k(\underline{n})).$$

Podle indukčního předpokladu existují Σ-formule $\chi(x_1, \ldots, x_k, y)$ a $\psi_1(x_1, \ldots, x_r, y)$ až $\psi_k(x_1, \ldots, x_r, y)$, které definují grafy funkcí h a $g_1, \ldots, g_k$ v $\mathbf{N}$. Vezměme za $\varphi(x_1, \ldots, x_r, y)$ formuli

$$\exists v_1 \ldots \exists v_k (\chi(v_1, \ldots, v_k, y) \ \&\ \psi_1(\underline{x}, v_1) \ \&\ \ldots \ \&\ \psi_k(\underline{x}, v_k)).$$

Je jasné, že φ je Σ-formule. Ověření, že φ definuje graf funkce f, přenecháváme čtenáři. QED

Lemma 4.3.8 *Každá primitivně rekurzívní množina je Σ-definovatelná v $\mathbf{N}$.*

Důkaz Nechť $A \subseteq \mathrm{N}^k$ je *PR*. Podle předchozího lemmatu k charakteristické funkci c_A množiny A existuje Σ-formule $\varphi(x_1, \ldots, x_k, y)$, která v $\mathbf{N}$ definuje její graf:

$$\forall m \forall n_1 \ldots \forall n_k (c_A(n_1, \ldots, n_k) = m \Leftrightarrow \mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_k}, \overline{m})).$$

Dosazení $m := 1$ dává

$$\forall n_1 \ldots \forall n_k (c_A(n_1, \ldots, n_k) = 1 \Leftrightarrow \mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_k}, \overline{1})).$$

Tato ekvivalence znamená, že formule $\varphi(x_1, \ldots, x_k, \overline{1})$ definuje množinu A: platí totiž $c_A(n_1, \ldots, n_k) = 1$, právě když $[n_1, \ldots, n_k] \in A$. Formule $\varphi(x_1, \ldots, x_k, \overline{1})$ samozřejmě je Σ-formulí. QED

Věta 4.3.9 *Nechť $n \geq 1$. Pak*

(a) Množina $A \subseteq \mathrm{N}^k$ je Σ_n-množina (ve smyslu kapitoly 2), právě když A je Σ_n-definovatelná v $\mathbf{N}$.

(b) Množina $A \subseteq \mathrm{N}^k$ je Π_n-množina, právě když A je Π_n-definovatelná v $\mathbf{N}$.

(c) Množina $A \subseteq \mathrm{N}^k$ je v některé třídě Σ_n nebo Π_n, právě když je v $\mathbf{N}$ definovatelná (libovolnou formulí).

Důkaz Nejprve dokažme, že (a) platí pro $n = 1$. Nechť $A \subseteq \mathrm{N}^k$ a nechť A je Σ_1, tedy rekurzívně spočetná. Podle věty o projekci 2.2.25 existuje PR relace $B \subseteq \mathrm{N}^{k+1}$ taková, že $A = \{\, [n_1, \ldots, n_k] \,;\, \exists m B(n_1, \ldots, n_k, m) \,\}$. K množině B podle lemmatu 4.3.8 existuje Σ_1-formule $\psi(x_1, \ldots, x_k, z)$, která ji definuje v $\mathbf{N}$. Pak ale formule $\exists z \psi(x_1, \ldots, x_k, z)$ je Σ-formule, která definuje množinu A v $\mathbf{N}$. Podle 4.3.4(f) formule $\exists z \psi(x_1, \ldots, x_k, z)$ je PA-ekvivalentní s jistou Σ_1-formulí $\varphi(x_1, \ldots, x_k)$. Je jasné, že PA-ekvivalentní formule definují v $\mathbf{N}$ tutéž množinu. Množina A je tedy Σ_1-definovatelná v $\mathbf{N}$.

Naopak, je-li A množina Σ_1-definovatelná v $\mathbf{N}$, pak A je rekurzívně spočetná podle věty 4.3.6.

Předpokládejme, že Σ_n-množiny jsou právě ty, které jsou definovatelné Σ_n-formulemi. Pak jejich komplementy, Π_n-množiny, jsou právě ty, které jsou definovatelné negacemi Σ_n-formulí. Ale negace Σ_n-formulí jsou PA-ekvivalentní s Π_n-formulemi, a tedy v $\mathbf{N}$ definují tytéž množiny jako Π_n-formule. Tím je zdůvodněno, že tvrzení (b) pro n plyne z tvrzení (a) pro totéž n.

Téměř stejně plyne tvrzení (a) pro $n+1$ z tvrzení (b) pro n, jen místo komplementu a negaci se mluví o projekci a existenční kvantifikaci.

Tvrzení (c) plyne z (a) a (b), dodat zbývá snad jen to, že dle (a)–(d) lemmatu 4.3.4 je každá aritmetická formule ekvivalentní s některou Σ_n-formulí a také s některou Π_n-formulí. QED

Označíme-li $\Gamma^{\mathbf{N}}$ množinu všech množin a relací definovatelných v $\mathbf{N}$ formulemi z množiny formulí Γ, pak tvrzení (a) a (b) věty 4.3.9 můžeme přehledně zapsat takto: $\Sigma_n^{\mathbf{N}} = \Sigma_n$, $\Pi_n^{\mathbf{N}} = \Pi_n$. Platí také $\Delta_0^{\mathbf{N}} \subseteq PR \subseteq \Sigma^{\mathbf{N}} = \Sigma_1^{\mathbf{N}} = RS$. Věta 4.3.9 má značný význam jak pro teoretickou informatiku, tak pro logiku. Význam pro informatiku je v tom, že pojem rekurzívně spočetné množiny, a tím vlastně i pojem algoritmu, má vzhledem k tvrzení (a) pro $n = 1$ také čistě logickou, „bezestrojovou“ definici. To lze chápat jako argument pro názor, že pojem algoritmu je jedním z absolutních pojmů, čili jako argument pro přijetí nebo přijatelnost Churchovy teze. Důsledky věty 4.3.9 pro logiku se budeme zabývat za chvíli.

Máme-li obecnou větu o definovatelnosti rekurzívně spočetných množin, neznamená to náhodou, že v oddílu 4.2 jsme se zbytečně dlouho zabývali jednotlivými rekurzívně spočetnými (většinou primitivně rekurzívními) množinami a formulemi, které ony množiny popisují? Snad ne. Na konci oddílu 4.2 jsme dosažené výsledky rozdělili na tvrzení o platnosti numerických instancí a na tvrzení o dokazatelnosti

obecných faktů v PA. Z výsledků o platnosti numerických instancí (tj. o definovatelnosti) jsme k důkazu věty 4.3.9 potřebovali lemma 4.2.7, a tedy i řadu tvrzení nutných k důkazu lemmatu 4.2.7 počínaje už tvrzením 4.1.5. Než jsme tedy mohli dokázat obecné tvrzení, museli jsme dokázat přímo definovatelnost řady konkrétních množin. Ostatní fakty o platnosti numerických instancí následující za lemmatem 4.2.7 jsou do oddílu 4.2 zařazeny hlavně proto, abychom mohli dospět k větě 4.2.13.

U tvrzení o dokazatelnosti obecných faktů v PA považujeme za užitečné zdůraznit, že nijak neplynou z příslušných tvrzení o definovatelnosti. Co přesně máme na mysli, ukažme na tvrzení *množina všech prvočísel je nekonečná* vyjádřeném sentencí $\theta := \forall x \exists y(x < y \ \& \ \mathsf{Prime}(y))$. Víme-li, že formule $\mathsf{Prime}(y)$ definuje v $\mathbf{N}$ množinu všech prvočísel, můžeme usoudit, že θ platí v $\mathbf{N}$, a platí tedy i v každém (nestandardním) modelu teorie $\mathrm{Th}(\mathbf{N})$. Je-li PA úplná, znamená to, že θ platí i v každém modelu teorie PA. Už brzy ale uvidíme, že PA úplná není! Dokazatelnost sentence θ v PA znamená, že θ platí v každém modelu $\mathbf{M}$ teorie PA bez ohledu na to, zda $\mathbf{M}$ je zároveň modelem teorie $\mathrm{Th}(\mathbf{N})$. Stejně jako na sentenci θ je třeba se dívat i na ostatní fakty o dokazatelnosti v PA, zejména na tvrzení z věty 4.2.14. V každém modelu PA (tj. i v nestandardních a bez ohledu na mohutnost nosné množiny) platí základní fakty o dokazatelnosti. V každém modelu teorie PA platí například sentence $\forall x \exists y(x < y \ \& \ \pi(y))$, protože v PA víme, že PA je teorií s nekonečnou množinou axiomů.

Všimněme si ještě, že z věty 4.3.9 plyne, že množina přirozených čísel je rekurzívní, právě když je v $\mathbf{N}$ současně Σ_1- i Π_1-definovatelná. A dále si všimněme, že ve větě 4.3.9 se nic netvrdí o případu $n = 0$, ani se tam nic netvrdí na téma, jaké množiny definují v $\mathbf{N}$ formule, které jsou $\Delta_n(\mathsf{PA})$. Je-li totiž nějaká množina současně Σ_1- i Π_1-definovatelná, nemusí to ještě znamenat, že je definovatelná nějakou $\Delta_1(\mathsf{PA})$-formulí, neboť dvě formule definující tutéž množinu ještě nemusí být PA-ekvivalentní.

Řekneme, že množina $A \subseteq \mathrm{N}^k$ je *aritmetická*, je-li v $\mathbf{N}$ definovatelná (libovolnou formulí). Věta 4.3.9(c) říká, že množina A je aritmetická, právě když A je v některé z tříd Σ_n či Π_n definovaných v kapitole 2. Tvrdit o nějaké množině, že není aritmetická, tedy znamená tvrdit o ní mnohem víc, než že není rekurzívní nebo že není rekurzívně spočetná.

Věta 4.3.10 *Množina* $\mathrm{Th}(\mathbf{N})$ *není aritmetická.*

Důkaz Předpokládejme, že $\mathrm{Th}(\mathbf{N})$ (tj. množina všech číselných kódů všech aritmetických sentencí, které platí v $\mathbf{N}$) je v některé z tříd Σ_n nebo Π_n. Nechť $\mathrm{Th}(\mathbf{N}) \in \Sigma_n$ a $n \geq 1$. Zvolme aritmetickou množinu A takovou, že $A \notin \Sigma_n$. Taková množina existuje podle tvrzení 2.2.39(c). Protože A je aritmetická, existuje aritmetická formule $\varphi(x)$, která množinu A definuje v $\mathbf{N}$. Platí tedy

$$\forall n(n \in A \Leftrightarrow \mathbf{N} \models \varphi(\overline{n})). \tag{1}$$

Označme f funkci $n \mapsto \varphi(\overline{n})$, která z libovolného přirozeného čísla n vytvoří term $\overline{n}$ a dosadí jej za x do φ. Funkce f zobrazuje množinu všech přirozených čísel do mno-

žiny všech aritmetických sentencí. Protože formule ztotožňujeme s jejich číselnými kódy, f je funkce z N do N. Několika způsoby lze zdůvodnit, že f je (primitivně) rekurzívní funkce. Užitím funkce f můžeme podmínku (1) přepsat na

$$\forall n(n \in A \Leftrightarrow f(n) \in \mathrm{Th}(\mathbf{N})). \tag{2}$$

Platí tedy $A \leq_{\mathrm{m}} \mathrm{Th}(\mathbf{N})$ via f. To je spor s 2.2.35(g) a s předpokladem, že množina A není Σ_n.

Stručná rekapitulace důkazu zní takto: fakt, že každá Σ_n- i Π_n-množina je definovatelná v $\mathbf{N}$, znamená, že každá aritmetická množina je m-převeditelná na $\mathrm{Th}(\mathbf{N})$. Kdyby platilo $\mathrm{Th}(\mathbf{N}) \in \Sigma_n$, znamenalo by to kolaps aritmetické hierarchie. QED

Věta 4.3.11 *Nechť T je rekurzívně axiomatizovatelná teorie s aritmetickým jazykem a nechť $\mathbf{N} \models T$. Pak T je neúplná.*

Důkaz Množina $\mathrm{Thm}(T)$ všech sentencí dokazatelných v T je přinejhorším rekurzívně spočetná (viz 3.6.6), tedy určitě aritmetická. Nemůže se tedy rovnat množině $\mathrm{Th}(\mathbf{N})$, která aritmetická není. QED

Peanova aritmetika je rekurzívně axiomatizovatelná a platí $\mathbf{N} \models \mathsf{PA}$. Peanova aritmetika je tedy neúplná. Věta 4.3.11 ale tvrdí víc: Peanovu aritmetiku nelze zúplnit přidáním jednotlivých axiomů nebo schémat platných v $\mathbf{N}$. Každým takovým přidáním vznikne rekurzívně axiomatizovatelná, tedy neúplná teorie. Větu 4.3.11 lze označit za jednu z variant První Gödelovy věty o neúplnosti. V dalších oddílech dospějeme k dalším variantám a také zdůvodníme, že podobná tvrzení platí i pro teorii množin a jiné teorie s dostatečně bohatým jazykem.

Na neúplnou teorii T jsme se dosud dívali nejspíš jako na polotovar, tj. jako na úkol najít další vhodné axiomy, po jejichž přidání lze teorii T (možná) brát vážně. První Gödelova věta nás nutí změnit pohled na neúplnost. Volíme-li teorii T, kterou lze přijmout jako prostředí pro matematickou práci (svět matematiky), jsou přirozené požadavky takové, aby T měla přehlednou množinu axiomů a aby měla dostatečně bohatý jazyk. V tom případě je *nutné* hledat mezi neúplnými teoriemi.

Podíváme-li se znovu na otázky, které jsme položili v závěru oddílu 4.1, lze říci, že věta 4.3.11 je zajímavou, možná překvapivou, ale pouze *částečnou* odpovědí na první otázku. Peanova aritmetika není úplná a nelze ji zúplnit přidáním rekurzívní množiny axiomů platných v $\mathbf{N}$. Nevíme ale dosud, zda Peanovu aritmetiku nelze zúplnit přidáním rekurzívní množiny *nějakých* axiomů. Také odpovědi na zbývající otázky musíme ještě odložit.

Víme, že Peanova aritmetika je neúplná, nemáme ale po ruce žádný příklad sentence nezávislé na PA. Tato situace by mohla svádět k prohlášení, že věta 4.3.11 je nekonstruktivní: tvrdí, že existuje jakýsi objekt, ale nepodává žádný návod k jeho sestrojení. S takto kategorickou formulací ale nelze bezvýhradně souhlasit. Podrobnější analýzou důkazu věty 4.3.11 by totiž bylo možné si nezávislou sentenci opatřit. Opatrnější formulaci otázky po sentenci nezávislé na PA ale pokládáme za oprávněnou:

- *Lze nezávislost na* PA *dokázat pro nějakou sentenci, která je zajímavá z matematického hlediska?*

To je řečeno trochu vágně, ale je asi jasné, co máme na mysli: ona sentence, kterou bychom získali analýzou důkazu věty 4.3.11, by pravděpodobně byla dlouhá a nenázorná. Kdežto sentence je matematicky zajímavá, pokud například vyjadřuje tvrzení, kterým se již předtím někdo zabýval a pokoušel se je dokazovat nebo vyvracet. Jiná, ale také oprávněná otázka zní:

- *Pro které nejmenší n existuje Σ_n-sentence nezávislá na* PA*?*

Nejmenší n takové, že v Σ_n existuje nezávislá sentence, je ovšem zároveň nejmenším n takovým, že v Π_n existuje nezávislá sentence, protože negace nezávislé Σ_n-sentence je nezávislou Π_n-sentencí a naopak. Následující věta dává částečnou odpověď na předchozí otázku. V příštím oddílu zjistíme, že vlastně jde o úplnou odpověď, neboť níže už jít nelze, Δ_0-sentence nezávislé na Peanově aritmetice neexistují.

Věta 4.3.12 *Nechť T je rekurzívně axiomatizovatelná teorie s aritmetickým jazykem a nechť $\mathbf{N} \models T$. Pak existují Σ_1- a Π_1-sentence nezávislé na T.*

Důkaz Postupujme podobně jako v důkazu věty 4.3.11. Fakt, že každá Π_1-množina A je Π_1-definovatelná, znamená, že $A \leq_{\mathrm{m}} \Pi_1 \cap \mathrm{Th}(\mathbf{N})$ pro každou $A \in \Pi_1$. Platí tedy $\Pi_1 \cap \mathrm{Th}(\mathbf{N}) \notin \Sigma_1$. Z předpokladu o rekurzívní axiomatizovatelnosti teorie T plyne $\Pi_1 \cap \mathrm{Thm}(T) \in \Sigma_1$. Tedy $\Pi_1 \cap \mathrm{Thm}(T) \neq \Pi_1 \cap \mathrm{Th}(\mathbf{N})$. Protože ale $\mathbf{N}$ je model teorie T, platí alespoň inkluze $\subseteq$. Můžeme tedy vzít Π_1-sentenci θ takovou, že $\theta \in \mathrm{Th}(\mathbf{N}) - \mathrm{Thm}(T)$. Sentence θ je Π_1-sentence nezávislá na T a její negace $\neg\theta$ je T-ekvivalentní se Σ_1-sentencí nezávislou na T. QED

Cvičení

1. Představte si modifikaci definice omezené formule, ve které se připouštějí i kvantifikátory tvaru $\forall v{<}t(\underline{x})$, $\forall v{\leq}t(\underline{x})$, $\exists v{<}t(\underline{x})$, $\exists v{\leq}t(\underline{x})$, v nichž jako mez může vystupovat libovolný aritmetický term $t(x_1, \ldots, x_k)$ s podmínkou, že neobsahuje kvantifikovanou proměnnou (tj. v). Dokažte, že každá formule omezená v tomto smyslu je ekvivalentní s nějakou omezenou formulí ve smyslu definice 4.3.1.

   Návod. Například formule tvaru $\exists v{\leq}t(\underline{x}) \cdot s(\underline{x})\varphi$ je ekvivalentní s formulí $(t(\underline{x}) = 0 \ \&\ \varphi_v(0)) \ \vee\ \exists v_1{\leq}s(\underline{x})\exists v_2{<}t(\underline{x})\,\varphi_v(t(\underline{x}) \cdot v_1 + v_2)$, pokud proměnné v_1 a v_2 zvolíme tak, aby se nevyskytovaly v termech t a s a ani se nevyskytovaly volně ve φ.

2. Nechť T je teorie. Nechť $\varphi(x) \in \Delta_n(T)$, kde $n \geq 1$, a nechť $\psi(x, y)$ je $\Sigma_n(T)$-formule taková, že $T \vdash \forall x \exists! y \psi(x, y)$. Dokažte, že formule $\exists y(\psi(x, y) \ \&\ \varphi(y))$ je Δ_n v T. Dokažte, že také formule ψ je Δ_n v T.

   Návod. Pište formuli ψ ve tvaru $\exists v \theta(x, y, v)$, kde $\theta \in \Pi_{n-1}(T)$, a zdůvodněte, že ψ je ekvivalentní s formulí $\forall v \forall y'(\theta(x, y', v) \ \rightarrow\ y = y')$.

E

3. Věta 4.3.12 říká, že existuje Δ_0-formule $\delta(v)$ taková, že sentence $\forall v\delta(v)$ platí v $\mathbf{N}$, ale není dokazatelná v PA. Zdůvodněte, že žádné dvě ze tří formulí

$$\mathsf{Prime}(x), \qquad \mathsf{Prime}(x)\ \&\ \forall v{\leq}x\,\neg\delta(v), \qquad \mathsf{Prime}(x)\ \vee\ \exists v{\leq}x\,\delta(v)$$

nejsou PA-ekvivalentní, všechny tři ale definují v $\mathbf{N}$ tutéž množinu.

4. Teorie $\mathrm{I}\Delta_0$ má (stejně jako všechny ostatní teorie definované ve zbývajících cvičeních tohoto oddílu) aritmetický jazyk, axiomy Q1–Q9 a $\forall x(x < S(x))$ a dále všechny sentence tvaru $\mathrm{Ind}(\varphi)$, kde $\varphi \in \Delta_0$. Axiomatika teorie $\mathrm{I}\Delta_0$ je tedy podobná axiomatice Peanovy aritmetiky; hlavní rozdíl je, že schéma indukce je nahrazeno *schématem omezené indukce*. Dokažte, že všechny sentence z věty 4.1.1 jsou dokazatelné v $\mathrm{I}\Delta_0$.

   Návod. Při důkazu poslední sentence v (a) užijte omezenou indukci na formuli $\exists u{\leq}y\,(u + x = y)\ \vee\ \exists u{\leq}x\,(u + y = x)$. Ostatní důkazy projdou beze změny.

   Poznamenejme, že teorie $\mathrm{I}\Delta_0$ je nebo v nedávné době byla předmětem intenzívního výzkumu. Je například otevřeným problémem, zda v $\mathrm{I}\Delta_0$ lze dokázat, že existuje nekonečně mnoho prvočísel. Není také známo, zda $\mathrm{I}\Delta_0$ je konečně axiomatizovatelná.

5. Nechť $\mathrm{B}(\varphi)$ označuje instanci schématu kolekce utvořenou z formule φ, viz lemma 4.3.3. Teorie $\mathrm{B}\Gamma$, kde Γ je Σ_n nebo Π_n, má aritmetický jazyk a jejími axiomy jsou všechny axiomy teorie $\mathrm{I}\Delta_0$ a navíc všechny sentence $\mathrm{B}(\varphi)$, kde $\varphi \in \Gamma$. Teorie $\mathrm{B}\Gamma$ má tedy kromě axiomů Q1–Q9 dvě axiomatická schémata, schéma indukce pro omezené formule a schéma kolekce pro Γ-formule. Analyzujte důkaz lemmatu 4.3.4 a dokažte následující tvrzení.
   (a) Je-li $m \leq n + 1$, pak každá formule utvořená ze Σ_m- nebo Π_m-formule omezenou kvantifikací je $\mathrm{B}\Pi_n$-ekvivalentní se Σ_m- resp. s Π_m-formulí. Jinými slovy, množiny $\Sigma_m(\mathrm{B}\Pi_n)$ i $\Pi_m(\mathrm{B}\Pi_n)$ jsou uzavřeny na omezenou kvantifikaci.
   (b) Je-li $m \leq n + 2$, pak množiny $\Sigma_m(\mathrm{B}\Pi_n)$ i $\Pi_m(\mathrm{B}\Pi_n)$ jsou uzavřeny na konjunkci a disjunkci.
   (c) Je-li $0 < m \leq n + 2$, pak množina $\Sigma_m(\mathrm{B}\Pi_n)$ je uzavřena na existenční kvantifikaci a množina $\Pi_m(\mathrm{B}\Pi_n)$ je uzavřena na univerzální kvantifikaci.
   (d) $\mathrm{B}\Pi_n$ a $\mathrm{B}\Sigma_{n+1}$ jsou ekvivalentní teorie.

6. Teorie $\mathrm{I}\Gamma$, kde Γ je Σ_n nebo Π_n, má aritmetický jazyk, axiomy Q1–Q9 a schéma indukce pro Γ-formule. Teorie $\mathrm{I}\Sigma_0$, $\mathrm{I}\Pi_0$ a $\mathrm{I}\Delta_0$ jsou tedy totožné. Dokažte, že pro každé n platí, že $\mathrm{B}\Pi_n$ je podteorie teorie $\mathrm{I}\Sigma_{n+1}$, tj. že v $\mathrm{I}\Sigma_{n+1}$ lze dokázat všechny instance schématu kolekce utvořené z Π_n-formulí.

   Návod. Uvažujte v $\mathrm{I}\Sigma_{n+1}$ za předpokladu $\forall u{<}x\,\exists w\varphi(u, v, \underline{y})$, kde $\varphi \in \Pi_n$. Označte ψ formuli $z \leq x \ \rightarrow\ \exists w\forall u{<}z\,\exists v{<}w\,\varphi(u, v, \underline{y})$, zdůvodněte, že ψ je v $\Sigma_{n+1}(\mathrm{I}\Sigma_{n+1})$, a užijte indukci dle z.

7. Dokažte, že $\mathrm{I}\Sigma_n$ a $\mathrm{I}\Pi_n$ jsou ekvivalentní teorie.

Návod. Uvažujte za předpokladů $\varphi(0,\underline{y})$, $\forall v(\varphi(v,\underline{y}) \to \varphi(\mathrm{S}(v),\underline{y}))$ a $\neg\varphi(x,\underline{y})$. Indukcí dle z dokažte $\forall z\neg\varphi(x \dot{-} z,\underline{y})$ a pak zvolte $z := x$. Podrobněji, předpokládejte, že $\varphi \in \Sigma_n$, kde $n \geq 2$, a že usuzujete v $\mathrm{I}\Pi_n$. Označte $\psi(z,x,\underline{y})$ formuli $\forall u(z{+}u = x \to \neg\varphi(u,\underline{y}))$. Dokažte, že ψ je v $\Pi_n(\mathrm{I}\Pi_n)$. Přitom můžete předpokládat $\mathrm{I}\Sigma_{n-1}$, tedy $\mathrm{B}\Pi_{n-2}$, tudíž uzavřenost množiny $\Pi_n(\mathrm{I}\Pi_n)$ na univerzální kvantifikátory. Pak dokažte $\forall z\psi(z,x,\underline{y})$ indukcí dle z (tj. Π_n-indukcí). Je-li $\varphi \in \Pi_n$ a usuzujete-li v $\mathrm{I}\Sigma_n$, užijte formuli $\exists x(z + u = x \ \&\ \neg\varphi(u,\underline{y}))$. Domyslete i případy $n < 2$.

8. Dokažte, že pro každé n platí, že $\mathrm{I}\Sigma_n$ je podteorie teorie $\mathrm{B}\Pi_n$.

   Návod. Indukcí podle k dokažte, že v $\mathrm{B}\Pi_n$ lze dokázat schéma indukce pro Σ_k-formule. Nechť $0 < k \leq n$ a $\varphi(u,z,\underline{y}) \in \Pi_{n-1}$. Uvažujte v $\mathrm{B}\Pi_n$ za předpokladů $\exists z\varphi(0,z,\underline{y})$, $\forall v(\exists z\varphi(v,z,\underline{y}) \to \exists z\varphi(\mathrm{S}(v),z,\underline{y}))$ a $\neg\exists z\varphi(x,z,\underline{y})$. Zvolte za ψ formuli $\varphi(u,v,\underline{y}) \vee (\neg\exists z\varphi(u,z,\underline{y}) \ \&\ v = 0)$. Formule ψ je v $\overline{\Pi}_n(\mathrm{B}\Pi_n)$ a platí $\forall u{\leq}x\,\exists v\psi(u,v,\underline{y})$. Axiom $\mathrm{B}(\psi)$ dává $\exists w\forall u{\leq}x\,\exists v{<}w\,\psi(u,v,\underline{y})$. Pak podmínky $\exists z\varphi(v,z,\underline{y})$ a $\exists z{<}w\,\varphi(v,z,\underline{y})$ jsou pro $v \leq x$ ekvivalentní. To znamená, že formule $\exists z{<}w\,\varphi(v,z,\underline{y})$ porušuje Π_{k-1}-indukci.

9. Teorie $\mathrm{L}\Gamma$, kde Γ je Σ_n nebo Π_n, je teorie s aritmetickým jazykem, jejíž axiomy jsou Q1–Q9, $\forall x(x < \mathrm{S}(x))$, a dále všechny instance schématu LNP utvořené z Γ-formulí. Dokažte, že každá z teorií $\mathrm{L}\Sigma_n$ i $\mathrm{L}\Pi_n$ je ekvivalentní s teorií $\mathrm{I}\Sigma_n$.

   Poznamenejme, že teoriím $\mathrm{I}(\Gamma)$, $\mathrm{B}(\Gamma)$ a $\mathrm{L}(\Gamma)$, kde Γ je Σ_n nebo Π_n a $n \geq 1$, se obvykle říká *silné fragmenty Peanovy aritmetiky*. Za základní zdroj informace o těchto teoriích lze považovat článek [64]. V tomto a v předchozích cvičeních jsme zdůvodnili následující vztahy mezi silnými fragmenty Peanovy aritmetiky a teoriemi $\mathrm{I}\Delta_0$, $\mathrm{B}\Pi_0$ a PA:

$$\begin{array}{ccccccccccccc}
\mathrm{I}\Delta_0 & \Leftarrow & \ldots & \Leftarrow & \mathrm{I}\Sigma_n & \Leftarrow & \mathrm{B}\Pi_n & \Leftarrow & \mathrm{I}\Sigma_{n+1} & \Leftarrow & \ldots & \Leftarrow & \mathsf{PA} \\
 & & & & & & \Updownarrow & & \Updownarrow & & & & \\
 & & & & & & \mathrm{B}\Sigma_{n+1} & & \mathrm{I}\Pi_{n+1} & & & & \\
 & & & & & & & & \Updownarrow & & & & \\
 & & & & & & & & \mathrm{L}\Sigma_{n+1} & & & & \\
 & & & & & & & & \Updownarrow & & & & \\
 & & & & & & & & \mathrm{L}\Pi_{n+1}. & & & &
\end{array}$$

10. Nechť $\mathbf{M}$ je model Peanovy aritmetiky. Neprázdná množina $I \subseteq M$ je *řez*, jestliže je uzavřená na funkci S a na relaci $\leq$, tj. jestliže $\forall a(a \in I \Rightarrow \mathrm{S}(a) \in I)$ a $\forall a\forall b(a \leq b \ \&\ b \in I \to a \in I)$. Řez I je *segment*, je-li navíc uzavřen na sčítání a na násobení. Například množina všech standardních prvků modelu $\mathbf{M}$ je segment. Rozmyslete si, že je-li a nestandardní prvek modelu $\mathbf{M}$, pak množina $a + \mathrm{N}$, tj. množina $I = \{\, b \in M \,;\, \exists n \in \mathrm{N}(b \leq a + \overline{n}) \,\}$, je řez. Není to ale segment, protože $a \in I$ a $a + a \notin I$. Definujte analogicky množiny $a \cdot \mathrm{N}$ a a^{N}. Zdůvodněte, že obě jsou řezy, první není segment, druhá je segment.

11. Když $\mathbf{M} \models \mathsf{PA}$ a $I \subseteq M$ je segment, pak Δ_0-formule jsou absolutní pro segment I chápaný jako podstruktura struktury $\mathbf{M}$. Jinými slovy, segment I je Δ_0-elementární podstruktura struktury $\mathbf{M}$. Dokažte.

12. Užijte předchozí cvičení k důkazu, že když $\mathbf{M} \models \mathsf{PA}$ a $I \subseteq M$ je segment, pak $I \models \mathrm{I}\Delta_0$.

13. Dokažte, že za stejných předpokladů platí dokonce $I \models \mathrm{B}\Pi_0$.

14. Nechť $\mathbf{M} \models \mathsf{PA}$, nechť $b \in M$ je nestandardní prvek modelu $\mathbf{M}$, nechť $a \in M$ je dělitelný všemi $d \leq b$ a nechť $c \in M$ je dělitelný všemi prvky tvaru $1+(d+1)a$, kde $d \leq b$. Zdůvodněte využitím cvičení 7 oddílu 4.2, že (v $\mathbf{M}$) pro každé přirozené n platí $a^n < c$. Vyvoďte z toho, že c není prvek segmentu a^{N}. Zdůvodněte, že sentence $\forall x \forall z \exists t \forall v \leq x\, (\overline{1} + (v + \overline{1}) \cdot z \mid t)$ a $\forall x \exists w \forall v (v \in w \equiv v < x)$ nejsou dokazatelné v teorii $\mathrm{I}\Delta_0$ (ani v teorii $\mathrm{B}\Pi_0$).

4.4 Σ-úplnost Robinsonovy aritmetiky

V oddílu 4.1 jsme viděli, že Robinsonova aritmetika je slabou teorií, ve které nelze dokázat ani některá dost běžná tvrzení o přirozených číslech. Příkladem takového tvrzení je komutativita sčítání vyjádřená sentencí $\forall x \forall y (x + y = y + x)$.

Není-li jisté, že sčítání je komutativní, znamená to snad, že například $\overline{3} + \overline{2}$ by pro Robinsonovu aritmetiku mohlo být něco jiného než $\overline{2} + \overline{3}$? Uvidíme, že ne. V modelech Robinsonovy aritmetiky, které se vyskytly v oddílu 4.1 (včetně cvičení), vždy platilo $\overline{3} + \overline{2} = \overline{2} + \overline{3}$. Ukážeme, že je to zákonité. Robinsonova aritmetika ví, že $\overline{3} + \overline{2} = \overline{2} + \overline{3}$, protože ví, že $\overline{3} + \overline{2}$ i $\overline{2} + \overline{3}$ je rovno číslu $\overline{5}$. Prvky, které v nějakém modelu Robinsonovy aritmetiky porušují komutativitu sčítání, *musí* být nestandardní. Dále v tomto oddílu uvidíme, že tvrzení o dokazatelnosti sentence $\overline{3} + \overline{2} = \overline{2} + \overline{3}$ lze zobecnit: každá *sentence* platná v $\mathbf{N}$ je dokazatelná v Q za předpokladu, že je *syntakticky jednoduchá*.

Při našich úvahách rozhodně neopouštíme Peanovu aritmetiku. U řady výsledků bude důležité, že platí pro mnohé teorie (včetně Peanovy aritmetiky) vzniklé přidáním axiomů k Robinsonově aritmetice. A u některých tvrzení, která dokážeme o dokazatelnosti v Robinsonově aritmetice, bude také důležité, že jsou formalizovatelná v Peanově aritmetice.

Věta 4.4.1 *Sentence*

(a) $\overline{n} \neq \overline{m}, \qquad \neg(\overline{n} \leq \overline{m}) \quad a \quad \neg(\overline{n} < \overline{m})$

jsou dokazatelné v Q *za předpokladu, že platí v* $\mathbf{N}$*, tj. za předpokladu, že* $n \neq m$*,* $n > m$ *resp. že* $n \geq m$*. Sentence*

(b) $\overline{n} + \overline{m} = \overline{n+m}$,
(c) $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$,
(d) $\forall x (x \leq \overline{n} \to x = \overline{0} \vee \ldots \vee x = \overline{n})$,
(e) $\forall x (x \leq \overline{n} \vee \overline{n} \leq x)$

jsou v Q *dokazatelné pro každou volbu čísel* n *a* m*.*

Důkaz U všech sentencí uvedených ve znění věty je důležité si uvědomit, že pro každou volbu čísel n a m máme právo napsat *jiný* důkaz v Q. Ukažme si důkaz sentence v (b) například pro $n = 4$, $m = 3$:

> Axiom Q5 dává $\overline{4} + \mathrm{S}^{(3)}(0) = \mathrm{S}(\overline{4} + \mathrm{S}(\mathrm{S}(0)))$. Ještě dvojnásobným užitím axiomu Q5 dostaneme $\overline{4} + \mathrm{S}^{(3)}(0) = \mathrm{S}^{(3)}(\overline{4} + 0)$. Podle Q4 platí $\overline{4} + 0 = \overline{4}$, tedy opravdu $\overline{4} + \mathrm{S}^{(3)}(0) = \mathrm{S}^{(3)}(\overline{4})$.

Nyní uvažme, že $\mathrm{S}^{(3)}(0)$ je jen jiné označení pro term $\overline{3}$ a $\mathrm{S}^{(3)}(\overline{4})$ je jen jiné označení pro term $\overline{7}$. Podobný důkaz sentence $\overline{n} + \overline{m} = \overline{n+m}$ lze napsat pro každou dvojici čísel n a m. Axiom Q5 se v něm použije m-krát. Mohli bychom také říci, že existence důkazu se dokazuje metamatematickou indukcí podle m.

Existenci důkazu sentence v (d) dokažme rovněž indukcí podle n. Nechť důkaz pro n je již sestrojen:

> ...
> Tedy opravdu $\forall x(x \leq \overline{n} \to x = \overline{0} \vee \ldots \vee x = \overline{n})$. ($\mathsf{d}_n$)

Jeho následujícím prodloužením dostaneme důkaz pro $n + 1$:

> Nechť x je dáno, nechť $x \leq \overline{n+1}$. Platí $x = 0$ nebo $x \neq 0$.
>
> Když $x = 0$, jsme hotovi.
>
> Jinak je dle Q3 x následníkem nějakého y: $x = \mathrm{S}(y)$. Předpoklad $x \leq \overline{n+1}$ znamená existenci v takového, že $v + x = \overline{n+1}$. Tedy $v + \mathrm{S}(y) = \overline{n+1}$. Dále platí $\mathrm{S}(v + y) = \overline{n+1}$ (dle Q5) a $v + y = \overline{n}$ (dle Q1). Tedy $y \leq \overline{n}$. Z již dokázané formule (d_n) plyne $y = \overline{0} \vee \ldots \vee y = \overline{n}$. Tedy pro $x = \mathrm{S}(y)$ platí $x = \overline{1} \vee \ldots \vee x = \overline{n+1}$.
>
> Tedy opravdu $\forall x(x \leq \overline{n+1} \to x = \overline{0} \vee \ldots \vee x = \overline{n+1})$. ($\mathsf{d}_{n+1}$)

Podívejme se ještě na (e). Opět předpokládejme, že důkaz pro n je již sestrojen, a napišme důkaz pro $n + 1$.

> Nechť x je dáno. Dle již dokázané formule platí $x \leq \overline{n}$ nebo $\overline{n} \leq x$.
>
> Nechť $x \leq \overline{n}$. Podle (d) je x rovno jednomu z čísel $\overline{0}, \overline{1}, \ldots, \overline{n}$. Každé z nich je menší nebo rovno číslu $\overline{n+1}$. Tedy $x \leq \overline{n+1}$.
>
> Nechť naopak $\overline{n} \leq x$. Tedy $u + \overline{n} = x$ pro jisté u. Je-li $u = 0$, máme $\overline{n} = x$ a $x \leq \overline{n+1}$. Jinak $u = \mathrm{S}(v)$ pro jisté v. Pokud na rovnost $\mathrm{S}(v) + \overline{n} = x$ užijeme n-krát axiom Q5, pak dvakrát axiom Q2 a pak $(n+1)$-krát axiom Q5 opačným směrem, dostaneme $v + \overline{n+1} = x$. Tedy $\overline{n+1} \leq x$.

Důkaz formule v (d) a v (e) pro $n = 0$ a důkazy formulí v (a) a (c) přenecháváme čtenáři. QED

Některé kroky v důkazu předchozí věty jsou dost závislé na přesné formulaci axiomů Robinsonovy aritmetiky. Tvrzení (e) by se nepodařilo dokázat, kdybychom v axiomech Q8 a Q9 zaměnili pořadí sčítanců.

Věta 4.4.2 (Σ-úplnost Robinsonovy aritmetiky) *Je-li $\sigma \in \Sigma$ sentence taková, že $\mathbf{N} \models \sigma$, pak $\mathsf{Q} \vdash \sigma$.*

Mělo by být zřejmé, že oba předpoklady věty, tj. že $\sigma \in \Sigma$ a σ je sentence, jsou podstatné. Slovo „úplnost“ v označení věty je užito neformálně ve významu podobném jako v obratu „úplnost kalkulu“: v Q lze dokázat všechny Σ-sentence, které *mají* být dokazatelné (protože jsou pravdivé). Důkaz věty 4.4.2 rozdělíme do několika lemmat.

Lemma 4.4.3 *Nechť t je uzavřený term a nechť m je jeho hodnota v $\mathbf{N}$. Pak $\mathsf{Q} \vdash t = \overline{m}$.*

Důkaz indukcí podle složitosti termu t. Term t buď sestává z jediného symbolu 0, nebo je utvořen z jednodušších termů pomocí některého ze symbolů $+$, $\cdot$ a S. Předpokládejme, že t má tvar $(t_1 + t_2)$. Pak t_1 a t_2 jsou opět uzavřené termy. Vezměme jejich hodnoty m_1 a m_2 v $\mathbf{N}$. Indukční předpoklad dává $\mathsf{Q} \vdash t_1 = \overline{m_1}$ a $\mathsf{Q} \vdash t_2 = \overline{m_2}$. Dle Tarského podmínky T2, hodnotou termu t je číslo $m_1 + m_2$. Z toho a z 4.4.1(b) plyne $\mathsf{Q} \vdash t_1 + t_2 = \overline{m_1 + m_2}$. Ostatní případy jsou podobné. QED

Lemma 4.4.4 *Nechť σ je atomická sentence. Pokud $\mathbf{N} \models \sigma$, pak $\mathsf{Q} \vdash \sigma$, a pokud $\mathbf{N} \not\models \sigma$, pak $\mathsf{Q} \vdash \neg\sigma$.*

Důkaz Sentence σ musí mít jeden z tvarů $t_1 = t_2$ nebo $t_1 < t_2$ nebo $t_1 \leq t_2$, kde t_1 a t_2 jsou uzavřené termy. Vezměme hodnoty m_1 a m_2 termů t_1 a t_2 v $\mathbf{N}$. Platí $\mathbf{N} \models t_1 = \overline{m_1}$ a $\mathbf{N} \models t_2 = \overline{m_2}$. Předpokládejme, že sentence σ má tvar $t_1 \leq t_2$, ostatní dva případy jsou podobné. Lemma 4.4.3 dává $\mathsf{Q} \vdash t_1 = \overline{m_1}$ a $\mathsf{Q} \vdash t_2 = \overline{m_2}$.

Když $\mathbf{N} \models t_1 \leq t_2$, pak $\mathbf{N} \models \overline{m_1} \leq \overline{m_2}$, tedy $m_1 \leq m_2$ a lze vzít k takové, že $k + m_1 = m_2$. Z předpokladů $t_1 = \overline{m_1}$, $t_2 = \overline{m_2}$ a $\overline{k} + \overline{m_1} = \overline{m_2}$ (viz 4.4.1(b)) lze v Q dokázat $t_1 \leq t_2$ (viz Q8).

Když $\mathbf{N} \not\models t_1 \leq t_2$, pak $\mathbf{N} \not\models \overline{m_1} \leq \overline{m_2}$, a tedy $m_1 > m_2$. Z předpokladů $t_1 = \overline{m_1}$, $t_2 = \overline{m_2}$ a $\neg(\overline{m_1} \leq \overline{m_2})$ (viz tvrzení 4.4.1(a)) lze v Q dokázat $\neg(t_1 \leq t_2)$. QED

Lemma 4.4.5 *Nechť $\varphi(x_1, \ldots, x_r)$ je Δ_0-formule a nechť $n_1, \ldots, n_r$ jsou přirozená čísla. Pokud $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathsf{Q} \vdash \varphi(\overline{n_1}, \ldots, \overline{n_r})$, a pokud $\mathbf{N} \not\models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathsf{Q} \vdash \neg\varphi(\overline{n_1}, \ldots, \overline{n_r})$.*

Důkaz Dokazujeme indukcí podle počtu logických spojek a omezených kvantifikátorů ve formuli φ, že tvrzení platí pro každé dosazení numerálů za volné proměnné formule φ.

Je-li $\varphi(x_1, \ldots, x_r)$ atomická, pak $\varphi(\overline{n_1}, \ldots, \overline{n_r})$ je atomická sentence a tvrzení platí díky lemmatu 4.4.4.

Nechť formule $\varphi(x_1, \ldots, x_r)$ je tvaru $\varphi_1(\underline{x}) \,\&\, \varphi_2(\underline{x})$. Označme ψ_1 a ψ_2 sentence $\varphi_1(\overline{n_1}, \ldots, \overline{n_r})$ a $\varphi_2(\overline{n_1}, \ldots, \overline{n_r})$. Pak $\varphi(\overline{n_1}, \ldots, \overline{n_r})$ je $\psi_1 \& \psi_2$. Když $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathbf{N} \models \psi_1$ a $\mathbf{N} \models \psi_2$. Dle indukčního předpokladu platí $\mathsf{Q} \vdash \psi_1$ a $\mathsf{Q} \vdash \psi_2$. Pak

ovšem $\mathsf{Q} \vdash \psi_1 \,\&\, \psi_2$. Když $\mathbf{N} \not\models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathbf{N} \not\models \psi_1$ nebo $\mathbf{N} \not\models \psi_2$. Dle indukčního předpokladu platí $\mathsf{Q} \vdash \neg\psi_1$ nebo $\mathsf{Q} \vdash \neg\psi_2$. V obou případech máme $\mathsf{Q} \vdash \neg(\psi_1 \,\&\, \psi_2)$, protože obě sentence $\neg\psi_1 \to \neg(\psi_1 \,\&\, \psi_2)$ a $\neg\psi_2 \to \neg(\psi_1 \,\&\, \psi_2)$ jsou tautologie, a jsou tedy dokazatelné v Q.

Nechť $\varphi(x_1, \ldots, x_r)$ je tvaru $\neg\varphi_1(x_1, \ldots, x_r)$. Označme ψ sentenci $\varphi_1(\overline{n_1}, \ldots, \overline{n_r})$. Pak $\varphi(\overline{n_1}, \ldots, \overline{n_r})$ je $\neg\psi$. Když $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathbf{N} \not\models \psi$. Dle indukčního předpokladu $\mathsf{Q} \vdash \neg\psi$. Když $\mathbf{N} \not\models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathbf{N} \models \psi$, $\mathsf{Q} \vdash \psi$ a $\mathsf{Q} \vdash \neg\neg\psi$. Přitom $\neg\neg\psi$ je $\neg\varphi(\overline{n_1}, \ldots, \overline{n_r})$.

Nechť $\varphi(x_1, \ldots, x_r)$ je tvaru $\forall v{\leq}x_j\, \varphi_1(v, x_1, \ldots, x_r)$, kde $1 \leq j \leq k$. Označme $\psi(v)$ formuli $\varphi_1(v, \overline{n_1}, \ldots, \overline{n_r})$. Pak $\varphi(\overline{n_1}, \ldots, \overline{n_r})$ je sentence $\forall v{\leq}\overline{n_j}\, \psi(v)$. Pišme m místo n_j. Když $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathbf{N} \models \forall v{\leq}\overline{m}\, \psi(v)$ a v $\mathbf{N}$ platí všechny sentence $\psi(\overline{0}), \ldots, \psi(\overline{m})$. Indukční předpoklad pro φ_1 říká, že *každá* sentence vzniklá z φ_1 dosazením numerálů je dokazatelná v Q, pokud ovšem platí v $\mathbf{N}$. Všechny sentence $\psi(\overline{0}), \ldots, \psi(\overline{m})$ jsou tedy dokazatelné v Q. Z předpokladů $\psi(\overline{0}), \ldots, \psi(\overline{m})$ lze v Q dokázat $\forall v{\leq}\overline{m}\, \psi(v)$ díky 4.4.1(d). Úvaha týkající se případu $\mathbf{N} \not\models \varphi(\overline{n_1}, \ldots, \overline{n_r})$ je podobná.

Úvahy týkající se ostatních omezených kvantifikátorů a případů, kdy $\varphi(x_1, \ldots, x_r)$ je utvořena z jednodušších formulí pomocí disjunkce nebo implikace, jsou rovněž analogické a přenecháváme je čtenáři. QED

Lemma 4.4.6 *Nechť $\varphi(x_1, \ldots, x_r)$ je Σ-formule a nechť $n_1, \ldots, n_r$ jsou přirozená čísla. Když $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_r})$, pak $\mathsf{Q} \vdash \varphi(\overline{n_1}, \ldots, \overline{n_r})$.*

Důkaz Podobně jako v 4.4.5 dokazujeme indukcí podle počtu kroků, kterými je formule φ utvořena z Δ_0-formulí, že tvrzení platí pro každé dosazení numerálů za její proměnné $x_1, \ldots, x_r$. Je-li počet oněch kroků nulový, pak φ je Δ_0-formule a tvrzení pro ni platí díky lematu 4.4.5.

V důkazu lematu 4.4.5 je důležité si všimnout, že v kroku týkajícím se negace a implikace (což jsou kroky, které nyní v úvahu nepřipadají) se při důkazu pozitivního případu (když $\models$, pak $\vdash$) použije indukční předpoklad pro negativní případ (když $\not\models$, pak $\vdash \neg$). Ale v krocích týkajících se konjunkce, disjunkce a omezené kvantifikace se při důkazu pozitivního případu vystačí s indukčním předpokladem rovněž pro pozitivní případ. To znamená, že je-li φ utvořena z jednodušších Σ-formulí pomocí konjunkce, disjunkce nebo omezené kvantifikace, lze postupovat úplně stejně jako v důkazu lemmatu 4.4.5.

Nechť $\varphi(x_1, \ldots, x_r)$ je tvaru $\exists v \varphi_1(v, x_1, \ldots, x_r)$ a nechť $\mathbf{N} \models \varphi(\overline{n_1}, \ldots, \overline{n_r})$. Platí tedy $\mathbf{N} \models \varphi_1(\overline{m}, \overline{n_1}, \ldots, \overline{n_r})$ pro jisté m. Indukční předpoklad dává $\mathsf{Q} \vdash \varphi_1(\overline{m}, \overline{n_1}, \ldots, \overline{n_r})$. Z předpokladu $\varphi_1(\overline{m}, \overline{n_1}, \ldots, \overline{n_r})$ lze v Q dokázat $\exists v \varphi_1(v, \overline{n_1}, \ldots, \overline{n_r})$. QED

Tím je dokázána věta 4.4.2, tj. věta o Σ-úplnosti Robinsonovy aritmetiky: v lematu 4.4.6 stačí volit $r = 0$ a dostaneme tvrzení pro sentence.

V závěru důkazu lematu 4.4.6 stojí ještě za povšimnutí, že kvantifikátory se v nyní uvažovaném kontextu nechovají „duálně“. Když některá instance $\varphi(\overline{m})$ formule $\varphi(x)$ je dokazatelná, znamená to i dokazatelnost sentence $\exists x \varphi(x)$, jsou-li však

všechny instance $\varphi(\overline{m})$ formule $\varphi(x)$ dokazatelné, nemusí to znamenat dokazatelnost sentence $\forall x\varphi(x)$.

Na konci oddílu 4.2 jsme poznamenali, že tehdy dosažené výsledky o formulích, jako je $\mathsf{Sent}(x)$ nebo $\mathsf{LogAx}(x)$, popisujících syntaktické pojmy, lze většinou rozdělit na výsledky o dokazatelnosti obecných faktů v PA a na výsledky o platnosti numerických instancí v $\mathbf{N}$. Nyní víme více i o dokazatelnosti numerických instancí. Je-li φ sentencí, pak podle 4.2.11(a) platí $\mathbf{N} \models \mathsf{Sent}(\overline{\varphi})$. Σ-úplnost (plus fakt, že $\mathrm{Thm}(\mathsf{Q}) \subseteq \mathrm{Thm}(\mathsf{PA})$) dává $\mathsf{PA} \vdash \mathsf{Sent}(\overline{\varphi})$, protože $\mathsf{Sent}(x)$ je Σ-formule, viz 4.3.5. Ze stejného důvodu, je-li φ axiomem Peanovy aritmetiky, platí $\mathbf{N} \models \pi(\overline{\varphi})$ a $\mathsf{PA} \vdash \pi(\overline{\varphi})$. Je-li m důkazem formule φ v PA, pak (viz 4.2.12) $\mathsf{Q} \vdash \mathsf{Proof}_\pi(\overline{\varphi}, \overline{m})$. A je-li φ dokazatelná v Q nebo v PA, pak (viz 4.2.13) $\mathsf{PA} \vdash \mathsf{Pr}_\mathsf{Q}(\overline{\varphi})$ resp. $\mathsf{PA} \vdash \mathsf{Pr}_\pi(\overline{\varphi})$. Formule Proof_π, Pr_Q a Pr_π jsou totiž všechny v Σ. Ukažme si, že z toho v podstatě plyne odpověď na jednu z otázek ze závěru oddílu 4.2. Nechť $\tau(z)$ definuje množinu axiomů nějaké teorie T v $\mathbf{N}$, a nechť navíc $\tau(z) \in \Sigma$. Domluvme se, že tento případ (kdy $\tau(z) \in \Sigma$) nás zajímá především. Pak podmínky $T \vdash \varphi$ a $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi})$ jsou ekvivalentní: o implikaci $\Leftarrow$ jsme se již zmínili v závěru oddílu 4.2, implikace $\Rightarrow$ je 4.2.13, plus $\mathrm{Thm}(\mathsf{Q}) \subseteq \mathrm{Thm}(\mathsf{PA})$, plus Σ-úplnost. Peanova aritmetika může o všech formulích φ dokazatelných v nějaké teorii T tvrdit, že jsou dokazatelné, pokud jí množinu axiomů teorie T popíšeme nějakou Σ-formulí. A popsat množinu axiomů teorie T nějakou Σ-formulí lze právě tehdy, je-li T rekurzívně axiomatizovatelná.

Věta o Σ-úplnosti nám umožňuje tvrdit něco i o dokazatelnosti negovaných numerických instancí. Není-li φ například logickým axiomem, pak $\mathbf{N} \models \neg\mathsf{LogAx}(\overline{\varphi})$ podle 4.2.11(a). V tom případě platí $\mathsf{PA} \vdash \neg\mathsf{LogAx}(\overline{\varphi})$, neboť formule $\neg\mathsf{LogAx}(x)$ je $\Sigma(\mathsf{PA})$-formule, viz 4.3.5(b). Podobně není-li m důkazem formule φ v PA, pak $\mathsf{PA} \vdash \neg\mathsf{Proof}_\pi(\overline{\varphi}, \overline{m})$ dle 4.3.5(e). To ale nedává odpověď na otázku, jaký je vztah mezi podmínkami $\mathsf{PA} \nvdash \varphi$ a $\mathsf{PA} \vdash \neg\mathsf{Pr}_\pi(\overline{\varphi})$. O formuli $\neg\mathsf{Pr}_\pi(x)$ jsme totiž nikdy netvrdili, že je v $\Sigma(\mathsf{PA})$. Pomohla by nám „věta o Π_1-úplnosti“, viz 4.3.5(e), tu ale nemáme, a z věty 4.3.12 víme, že určitě neplatí.

V následující větě 4.4.8 zobecníme větu 4.3.12 ve dvou směrech. Jednak Σ-úplnost nám umožní dokázat nerozhodnutelnost příslušné teorie. A dále si uvědomíme, že není nutné, aby teorie T měla aritmetický jazyk. Má-li *alespoň* aritmetický jazyk, tj. má-li nějaký jazyk L, v němž je všech šest symbolů aritmetického jazyka, pak každá aritmetická formule je zároveň formulí jazyka L, a o aritmetických sentencích dokazatelných v T můžeme říkat totéž, co jsme říkali dosud.

Definice 4.4.7 *Nechť T je teorie s alespoň aritmetickým jazykem. Řekneme, že T je* korektní*, jestliže každá aritmetická sentence dokazatelná v T platí v $\mathbf{N}$. Řekneme, že T je* Σ-korektní*, jestliže každá aritmetická Σ-sentence dokazatelná v T platí v $\mathbf{N}$.*

Je zřejmé, že PA obsahuje Q, teorie PA i Q jsou korektní, každá korektní teorie je Σ-korektní a každá Σ-korektní teorie je bezesporná. Připomeňme, že teorie T obsahuje teorii S, jestliže platí inkluze $L(S) \subseteq L(T)$ pro jejich jazyky a inkluze $\mathrm{Thm}(S) \subseteq \mathrm{Thm}(T)$ pro množiny všech dokazatelných sentencí.

Věta 4.4.8 *Nechť T je rekurzívně axiomatizovatelná teorie, která obsahuje Robinsonovu aritmetiku a je Σ-korektní. Pak T je nerozhodnutelná a neúplná. Existují dokonce Σ_1- a Π_1-sentence nezávislé na T.*

Důkaz Postupujme podobně jako v důkazech vět 4.3.10 a 4.3.12. Nechť $A \subseteq \mathrm{N}$ je rekurzívně spočetná množina. Díky tvrzení 4.3.9(a) existuje Σ_1-formule $\varphi(x)$, která definuje množinu A v $\mathbf{N}$:

$$\forall n(n \in A \Leftrightarrow \mathbf{N} \models \varphi(\overline{n})). \tag{1}$$

Podmínka $\mathbf{N} \models \varphi(\overline{n})$ je ekvivalentní s $T \vdash \varphi(\overline{n})$: jestliže $\mathbf{N} \models \varphi(\overline{n})$, pak $\mathsf{Q} \vdash \varphi(\overline{n})$ vzhledem k Σ-úplnosti a $T \vdash \varphi(\overline{n})$ díky předpokladu, že T obsahuje Q, a naopak jestliže $T \vdash \varphi(\overline{n})$, pak $\mathbf{N} \models \varphi(\overline{n})$ díky předpokladu, že T je Σ-korektní. Ekvivalenci (1) tedy můžeme přepsat na

$$\forall n(n \in A \Leftrightarrow T \vdash \varphi(\overline{n})). \tag{2}$$

Podmínka (2) znamená $A \leq_{\mathrm{m}} \mathrm{Thm}(T)$ prostřednictvím funkce $n \mapsto \varphi(\overline{n})$. Toto platí pro každou rekurzívně spočetnou množinu A. Každá $A \in \mathit{RE}$ je tedy převeditelná na množinu $\mathrm{Thm}(T)$. Z věty 3.6.6 víme, že $\mathrm{Thm}(T)$ je rekurzívně spočetná. Množina $\mathrm{Thm}(T)$ je tedy Σ_1-kompletní, a tedy nerekurzívní. Teorie T je nerozhodnutelná.

Existence nezávislých Σ_1- a Π_1-sentencí plyne z (důkazu) věty 4.3.12. Ukažme si ale ještě jiné zdůvodnění. Vraťme se k ekvivalenci (2) a mysleme si, že rekurzívně spočetná množina A byla zvolena pevně a že je nerekurzívní. Označme Y množinu $\{\, n \,;\, T \vdash \neg\varphi(\overline{n}) \,\}$. Z (2) plyne $A \cap Y = \emptyset$, jinak by T byla sporná. Množina Y je rekurzívně spočetná, a to například proto, že je prostřednictvím funkce $n \mapsto \neg\varphi(\overline{n})$ převeditelná na množinu $\mathrm{Thm}(T)$. Platí-li $A \cup Y = \mathrm{N}$, pak podle Postovy věty 2.2.27 množiny A i Y jsou rekurzívní. To ale nejsou, o A předpokládáme, že je nerekurzívní. Tedy $A \cup Y \neq \mathrm{N}$, takže můžeme zvolit $n_0 \notin A \cup Y$. Podmínka $n_0 \notin Y$ znamená $T \nvdash \neg\varphi(\overline{n_0})$ a podmínka $n_0 \notin A$ znamená $T \nvdash \varphi(\overline{n_0})$ vzhledem k (2). Tedy $\varphi(\overline{n_0})$ je nezávislá Σ_1-sentence a $\neg\varphi(\overline{n_0})$ je T-ekvivalentní s nezávislou Π_1-sentencí. QED

Nechť T je rekurzívně axiomatizovatelná teorie s aritmetickým jazykem a nechť platí $\mathbf{N} \models T$. Utvořme teorii $(T + \mathsf{Q})$, tj. přidejme k T axiomy Robinsonovy aritmetiky. Dostaneme teorii, která splňuje předpoklady věty 4.4.8, a je tedy neúplná. Je-li $(T+\mathsf{Q})$ neúplná, pak ovšem i T je neúplná. Tím je zdůvodněno, že věta 4.4.8 je zesílením věty 4.3.12. Větu 4.4.8 také považujme za jednu z variant První Gödelovy věty o neúplnosti.

Když θ je Δ_0-sentence, pak θ i $\neg\theta$ jsou Σ-sentence a ta z nich, která platí v $\mathbf{N}$, je podle věty o Σ-úplnosti dokazatelná už v Q. Tato úvaha doplňuje naši dřívější odpověď (danou větou 4.3.12) na otázku ze závěru oddílu 4.3, pro které nejmenší n existují Σ_n-sentence nezávislé na PA. Nezávislé Σ_1- a Π_1-sentence existují, nezávislé Δ_0-sentence neexistují. A Peanova aritmetika se v tomto ohledu nijak neliší od Robinsonovy aritmetiky.

Pozastavme se ještě u důkazu věty 4.4.8. Formule $\varphi(x)$ je Σ_1, lze ji tedy psát ve tvaru $\exists v \lambda(x, v)$, kde $\lambda \in \Delta_0$. Víme, že sentenci $\forall v \neg\lambda(\overline{n_0}, v)$ nelze dokázat v T. Z ekvivalencí (1) a (2) plyne, že sentence $\forall v \neg\lambda(\overline{n_0}, v)$ platí v $\mathbf{N}$ (kdyby ne, byla by sentence $\exists v \lambda(\overline{n}, v)$ protipříkladem na větu o Σ-úplnosti). V $\mathbf{N}$ tedy platí i všechny sentence tvaru $\neg\lambda(\overline{n_0}, \overline{k})$. Každá z těchto sentencí je Δ_0, a je tedy dokazatelná v T. Existuje tedy Δ_0-formule $\theta(v)$ taková, že všechny instance tvaru $\theta(\overline{k})$ jsou dokazatelné v T, ale $\forall v \theta(v)$ nikoliv. Pro Robinsonovu aritmetiku jsme to věděli, tam stačilo za $\theta(v)$ volit například formuli $0 + v = v$. Fakt, že taková Δ_0-formule existuje pro každou „rozumnou“ teorii T, se může zdát překvapivý. Domníváme se ale, že je přirozený. Platí-li všechny instance $\theta(\overline{0})$, $\theta(\overline{1})$, $\theta(\overline{2})$, … ve struktuře $\mathbf{N}$, je správné usoudit, že v $\mathbf{N}$ platí i sentence $\forall v \theta(v)$. Ale máme-li nekonečně mnoho různých důkazů, jeden pro každou sentenci $\theta(\overline{k})$, nemusí to znamenat, že z nich lze utvořit jeden společný důkaz sentence $\forall v \theta(v)$. Podobná situace se vyskytuje i v teoretické informatice: máme-li pro každé n program, který počítá nějakou funkci $g_n : \mathrm{N} \to \mathrm{N}$, nemusí to znamenat existenci společného programu, který počítá funkci $[n, x] \mapsto g_n(x)$.

Z věty 4.4.8 můžeme usoudit něco i o rozhodnutelnosti predikátové logiky.

Věta 4.4.9 *Množina všech formulí v jazyce aritmetiky, které jsou logicky platné, je algoritmicky nerozhodnutelná.*

Důkaz Robinsonova aritmetika je podle věty 4.4.8 nerozhodnutelnou teorií. Odstraníme-li z nerozhodnutelné teorie konečně mnoho axiomů, dostaneme opět nerozhodnutelnou teorii, viz větu 3.6.10. Robinsonova aritmetika je konečně axiomatizovatelná, můžeme tedy odstranit všechny. Formule v aritmetickém jazyce dokazatelné v teorii bez vlastních axiomů jsou podle věty o úplnosti predikátového kalkulu přesně ty, které jsou logicky platné. QED

O Peanově aritmetice víme, že existuje Π_1-sentence ψ, kterou v PA nelze dokázat ani vyvrátit. Tedy $(\mathsf{PA} + \psi)$ i $(\mathsf{PA} + \neg\psi)$ jsou bezesporné teorie. Jen jedna z nich je korektní, a lze dokonce říci která. Kdyby totiž v $\mathbf{N}$ platila sentence $\neg\psi$, musela by být dokazatelná, protože je to $\Sigma(\mathsf{Q})$-sentence, a ψ by tudíž nemohla být nezávislá na PA. Takže $(\mathsf{PA} + \psi)$ je korektní teorie a podle věty 4.4.8 je neúplná a nerozhodnutelná. Teorie $(\mathsf{PA} + \neg\psi)$ není Σ-korektní, a věta 4.4.8 se na ni tudíž nevztahuje. Nyní uvidíme, že větu 4.4.8 lze zobecnit i na nekorektní teorie, a tím definitivně odpovíme na první dvě otázky ze závěru oddílu 4.1. Žádné přidání rekurzívní množiny axiomů k PA nebo ke Q nedá úplnou teorii, a to bez ohledu na to, zda přidané axiomy platí v $\mathbf{N}$. Žádné přidání rekurzívní množiny axiomů ke Q nedá rozhodnutelnou teorii, ledaže bychom porušili bezespornost.

Lemma 4.4.10 *Nechť $A \subseteq \mathrm{N}$ a $B \subseteq \mathrm{N}$ jsou disjunktní rekurzívně spočetné množiny. Pak existuje formule $\varphi(x) \in \Sigma_1$ taková, že $\mathsf{Q} \vdash \varphi(\overline{n})$, kdykoliv $n \in A$, a $\mathsf{Q} \vdash \neg\varphi(\overline{n})$, kdykoliv $n \in B$.*

Důkaz Dle tvrzení 4.3.9(a) množiny A a B jsou Σ_1-definovatelné v $\mathbf{N}$. Existují tedy Δ_0-formule $\theta(x,v)$ a $\lambda(x,v)$ takové, že formule $\exists v\theta(x,v)$ definuje množinu A a formule $\exists v\lambda(x,v)$ definuje množinu B:

$$\forall n(n \in A \Leftrightarrow \mathbf{N} \models \exists v\theta(\overline{n},v)), \tag{1}$$
$$\forall n(n \in B \Leftrightarrow \mathbf{N} \models \exists v\lambda(\overline{n},v)). \tag{2}$$

Označme $\varphi(x)$ formuli $\exists v(\theta(x,v) \,\&\, \forall u{\leq}v\neg\lambda(x,u))$. Formule $\theta(x,v)$ a $\lambda(x,v)$ lze číst číslo v je svědek pro náležení čísla x do množiny A resp. do množiny B. V tom případě formule $\varphi(x)$ říká náležení čísla x do A se dosvědčí dříve než náležení do B. Evidentně platí $\varphi \in \Sigma_1$. Ověříme, že formule φ má i ostatní požadované vlastnosti. Předpokládejme $n \in A$. Pak $n \notin B$, protože A a B jsou disjunktní množiny. V tom případě z podmínek (1) a (2) plyne $\mathbf{N} \models \varphi(\overline{n})$. Dále Σ-úplnost dává $\mathsf{Q} \vdash \varphi(\overline{n})$. Zbývá dokázat implikaci $n \in B \;\Rightarrow\; \mathsf{Q} \vdash \neg\varphi(\overline{n})$. Nechť tedy $n \in B$. Díky podmínce (2) existuje m takové, že $\mathbf{N} \models \lambda(\overline{n},\overline{m})$. Σ-úplnost dává

$$\mathsf{Q} \vdash \lambda(\overline{n},\overline{m}). \tag{3}$$

Protože množiny A a B jsou disjunktní, máme $n \notin A$, tedy $\mathbf{N} \models \forall v\neg\theta(\overline{n},v)$. Tudíž pro každé k platí $\mathbf{N} \models \neg\theta(\overline{n},\overline{k})$, a opětovné užití Σ-úplnosti dává

$$\forall k(\mathsf{Q} \vdash \neg\theta(\overline{n},\overline{k})). \tag{4}$$

Chceme v Q dokázat sentenci $\neg\varphi(\overline{n})$, tj. sentenci $\forall v(\theta(\overline{n},v) \to \exists u{\leq}v\,\lambda(\overline{n},u))$. Postupujme takto:

> Nechť v je dáno a nechť $\theta(\overline{n},v)$. Platí $v \leq \overline{m}$ nebo $\overline{m} \leq v$, viz 4.4.1(e).
>
> Případ $v \leq \overline{m}$ je ale vyloučen. Když totiž $v \leq \overline{m}$, pak dle 4.4.1(d) je v jedno z čísel $\overline{0},\overline{1},\ldots,\overline{m}$ a pro každé z těchto v platí $\neg\theta(\overline{n},v)$, viz (4).
>
> Takže $\overline{m} \leq v$. V tom případě existuje číslo $u \leq v$, totiž $\overline{m}$, pro které platí $\lambda(\overline{n},u)$, viz (3).

QED

Připomeňme, že $\mathrm{Ref}(T)$ označuje množinu $\{\,\varphi\,;\,\varphi$ je sentence a $T \vdash \neg\varphi\,\}$, tj. množinu všech sentencí vyvratitelných v T.

Věta 4.4.11 (Rosserova) *Nechť T je rekurzívně axiomatizovatelná teorie, která obsahuje Robinsonovu aritmetiku a je bezesporná. Pak existují Σ_1- a Π_1-sentence nezávislé na T. Každá z množin $\mathrm{Thm}(T)$ a $\mathrm{Ref}(T)$ je Σ_1-kompletní. Teorie T je tedy neúplná a nerozhodnutelná.*

Důkaz Díky větě 2.2.47 můžeme zvolit disjunktní rekurzívně spočetné množiny A a B přirozených čísel takové, že každá rekurzívně spočetná nadmnožina jedné z nich disjunktní s druhou je Σ_1-kompletní. Podle lemmatu 4.4.10 k množinám

A a B existuje Σ_1-formule $\varphi(x)$ taková, že $\mathsf{Q} \vdash \varphi(\overline{n})$ pro všechna $n \in A$ a $\mathsf{Q} \vdash \neg\varphi(\overline{n})$ pro všechna $n \in B$. Protože teorie T obsahuje Robinsonovu aritmetiku, máme

$$\forall n(n \in A \;\Rightarrow\; T \vdash \varphi(\overline{n})), \tag{1}$$
$$\forall n(n \in B \;\Rightarrow\; T \vdash \neg\varphi(\overline{n})). \tag{2}$$

Opačné implikace netvrdíme, k tomu bychom potřebovali Σ-korektnost. Položme $X = \{\, n \,;\, T \vdash \varphi(\overline{n}) \,\}$ a $Y = \{\, n \,;\, T \vdash \neg\varphi(\overline{n}) \,\}$. Jako v důkazu věty 4.4.8 rekurzívní axiomatizovatelnost teorie T dává $X \in \mathit{RS}$ a $Y \in \mathit{RS}$. Navíc množiny X a Y jsou disjunktní, jinak by T byla sporná. Podmínky (1) a (2) dávají $A \subseteq X$ a $B \subseteq Y$. Kdyby platilo $\mathrm{N} = X \cup Y$, podle Postovy věty by množina X byla rekurzívní. To není možné, rekurzívní nadmnožiny množiny A disjunktní s B neexistují. Platí tedy $\mathrm{N} \neq X \cup Y$, takže existuje $n_0 \notin X \cup Y$. Pak $\varphi(\overline{n_0})$ je nezávislá Σ_1-sentence, $\neg\varphi(\overline{n_0})$ je nezávislá $\Pi_1(T)$-sentence, a T je tedy neúplná.

Platí $X \leq_{\mathrm{m}} \mathrm{Thm}(T)$ via $n \mapsto \varphi(\overline{n})$ a $Y \leq_{\mathrm{m}} \mathrm{Ref}(T)$ via $n \mapsto \neg\varphi(\overline{n})$. Množiny $\mathrm{Thm}(T)$ a $\mathrm{Ref}(T)$ jsou rekurzívně spočetné. Je jasné, že rekurzívně spočetná množina, na kterou je převeditelná Σ_1-kompletní množina, je také Σ_1-kompletní (viz poznámku za příkladem 2.2.32). Tedy $\mathrm{Thm}(T)$ a $\mathrm{Ref}(T)$ jsou Σ_1-kompletní množiny. QED

Větu 4.4.11 lze označit jako Rosserovu verzi První Gödelovy věty o neúplnosti. Rosserovi se připisuje nápad, na kterém je založena konstrukce formule $\varphi(x)$ v důkazu věty 4.4.11: mluvit o tom, zda svědek pro náležení čísla x do množiny A je menší nebo větší než svědek pro náležení x do množiny B, a nespoléhat se na fakt, že obojí najednou dosvědčit nelze. Podmínka „A a B jsou disjunktní“ totiž není Σ a jako taková je uvnitř teorie T nejistá, přestože ve skutečnosti platí. Rosserova metoda „porovnávání svědků“ umožnila zobecnit První Gödelovu větu i na nekorektní teorie.

Nerozhodnutelnost (některé aritmetiky nebo predikátové logiky) se někdy cituje jako *Churchova věta*. Základními odkazy jsou [42] a [41]. Metoda důkazu věty 4.4.9, přes větu 3.6.10, také patří Churchovi. Důkazy vět 4.4.8 a 4.4.11, které jsme uvedli, jsou v podstatě převzaty z rukopisu C. Smoryńského [83].

Tvrzení věty 4.4.11 o nerozhodnutelnosti lze přeformulovat pomocí pojmu podstatně nerozhodnutelná teorie.

Definice 4.4.12 *Teorie T je* podstatně nerozhodnutelná*, jestliže T je bezesporná a každá bezesporná teorie S obsahující T je nerozhodnutelná.*

Věta 4.4.13 *Robinsonova aritmetika Q je podstatně nerozhodnutelná.*

Je-li f rekurzívní funkce jedné proměnné, pak její graf je rekurzívně spočetná množina, a existuje tedy Σ_1-formule $\varphi(x, y)$, která jej definuje v $\mathbf{N}$. Tedy v $\mathbf{N}$ platí sentence $\varphi(\overline{n}, \overline{m})$, právě když $m = f(n)$. Z toho plyne $\mathbf{N} \models \forall x \exists! y \varphi(x, y)$. Díky Σ-úplnosti víme, že $\mathbf{N} \models \varphi(\overline{n}, \overline{m})$, právě když $\mathsf{Q} \vdash \varphi(\overline{n}, \overline{m})$. Takže je-li m funkční hodnotou v bodě n, uvnitř Q víme, že $\overline{m}$ je funkční hodnotou v bodě $\overline{n}$.

Uvnitř Q ale nevíme, že každé číslo má jednoznačně určenou funkční hodnotu, protože $\forall x \exists! y \varphi(x,y)$ není Σ-sentence. Ale formule $\varphi(x,y)$ není funkcí f jednoznačně určena. Je více způsobů, jak Robinsonově (nebo Peanově) aritmetice popsat funkci f. V následující větě ukážeme, že popis funkce f aritmetickou Σ_1-formulí lze zvolit tak, aby uvnitř Q bylo jisté, že alespoň standardní čísla mají jednoznačně určenou funkční hodnotu. Jinými slovy, formuli φ definující graf funkce f lze zvolit tak, aby všechny sentence tvaru $\exists! y \varphi(\overline{n}, y)$ byly dokazatelné. Dokazatelnost sentence $\forall x \exists! y \varphi(x,y)$ zaručit nelze, ale bez té se obejdeme.

Větu 4.4.14 uvádíme zde, protože důkaz je snazší, máme-li v paměti větu 4.4.1 a důkaz Rosserovy věty 4.4.11. Použijeme ji ale až v následujícím oddílu, v důkazu věty o autoreferenci. V důkazu věty 4.4.14 se stejně jako v důkazu věty 4.4.11 a na rozdíl od důkazů vět 4.4.2 a 4.4.8 uplatní tvrzení (e) věty 4.4.1.

Věta 4.4.14 (Reprezentovatelnost funkcí v Q) *Pro každou obecně rekurzívní funkci f existuje Σ_1-formule $\varphi(x,y)$ taková, že pro každé n platí*

$$\mathsf{Q} \vdash \forall y \big(\varphi(\overline{n}, y) \;\equiv\; y = \overline{f(n)} \,\big). \tag{$*$}$$

Důkaz Graf funkce f je rekurzívně spočetná množina. Existuje tedy Δ_0-formule $\theta(x,y,v)$ taková, že formule $\exists v \theta(x,y,v)$ jej definuje v $\mathbf{N}$. Tedy ekvivalence

$$m = f(n) \;\Leftrightarrow\; \mathbf{N} \models \exists v \theta(\overline{n}, \overline{m}, v) \tag{1}$$

platí pro libovolnou dvojici čísel m a n. Formuli $\theta(x,y,v)$ lze číst číslo v svědčí pro fakt, že y je funkční hodnota funkce f v bodě x. Na metamatematické úrovni má každé n jednoznačně určenou funkční hodnotu $f(n)$. Uvnitř Robinsonovy aritmetiky ale není zaručeno, že ke každému x existuje y, pro které lze dosvědčit, že je funkční hodnotou v bodě x, a není ani vyloučena existence vzájemně si protiřečících svědků. Naším úkolem je nově definovat význam „svědectví“ tak, aby alespoň standardní čísla $\overline{0}$, $\overline{1}$, $\overline{2}$, … měla jednoznačně určenou funkční hodnotu, a to stejnou jako ve skutečnosti. To uděláme následovně. Označme $\varphi(x,y)$ formuli

$$\exists w (y \le w \;\&\; \exists v {\le} w \, \theta(x,y,v) \;\&\; \forall z {\le} w \forall v {\le} w \, (\theta(x,z,v) \;\to\; z = y)).$$

Číslu w ve formuli φ říkejme „svědek v novém smyslu“. Číslo w svědčí pro y v novém smyslu, jestliže mezi čísly nepřevyšujícími w jsou y i svědkové pro y ve starém smyslu, ale nejsou tam vzájemně si protiřečící svědkové. Ověříme, že formule φ má požadovanou vlastnost.

Nechť n_0 je pevné. Označme $m_0 = f(n_0)$ a zvolme pevně číslo k_0, pro které platí $\mathbf{N} \models \theta(\overline{n_0}, \overline{m_0}, \overline{k_0})$. To lze díky podmínce (1). Z toho a ze Σ-úplnosti plyne

$$\mathsf{Q} \vdash \theta(\overline{n_0}, \overline{m_0}, \overline{k_0}), \tag{2}$$

$$\mathsf{Q} \vdash \neg\theta(\overline{n_0}, \overline{m}, \overline{k}), \qquad \text{je-li } m \neq m_0 \text{ a } k \text{ libovolné.} \tag{3}$$

Netvrdíme ovšem nic o dokazatelnosti sentence $\forall v \neg\theta(\overline{n_0}, \overline{m}, v)$, ta není Σ. Označme $r = \max\{m_0, k_0\}$. Platí $\mathsf{Q} \vdash \overline{m_0} \le \overline{r}$ a $\mathsf{Q} \vdash \overline{k_0} \le \overline{r}$. Dále platí

$$\mathsf{Q} \vdash \forall z {\le} \overline{r} \forall v {\le} \overline{r} \, (\theta(\overline{n_0}, z, v) \;\to\; z = \overline{m_0}). \tag{4}$$

To plyne z (3), neboť uvnitř Q víme, že každé $z \leq \overline{r}$ i $v \leq \overline{r}$ je rovno některému z čísel $\overline{0}, \overline{1}, \ldots, \overline{r}$, viz 4.4.1(d). Uvažujme v Q:

Máme $\overline{m_0} \leq \overline{r}$. Z (2) a z $\overline{k_0} \leq \overline{r}$ plyne $\exists v{\leq}\overline{r}\,\theta(\overline{n_0}, \overline{m_0}, v)$. To dohromady s podmínkou (4) dává $\varphi(\overline{n_0}, \overline{m_0})$. Tím je ověřena implikace $\leftarrow$ v podmínce $*$.

Nechť naopak y je takové, že $\varphi(\overline{n_0}, y)$. Máme tedy w, které splňuje podmínky (i) $y \leq w$, (ii) $\exists v{\leq}w\,\theta(\overline{n_0}, y, v)$ a (iii) $\forall z{\leq}w\,\forall v{\leq}w\,(\theta(\overline{n_0}, z, v) \rightarrow z = y)$.

Platí $w \leq \overline{r}$ nebo $\overline{r} \leq w$.

Když $w \leq \overline{r}$, pak podmínka (ii) a podmínka (4) užitá na $z := y$ dávají $y = \overline{m_0}$. Přitom jsme implikaci $t \leq w \leq \overline{r} \rightarrow t \leq \overline{r}$, jejíž důkaz ponecháváme za cvičení, použili na $t := v$ a na $t := y$.

Když $\overline{r} \leq w$, pak podmínka (iii) užitá na $z := \overline{m_0}$ a $v := \overline{k_0}$ dávají $\overline{m_0} = y$. Přitom jsme implikaci $t \leq \overline{r} \leq w \rightarrow t \leq w$, jejíž důkaz také ponecháváme za cvičení, použili na $t := \overline{m_0}$ a na $t := \overline{k_0}$.

QED

Mělo by být jasné (cvičení), že splňuje-li formule $\varphi(x, y)$ podmínku $(*)$, pak φ definuje graf funkce f v $\mathbf{N}$ a všechny sentence tvaru $\exists!y\varphi(\overline{n_0}, y)$ jsou dokazatelné v Q.

Vyslovme větu o Σ-úplnosti tak, abychom zakryli, že je v ní řeč o standardním modelu Peanovy aritmetiky: když Σ-sentence σ (ve skutečnosti) platí, pak σ je dokazatelná v Q. Tato formulace naznačuje, jak máme větu o Σ-úplnosti formalizovat v aritmetickém jazyce: pomocí implikace $\sigma \rightarrow \mathsf{Pr}_{\mathsf{Q}}(\overline{\sigma})$. Platí-li $\mathsf{Q} \vdash \sigma$, pak sentence $\sigma \rightarrow \mathsf{Pr}_{\mathsf{Q}}(\overline{\sigma})$ je dokazatelná v PA (dokonce už v Q) díky tomu, že je dokazatelný její závěr $\mathsf{Pr}_{\mathsf{Q}}(\overline{\sigma})$. Platí-li $\mathsf{Q} \vdash \neg\sigma$, pak sentence $\sigma \rightarrow \mathsf{Pr}_{\mathsf{Q}}(\overline{\sigma})$ je ovšem také dokazatelná. *Věta o formalizované Σ-úplnosti* tvrdí, že implikace $\sigma \rightarrow \mathsf{Pr}_{\mathsf{Q}}(\overline{\sigma})$ je v PA dokazatelná vždy, tj. i v případech, kdy σ je nezávislá Σ-sentence.

Důkaz věty o formalizované Σ-úplnosti lze získat „přeříkáním“ důkazu věty o Σ-úplnosti, který jsme uvedli, uvnitř PA. A u toho bychom případně mohli skončit. Ale neskončíme, důkazem se budeme dost podrobně zabývat. Chceme totiž upozornit na některé potíže a na některé zajímavé aspekty. Naším cílem není podat kompletní důkaz. To by opravdu znamenalo rozsáhlé části lemmat 4.4.3–4.4.6 pouze přepsat s užitím bezpatkového písma.

Věta o Σ-úplnosti tvrdí něco pro všechny Σ-sentence σ. V důkazu se postupuje indukcí podle počtu logických spojek a kvantifikátorů v sentenci σ. Potíž s tím, že některé podformule sentencí nejsou sentence, jsme překonali tak, jak je vidět ve znění lemmat 4.4.5 a 4.4.6: indukcí podle složitosti se pro každou *formuli* dokazuje tvrzení o jejích *numerických instancích*.

Naprosto stejně postupujeme uvnitř PA při formalizaci důkazu věty o Σ-úplnosti. V PA tedy budeme mluvit o *formálních numerálech*, tj. o číslech y splňujících podmínku $\mathsf{Numeral}(x, y)$ vůči *libovolnému* číslu x. Číslo x je zde opět vhodné představit si jako (standardní nebo nestandardní) prvek nějakého modelu Peanovy aritmetiky.

Nechť ψ je nějaká aritmetická formule s jednou volnou proměnnou u. Prohlédněme si následující formuli:

$$\exists y \exists z(\mathsf{Numeral}(x,y) \,\&\, \mathsf{SubF}(\overline{u},\overline{\psi},y,z) \,\&\, \mathsf{Pr}_{\mathsf{Q}}(z)). \qquad (*)$$

Již jsme si zvykli, že formule ψ je jak syntaktický objekt, tak přirozené číslo, a nepřekvapuje nás výskyt numerálu $\overline{\psi}$ v jakékoliv formuli. Σ-úplnost spolu s 4.2.11(a) dávají $\mathsf{PA} \vdash \mathsf{Fm}(\overline{\psi})$. Uvnitř PA tedy o čísle $\overline{\psi}$ víme, že je formulí. Také proměnná u je syntaktický objekt, skládá se ze symbolu v následovaného zápisem přirozeného čísla. Uvnitř PA tedy víme také $\mathsf{Var}(\overline{u})$, neboli víme, že číslo $\overline{u}$ je proměnná. Uvnitř PA dále víme, že za $\overline{u}$ do $\overline{\psi}$ můžeme substituovat libovolný substituovatelný term, například ono y, pro které platí $\mathsf{Numeral}(x,y)$. Výsledkem takové substituce je sentence z, o které je řeč v $(*)$. Podmínku $(*)$ tedy čteme sentence vzniklá z $\overline{\psi}$ dosazením x-tého numerálu je dokazatelná v Q a z metamatematického hlediska je to formule s jednou volnou proměnnou x. Nic nebrání, aby proměnné x a u byly totožné. Mysleme si tedy, že jediná volná proměnná formule ψ je x. Pak formule

$$\exists y \exists z(\mathsf{Numeral}(x,y) \,\&\, \mathsf{SubF}(\overline{x},\overline{\psi},y,z) \,\&\, \mathsf{Pr}_{\mathsf{Q}}(z)) \qquad (**)$$

opět říká, že sentence vzniklá z $\overline{\psi}$ dosazením x-tého numerálu za jedinou volnou proměnnou je dokazatelná v Q. Ve formuli $(**)$ hraje „x“ dvojí úlohu. Z metamatematického hlediska je x proměnná volná ve formulích $(**)$ a ψ. Uvnitř PA je řeč o libovolném (standardním nebo nestandardním) přirozeném čísle x (tomu odpovídají volné výskyty proměnné x ve formuli $(**)$) a dále o syntaktickém objektu $\overline{x}$, který se objeví při syntaktické analýze formule $\overline{\psi}$.

Ztotožnění proměnných u a x značně zvyšuje nároky na představivost, ale umožňuje také následující úmluvu. Místo $(**)$ pišme

$$\mathsf{Pr}_{\mathsf{Q}}(\ulcorner \psi(\dot{x}) \urcorner).$$

Volných proměnných ve formuli ψ může být i více. Zápis

$$\mathsf{Pr}_{\mathsf{Q}}(\ulcorner \varphi(\dot{x}_1,\ldots,\dot{x}_r) \urcorner)$$

čteme sentence vzniklá dosazením x_1-tého až x_r-tého numerálu za volné proměnné formule $\overline{\varphi}$ je dokazatelná v Q a rozumí se, že formule φ nemá jiné volné proměnné než $x_1,\ldots,x_r$. Výraz $\ulcorner \varphi(\dot{x}_1,\ldots,\dot{x}_r) \urcorner$ s uvozujícími „růžky“ a s tečkami nad proměnnými tedy v aritmetickém jazyce označuje formální sentenci (číslo, které může být standardní nebo nestandardní), která vznikla z formule φ dosazením formálních numerálů. Formální numerály lze ovšem dosadit do libovolné formule. Protože ale vystačíme s dosazováním do skutečných (standardních) formulí, v zápisech tvaru $\ulcorner \ldots \varphi(\dot{x}) \ldots \urcorner$ nepíšeme pruh nad formulí, do které se dosazuje. Také v zápisech tvaru $\ulcorner \neg(\mathtt{v10{=}S(}\dot{x}\mathtt{)}) \urcorner$, v nichž jsou jednotlivé symboly vyznačeny strojopisným písmem, vynecháváme pruhy (a levé apostrofy); o tom jsme se domluvili již dříve.

Uvažujme o formalizaci jednotlivých tvrzení z věty 4.4.1. Označme α formuli $\neg(0 = \mathrm{S}(x))$ a posuďme následující úvahu uvnitř PA:

Číslo $\overline{\forall x\alpha}$ je axiomem Robinsonovy aritmetiky. Číslo $\ulcorner\overline{\forall x\alpha}\#(\overline{\forall x\alpha}\to\alpha(\dot v))\#\alpha(\dot v)\urcorner$ je tedy důkazem v Q, protože je kódem posloupnosti tvaru $\ulcorner z_1\#z_2\#z_3\urcorner$, přičemž platí $[\mathsf{Q}](z_1)$, $\mathsf{LogAx}(z_2)$ a formule z_3 je ze z_1 a z_2 odvozena pravidlem MP.

Napsali jsme důkaz formule $\mathsf{Pr}_\mathsf{Q}(\ulcorner\neg(0{=}\mathsf{S}(\dot v))\urcorner)$. Tedy

$$\mathsf{PA}\vdash\forall v\mathsf{Pr}_\mathsf{Q}(\ulcorner\neg(0{=}\mathsf{S}(\dot v))\urcorner). \tag{1}$$

Mezi mnoha „triviálními fakty o syntaktických objektech“, o kterých je řeč ve větě 4.2.11(b), by mohly být i

$$\mathsf{PA}\vdash\forall x\forall z(\mathsf{Numeral}(v+\overline{1},z)\equiv z=\ulcorner\mathsf{S}(\dot v)\urcorner), \tag{2}$$

$$\mathsf{PA}\vdash\forall z(\mathsf{Numeral}(0,z)\equiv z=\ulcorner\overline{0}\urcorner), \tag{3}$$

neboť (v PA) je jasné, že $(v+\overline{1})$-tý numerál je jediným způsobem utvořen z v-tého pomocí dvou závorek a symbolu S, a je také jasné, co je nultý numerál. Pokračujme v úvahách uvnitř PA:

Nechť $y\neq 0$. Vezměme v takové, že $v+\overline{1}=y$. Z (2) víme, že $\ulcorner\mathsf{S}(\dot v)\urcorner$ je y-tý numerál. Vzhledem k (1) je formule $\ulcorner\neg(0{=}\dot y)\urcorner$ dokazatelná v Q.

Tím jsme dospěli k mezivýsledku

$$\mathsf{PA}\vdash\forall y(0<y\to\mathsf{Pr}_\mathsf{Q}(\ulcorner\neg(0{=}\dot y)\urcorner)). \tag{4}$$

Nechť tentokrát $\alpha(z,u)$ označuje formuli $\neg(z=u)\to\neg(\mathrm{S}(z)=\mathrm{S}(u))$ a nechť dále $\beta(z)$ označuje formuli $\forall u\alpha(z,u)$ a γ označuje sentenci $\forall z\beta(z)$. Sentence γ je dokazatelná v Q. Vezměme některý její důkaz a označme jej m. V PA ovšem víme, že $\overline{m}$ je důkaz v Q sentence γ, tj. sentence $\forall z\forall u\alpha(z,u)$. Uvažujme v PA dále, a to za předpokladu $\forall y(x<y\to\mathsf{Pr}_\mathsf{Q}(\ulcorner\neg(\dot x{=}\dot y)\urcorner))$:

Nechť je dáno y takové, že $x+\overline{1}<y$. Vezměme v takové, že $v+\overline{1}=y$. Platí $x<v$. Dle předpokladu existuje w, které je důkazem sentence $\ulcorner\neg(\dot x{=}\dot v)\urcorner$. Vezměme posloupnosti $\overline{m}$, $\ulcorner(\overline{\gamma}\to\beta(\dot x))\urcorner$, $\ulcorner\beta(\dot x)\urcorner$, $\ulcorner(\beta(\dot x)\to\alpha(\dot x,\dot v))\urcorner$, $\ulcorner\alpha(\dot x,\dot v)\urcorner$, w a $\ulcorner\neg(\mathsf{S}(\dot x){=}\mathsf{S}(\dot v))\urcorner$ a spojme je do jedné užitím šesti znaků #. Dostaneme důkaz v Q sentence $\ulcorner\neg(\mathsf{S}(\dot x){=}\mathsf{S}(\dot v))\urcorner$, tj. sentence $\ulcorner\neg(\mathsf{S}(x){=}\dot y)\urcorner$.

Tím jsme provedli indukční krok. Podmínky (4) a (3) se týkají případu $x=0$. Výsledkem je $\mathsf{PA}\vdash\forall x\forall y(x<y\to\mathsf{Pr}_\mathsf{Q}(\ulcorner\neg(\dot x{=}\dot y)\urcorner))$. Z toho dále plyne

$$\mathsf{PA}\vdash\forall x\forall y(x\neq y\to\mathsf{Pr}_\mathsf{Q}(\ulcorner\neg(\dot x{=}\dot y)\urcorner)), \tag{5}$$

a tím je řečeno, že první ze tří tvrzení v 4.4.1(a) je formalizovatelné v PA. Podobnými úvahami lze dospět i k formalizaci zbývajících tvrzení v (a)–(e). Z formalizace tvrzení (b) a (c) dále plyne

$$\mathsf{PA}\vdash\forall x_1\,..\,\forall x_r\forall y(t(x_1,..,x_r)=y\to\mathsf{Pr}_\mathsf{Q}(\ulcorner t(\dot x_1,..,\dot x_r){=}\dot y\urcorner)) \tag{6}$$

pro každý aritmetický term $t(x_1,..,x_r)$. Tím jsme se přesvědčili, že lemma 4.4.3 je formalizovatelné v PA.

V dosavadním textu se obvykle pohybujeme na dvou úrovních, dokazujeme, že něco je nebo není dokazatelné. Nyní máme co dělat se třemi úrovněmi. Podmínka (6) se dokazuje metamatematickou indukcí podle složitosti termu t. Přitom se užije podmínka (5) a několik podobných podmínek. Podmínku (5) jsme dokázali indukcí v PA podle x. A všechny formule, se kterými pracujeme, mluví o dokazatelnosti v Q, kde žádnou indukci nemáme a nepoužíváme.

K dokončení důkazu věty o formalizované Σ-úplnosti se musíme ještě v PA zabývat lemmaty 4.4.5 a 4.4.6 a postupně dokázat, že

$$\mathsf{PA} \vdash \forall x_1 \,..\, \forall x_r(\varphi(x_1,..,x_r) \to \mathsf{Pr}_{\mathsf{Q}}(\ulcorner\varphi(\dot{x}_1,..,\dot{x}_r)\urcorner)) \tag{7}$$

platí pro každou Δ_0-formuli φ resp. pro každou Σ-formuli φ. Zmíníme se již pouze o univerzálním omezeném kvantifikátoru; nejprve si ale rozmyslíme ještě jedno pomocné tvrzení.

Označme $\gamma(y)$ formuli $\forall v(v \le \mathrm{S}(y) \;\to\; v \le y \;\vee\; v = \mathrm{S}(y))$. Lze ověřit, že

$$\mathsf{Q} \vdash \gamma(0), \tag{8}$$

$$\mathsf{Q} \vdash \forall y(\gamma(y) \to \gamma(\mathrm{S}(y))). \tag{9}$$

Netvrdíme $\mathsf{Q} \vdash \forall y\gamma(y)$. Ukážeme ale, že (8) a (9) stačí k důkazu, že

$$\mathsf{PA} \vdash \forall x \mathsf{Pr}_{\mathsf{Q}}(\ulcorner\gamma(\dot{x})\urcorner). \tag{10}$$

Označme $\alpha(y)$ formuli $\gamma(y) \to \gamma(\mathrm{S}(y))$ a zvolme m, které je důkazem sentence $\forall y\alpha$ v Q. Jako v důkazu podmínky (5), v PA víme $\mathsf{Proof}_{\mathsf{Q}}(\overline{\forall y\alpha}, \overline{m})$. Dokážeme podmínku (10) indukcí podle x:

Pro $x = 0$ podmínka (10) platí vzhledem k (8), protože $\ulcorner\overline{0}\urcorner$ je nultý numerál, viz (3).

Nechť podmínka (10) platí pro x. Máme tedy číslo w, které je důkazem sentence $\ulcorner\gamma(\dot{x})\urcorner$. Spojíme-li dohromady posloupnosti $\ulcorner(\overline{\forall y\alpha}\to(\gamma(\dot{x})\to\gamma(\mathrm{S}(\dot{x}))))\urcorner$, $\overline{m}$, $\ulcorner(\gamma(\dot{x})\to\gamma(\mathrm{S}(\dot{x})))\urcorner$, w a $\ulcorner\gamma(\mathrm{S}(\dot{x}))\urcorner$ užitím čtyř znaků #, dostaneme důkaz sentence $\ulcorner\gamma(\mathrm{S}(\dot{x}))\urcorner$.

Tím jsme připraveni k úvaze o omezeném kvantifikátoru. Předpokládejme, že pro formuli ψ jsme již příslušné tvrzení dokázali, a zabývejme se formulí $\forall v{\le}x\,\psi$. Je-li proměnná x mezi volnými proměnnými formule ψ, můžeme ji dočasně přejmenovat na řekněme z a pak za z dosadit x. Z tohoto důvodu lze předpokládat, že x nemá volné výskyty ve formuli ψ. Máme tedy formuli $\psi(v, y_1,..,y_r)$, pro kterou jsme již dokázali

$$\mathsf{PA} \vdash \forall v \forall \underline{y}(\psi(v,\underline{y}) \to \mathsf{Pr}_{\mathsf{Q}}(\ulcorner\psi(\dot{v},\dot{y}_1,..,\dot{y}_r)\urcorner)), \tag{11}$$

a uvažujme formuli $\forall v{\le}x\,\psi(v,\underline{y})$. Podmínku

$$\mathsf{PA} \vdash \forall x(\forall v{\le}x\,\psi(v,\underline{y}) \to \mathsf{Pr}_{\mathsf{Q}}(\ulcorner\forall v{\le}\dot{x}\,\psi(v,\dot{y}_1,..,\dot{y}_r)\urcorner)) \tag{12}$$

dokážeme opět indukcí podle x. Indukční krok vypadá takto:

Nechť $\forall v{\leq}\mathrm{S}(x)\,\psi(v,\underline{y})$. Tedy $\forall v{\leq}x\,\psi(v,\underline{y})$ a $\psi(\mathrm{S}(x),\underline{y})$. Vzhledem k indukčnímu předpokladu existuje důkaz w_1 sentence $\ulcorner\forall v{\leq}\dot{x}\psi(v,\dot{y}_1,..,\dot{y}_r)\urcorner$. Vzhledem k (11) máme důkaz w_2 sentence $\ulcorner\psi(\mathrm{S}(\dot{x}),\dot{y}_1,..,\dot{y}_r)\urcorner$. Z důkazů w_1 a w_2 a z důkazu sentence $\ulcorner\forall v\,(v{\leq}\mathsf{S}(\dot{x}){\to}v{\leq}\dot{x}\vee v{=}\mathsf{S}(\dot{x}))\urcorner$, viz (10), lze sestavit důkaz sentence $\ulcorner\forall v{\leq}\mathsf{S}(\dot{x})\psi(v,\dot{y}_1,..,\dot{y}_r)\urcorner$.

Tím máme podmínky (12) a (7), a tím *všechno*, za dokázané:

Věta 4.4.15 (formalizovaná Σ-úplnost) *Implikace $\sigma\to\mathsf{Pr}_{\mathsf{Q}}(\overline{\sigma})$ je v* PA *dokazatelná pro každou Σ-sentenci σ. Pro každou Σ-formuli $\sigma(x_1,..,x_r)$ lze v* PA *dokázat sentenci $\forall\underline{x}(\sigma(\underline{x})\to\mathsf{Pr}_{\mathsf{Q}}(\ulcorner\sigma(\dot{x}_1,..,\dot{x}_r)\urcorner))$.*

Věta 4.4.16 (podmínky pro dokazatelnost) *Nechť T je rekurzívně axiomatizovatelná teorie obsahující Robinsonovu aritmetiku a nechť $\tau(z)$ je Σ-definice množiny axiomů teorie T v* **N**. *Pak pro libovolnou aritmetickou sentenci φ resp. pro libovolné dvě aritmetické sentence φ a ψ platí*

D1: *když $T\vdash\varphi$, pak* $\mathsf{PA}\vdash\mathsf{Pr}_\tau(\overline{\varphi})$,

D2: $\mathsf{PA}\vdash\mathsf{Pr}_\tau(\overline{\varphi})\ \&\ \mathsf{Pr}_\tau(\overline{\varphi\to\psi})\to\mathsf{Pr}_\tau(\overline{\psi})$,

D3: $\mathsf{PA}\vdash\mathsf{Pr}_\tau(\overline{\varphi})\to\mathsf{Pr}_\tau(\overline{\mathsf{Pr}_\tau(\overline{\varphi})})$.

Důkaz Nechť $T\vdash\varphi$. Podle 4.2.13(a) formule $\mathsf{Pr}_\tau(x)$ definuje v **N** množinu všech dokazatelných sentencí. Platí tedy $\mathbf{N}\models\mathsf{Pr}_\tau(\overline{\varphi})$. Podle 4.3.5 sentence $\mathsf{Pr}_\tau(\overline{\varphi})$ je Σ(PA)-sentence. Σ-úplnost dává $\mathsf{Q}\vdash\mathsf{Pr}_\tau(\overline{\varphi})$, tedy i $\mathsf{PA}\vdash\mathsf{Pr}_\tau(\overline{\varphi})$.

Podmínka D2 plyne z 4.2.14(b) pouhým dosazením.

Protože $\mathsf{Pr}_\tau(\overline{\varphi})$ je Σ-sentence, platí $\mathsf{PA}\vdash\mathsf{Pr}_\tau(\overline{\varphi})\to\mathsf{Pr}_{\mathsf{Q}}(\overline{\mathsf{Pr}_\tau(\overline{\varphi})})$ díky formalizované Σ-úplnosti. Zbývá pouze zdůvodnit $\mathsf{PA}\vdash\mathsf{Pr}_{\mathsf{Q}}(\overline{\mathsf{Pr}_\tau(\overline{\varphi})})\to\mathsf{Pr}_\tau(\overline{\mathsf{Pr}_\tau(\overline{\varphi})})$. Podle 4.2.14(d) platí dokonce $\mathsf{PA}\vdash\forall x(\mathsf{Pr}_{\mathsf{Q}}(x)\to\mathsf{Pr}_\tau(x))$. Každá sentence $\mathsf{Pr}_\tau(\overline{\alpha_i})$, kde α_i je některý z axiomů Robinsonovy aritmetiky, je totiž Σ-sentence platná v **N**. QED

Z 4.2.14(b) víme, že v PA je známo, že množina všech dokazatelných formulí je uzavřena na pravidlo MP. V některých aplikacích bude stačit vědět, že to platí alespoň pro „skutečné“ sentence, tj. že platí podmínka D2. Je dobré si všimnout, že ke zdůvodnění platnosti podmínky D2 jsme opravdu potřebovali tvrzení 4.2.14(d), nevystačili bychom s tvrzeními o definovatelnosti množin a podmínek uvedených v 4.2.12 a 4.2.13. Podmínku D2 lze označit jako formalizované pravidlo modus ponens. Podmínka D3 je vlastně formalizace podmínky D1. Když je něco dokazatelné, pak je dokazatelné, že je to dokazatelné. Podmínka D1 konstatuje, že na metamatematické úrovni to platí. Podmínka D3 tvrdí, že v PA je to známo také.

Podmínky D1–D3 použijeme v příštím oddílu, v důkazu Druhé Gödelovy věty o neúplnosti. Setkáme se s nimi i v oddílu 5.3. Název *podmínky pro dokazatelnost* (anglicky *derivability conditions*) je oprávněn tím, že jde o (minimální) podmínky kladené na formuli $\mathsf{Pr}_\tau(x)$ potřebné k tomu, aby se podařil (obvyklý) důkazy Druhé

Gödelovy věty. V literatuře se lze setkat s ekvivalentní formulací podmínky D2: $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi \to \psi}) \to (\mathsf{Pr}_\tau(\overline{\varphi}) \to \mathsf{Pr}_\tau(\overline{\psi}))$.

Poslední téma tohoto oddílu je formalizovatelnost (alespoň části) sémantiky predikátové logiky v PA. Vezmeme-li do hry ještě gentzenovský kalkulus, podaří se nám odpovědět na jednu z otázek ze závěru oddílu 4.2. Zbývající část tohoto oddílu pravděpodobně nebude podstatná pro pochopení výsledků z následujících oddílů.

Úvahy o *formalizované sémantice* začněme prohlédnutím formule $\mathsf{Val}(z,e,a)$, kterou čteme číslo a je hodnota termu z při ohodnocení proměnných e:

$$\begin{aligned}
&\mathsf{Term}(z)\ \&\ \mathsf{Seq}(e)\ \&\ \exists w(\mathsf{Seq}(w)\ \&\ \mathsf{Lh}(w, z+\overline{1})\ \&\\
&\quad \&\ \forall y{\le}z(\neg\mathsf{Term}(y)\ \vee\\
&\qquad \vee\ (y = \ulcorner\overline{0}\urcorner\ \&\ \mathsf{B}(w,y,0))\\
&\qquad \vee\ (\mathsf{Var}(y)\ \&\ \exists t(\mathsf{Lh}(e,t)\ \&\ y<t\ \&\ \exists v(\mathsf{B}(e,y,v)\ \&\ \mathsf{B}(w,y,v))))\\
&\qquad \vee\ (\mathsf{Var}(y)\ \&\ \exists t(\mathsf{Lh}(e,t)\ \&\ y\ge t\ \&\ \mathsf{B}(w,y,0)))\\
&\qquad \vee\ \exists u_1\exists u_2\exists v_1\exists v_2(y = \ulcorner(u_1{+}u_2)\urcorner\ \&\ \mathsf{B}(w,u_1,v_1)\ \&\ \mathsf{B}(w,u_2,v_2)\ \&\\
&\qquad\qquad \&\ \mathsf{B}(w,y,v_1+v_2))\\
&\qquad \vee\ (\ldots \text{ podobně pro symboly „}\cdot\text{“ a „}\mathsf{S}\text{“ } \ldots))\\
&\quad \&\ \mathsf{B}(w,z,a)).
\end{aligned}$$

Stejně jako již několikrát simulujeme primitivní rekurzi pomocí posloupnosti w, která kóduje počáteční úsek příslušné funkce. Posloupnost w kóduje výpočet, který stanoví hodnotu termu z tak, že určí hodnotu všech termů menších nebo rovných z. Přitom hodnota termu $\ulcorner\overline{0}\urcorner$ je nula, hodnota termu vzniklého ze dvou jednodušších termů pomocí znaménka + je součtem příslušných hodnot atd.

Jako ohodnocení e se ve formuli Val připouštějí všechny posloupnosti přirozených čísel. To znamená, že se dopouštíme následujícího zjednodušení: nedefinujeme pojem struktury, v sémantice formalizované uvnitř PA uznáváme jen jedinou strukturu, a sice univerzum *všech* (formálních) přirozených čísel. V pátém řádku formule Val je vidět, jak jsme obešli potíž s tím, že ohodnocení proměnných má být definováno pro všechny proměnné, ale uvnitř PA máme jen *konečné* posloupnosti. Za hodnoty proměnných větších nebo rovných délce ohodnocení e pokládáme nuly.

Jako obvykle, v PA lze dokázat, že formule Val má očekávané vlastnosti.

Lemma 4.4.17 *(a) Formule* $\mathsf{Val}(z,e,a)$ *je* Δ_1 *v* PA.
(b) V PA *lze dokázat, že* při každém ohodnocení e má každý term jednoznačně určenou hodnotu a. Hodnota termu $\ulcorner\overline{0}\urcorner$ je nula při jakémkoliv ohodnocení. Je-li term z utvořen z jednodušších termů pomocí symbolu + nebo $\cdot$, pak je jeho hodnota při ohodnocení e rovna součtu resp. součinu příslušných hodnot. A podobně, vznikne-li z z jednoduššího termu pomocí symbolu S.
(c) Je-li $s(v_1,\ldots,v_r)$ *libovolný (skutečný) aritmetický term, jsou-li* $n_1,\ldots,n_r$ *a* m *přirozená čísla taková, že* $\mathbf{N} \models \overline{m} = s(\overline{n_1},\ldots,\overline{n_r})$, *a je-li* q *kód posloupnosti, která v bodech* $v_1,\ldots,v_r$ *má hodnoty* $n_1,\ldots,n_r$, *pak* $\mathsf{PA} \vdash \forall a(\mathsf{Val}(\overline{s},\overline{q},a) \equiv a = \overline{m})$.

Důkaz Formule $\mathsf{Val}(z,e,a)$ má tvar $\mathsf{Term}(z)\ \&\ \mathsf{Seq}(e)\ \&\ \exists w((..)\ \&\ \mathsf{B}(w,z,a))$ a je ekvivalentní s formulí $\mathsf{Term}(z)\ \&\ \mathsf{Seq}(e)\ \&\ \forall w((..)\to\mathsf{B}(w,z,a))$. Všechny kvantifikátory ve formuli označené závorkou s tečkami lze psát jako omezené. Tím je zdůvodněno tvrzení (a). Tvrzení (b) se dokáže jako obvykle. Tvrzení (c) plyne z (b) indukcí podle počtu symbolů v termu s. QED

Podobně jako v důkazu věty formalizované Σ-úplnosti pracujeme uvnitř PA s termy a formulemi, což jsou (formální) přirozená čísla. Opět je vhodné si je představit jako prvky libovolného (nestandardního) modelu, které mohou být standardní nebo nestandardní, skutečné nebo neskutečné. Tvrzení (c) říká, že o každém (skutečném, metamatematickém) termu PA ví, že má při každém skutečném ohodnocení jedinou hodnotu, a sice tu skutečnou.

Dále chceme v aritmetickém jazyce simulovat Tarského definici, tj. definovat, kdy je formule splněna ohodnocením proměnných. Nebudeme se pokoušet udělat to najednou pro všechny formule. Pro začátek se spokojíme s definicí pro atomické formule a pro Δ_0-formule. Formuli

$$\begin{aligned}\exists z_1\exists z_2\exists a_1\exists a_2(\mathsf{Val}(z_1,e,a_1)\ \&\ \mathsf{Val}(z_2,e,a_2)\ \&\ ((x=\ulcorner z_1{=}z_2\urcorner\ \&\ a_1=a_2)\ \vee\\ \vee\ (x=\ulcorner z_1{<}z_2\urcorner\ \&\ a_1<a_2)\ \vee\ (x=\ulcorner z_1{\le}z_2\urcorner\ \&\ a_1\le a_2)))\end{aligned}$$

označme $\mathsf{SatAt}(x,e)$ a čtěme číslo x je atomická formule a číslo e je ohodnocení proměnných, které ji splňuje. V zápisu Tarského definice pro Δ_0-formule použijeme formuli $\mathsf{FmAt}(x)$ z oddílu 4.2 a dále formuli $\mathsf{FmBdd}(x)$, která je $\Delta_1(\mathsf{PA})$ a která říká, že číslo x je omezená formule. Její konstrukci neuvádíme, není v ní žádná potíž. Teď můžeme naznačit konstrukci formule $\mathsf{SatBdd}(x,e)$ vyjadřující, že číslo x je Δ_0-formule a e je ohodnocení proměnných, které ji splňuje:

$\mathsf{FmBdd}(x)\ \&\ \mathsf{Seq}(e)\ \&\ \exists w((w$ je posloupnost délky $x+\overline{1}$, jejíž všechny členy jsou posloupnosti nul a jedniček téže délky t dostatečné vzhledem k x a $e)\ \&$

$\&\ \forall y{\le}x\forall d{\le}w\,(\neg\mathsf{Fm}(y)\ \vee$

$\vee\ (d$ není posloupnost přípustná vzhledem k x a $e)$

$\vee\ (\mathsf{FmAt}(y)\ \&\ (\mathsf{B}(w,(y,d),\overline{1})\equiv\mathsf{SatAt}(y,d)))$

$\vee\ \exists u\exists y'\exists z\exists a(y=\ulcorner\forall u{<}zy'\urcorner\ \&\ \mathsf{B}(d,z,a)\ \&$

$\&\ (\mathsf{B}(w,(y,d),\overline{1})\equiv\forall b{<}a\forall d'($když d' vznikla z d změnou hodnoty v u z a na b, pak $\mathsf{B}(w,(y',d'),\overline{1}))))$

$\vee\ (\ldots$ podobně pro ostatní omezené kvantifikátory $\ldots)$

$\vee\ \exists y_1\exists y_2(y=\ulcorner(y_1{\to}y_2)\urcorner\ \&\ (\mathsf{B}(w,(y_1,d),\overline{0})\ \vee\ \mathsf{B}(w,(y_2,d),\overline{1})))$

$\vee\ (\ldots$ podobně pro ostatní logické spojky $\ldots))$

$\&\ \mathsf{B}(w,(x,e),\overline{1})).$

Tento semiformální zápis je pokusem o kompromis mezi přesností a přehledností. Číslo w je posloupnost posloupností a je užitečné představit si je jako tabulku nul

a jedniček s $x + \overline{1}$ řádky a t sloupci. Řádky odpovídají formulím nepřevyšujícím x a sloupce ohodnocením proměnných menším než t. Zápis $\mathsf{B}(w, (y, d), \overline{1})$ je zkratka pro $\exists v(\mathsf{B}(w, y, v) \,\&\, \mathsf{B}(v, d, \overline{1}))$ nebo pro $\forall v(\mathsf{B}(w, y, v) \to \mathsf{B}(v, d, \overline{1}))$ a lze jej číst hodnota v řádku y a sloupci d tabulky w je ANO. Závorky ve výrazu (y, d) tedy tentokrát neoznačují párovací funkci. Dále posloupnost d' je posloupnost vzniklá z d změnou hodnoty v u z a na b, jestliže členy posloupnosti d' s indexy menšími než $\min\{l, u\}$, kde l je délka posloupnosti d, se shodují s členy posloupnosti d, pak následuje $u - l$ nulových členů v případě, kdy $u \geq l$, pak člen b a nakonec $l - u - \overline{1}$ posledních členů posloupnosti d v případě, kdy $l > u$. Lze ověřit, že právě zapsaná podmínka začínající slovy „členy s indexy...“ je Δ_1 v PA.

Jako obvykle je posloupnost w ve formuli $\mathsf{SatBdd}(x, e)$ záznamem výpočtu, který určí pravdivostní hodnotu formule x při ohodnocení e. Vedlejším produktem výpočtu je určení pravdivostních hodnot všech formulí $y \leq x$ při všech ohodnoceních proměnných d přípustných vzhledem k x a e. Je-li formule y sestavena z jednodušších formulí y_1 a y_2 pomocí některé logické spojky, výpočet se odvolává na pravdivostní hodnoty formulí y_1 a y_2 při tomtéž ohodnocení, a ty jsou umístěny v tomtéž sloupci tabulky w v dřívějších řádcích příslušných k y_1 a y_2. Složitější situace nastane, je-li y utvořena z jednodušší formule y' pomocí omezené kvantifikace. V tom případě se výpočet odvolává na pravdivostní hodnoty formule y' při ohodnoceních d', o kterých byla řeč v předchozím odstavci. Tyto pravdivostní hodnoty jsou umístěny v dřívějším řádku příslušném k formuli y'.

Tím jsme se dostali k vysvětlení obratu posloupnost d je vzhledem k x a e přípustná a obratu číslo t je dostatečně velké vzhledem k x a e. Posloupnost d pokládejme za *přípustnou* vzhledem k x a e, jestliže e má nenulovou délku, délka posloupnosti d je nejvýše $\max\{x+\overline{1}, \text{délka } e\}$ a žádný její člen nepřevyšuje maximální člen posloupnosti e. Předpokládejme, že d je posloupnost přípustná vzhledem k x a e a dále že $y \leq x$ je formule tvaru $\ulcorner \forall u{<}zy' \urcorner$ a d má v bodě z hodnotu a. Změníme-li v posloupnosti d hodnotu v bodě u na novou hodnotu b, kde $b < a$, dostaneme posloupnost, jejíž délka je nejvýše $\max\{u + \overline{1}, \text{délka } d\} \leq \max\{x + \overline{1}, \text{délka } e\}$ (neboť pro čísla u a y platí $u < y$) a jejíž členy nepřevyšují maximální člen posloupnosti d, tj. ani maximální člen posloupnosti e. Jinými slovy, utvoříme-li z posloupnosti d přípustné vzhledem k x a e posloupnost d' tak, jak je řečeno ve formuli SatBdd, dostaneme opět posloupnost přípustnou vzhledem k x a e. Číslo t je *dostatečně velké* vzhledem k x a e, jestliže je větší než všechny posloupnosti přípustné vzhledem k x a e. Pro jistotu dodejme, že netvrdíme, že všechny posloupnosti d menší než t jsou přípustné: nějaká posloupnost s malým číselným kódem může mít nepřípustně velké členy nebo i délku.

Formuli SatBdd říkejme *definice pravdy pro* Δ_0*-formule*. Mohli bychom nyní vyslovit její vlastnosti. Místo toho nejprve zkonstruujeme definice pravdy pro další třídy formulí. Vlastnosti pak vyslovíme najednou.

Nechť Γ je množina aritmetických formulí. Označme $\Delta_0(\Gamma)$ množinu všech formulí utvořených z formulí v Γ pomocí logických spojek a omezených kvantifikátorů. Označme $\exists\Gamma$ množinu všech formulí utvořených z formulí v Γ pomocí jednoho existenčního kvantifikátoru. Analogicky $\forall\Gamma$ je množina všech formulí tvaru $\forall v\varphi$,

kde $\varphi \in \Gamma$. Označuje-li FmAt (jako v oddílu 3.6) množinu všech atomických aritmetických formulí, pak $\Gamma \subseteq \Delta_0(\Gamma)$, $\Delta_0(\mathrm{FmAt}) = \Delta_0(\Delta_0) = \Delta_0$ a $\exists\Delta_0 = \Sigma_1$. Dále definujme modifikace Σ_n^+ a Π_n^+ množin Σ_n a Π_n:

$$\begin{aligned}\Sigma_0^+ &= \Pi_0^+ = \mathrm{FmAt},\\ \Sigma_{n+1}^+ &= \Delta_0(\Sigma_n^+ \cup \Pi_n^+) \cup \exists\Delta_0(\Sigma_n^+ \cup \Pi_n^+),\\ \Pi_{n+1}^+ &= \Delta_0(\Sigma_n^+ \cup \Pi_n^+) \cup \forall\Delta_0(\Sigma_n^+ \cup \Pi_n^+).\end{aligned}$$

Tedy Σ_{n+1}^+-formule (Π_{n+1}^+-formule) jsou všechny formule, které jsou ze Σ_n^+- a Π_n^+-formulí utvořeny pomocí logických spojek a omezených kvantifikátorů plus případně jednoho existenčního (resp. univerzálního) kvantifikátoru.

Příklad 4.4.18 Nechť $\alpha(x,y)$ a $\beta(v)$ jsou Δ_0-formule. Pak formule $\forall x\forall y\alpha(x,y)$ a $\forall x\forall y\alpha(x,y) \to \exists v\beta(v)$ nejsou v žádné z množin Σ_n ani Π_n (protože formule v Σ_n i v Π_n musí začínat střídajícími se neomezenými kvantifikátory). První z nich je v Π_2^+, druhá je v $\Delta_0(\Pi_2^+)$.

Pro $n \geq 1$ platí $\Sigma_n \subseteq \Sigma_n^+ \subseteq \Sigma_n(\mathsf{PA})$ a $\Pi_n \subseteq \Pi_n^+ \subseteq \Pi_n(\mathsf{PA})$. Každá aritmetická formule patří do některé z množin Σ_n^+ či Π_n^+, a to je důvod, proč množiny Σ_n^+ a Π_n^+ zavádíme.

Všechny právě definované množiny formulí lze definovat i uvnitř PA. Formuli FmAt jsme již použili. Nechť $\mathsf{FmBdd}_n(x)$ je aritmetická formule, která vyjadřuje, že číslo x je formule v $\Delta_0(\Sigma_n^+ \cup \Pi_n^+)$, a nechť $\mathsf{Fm}_n(x)$ vyjadřuje, že číslo x je formule v Σ_n^+. Předpokládáme, že čtenář si dovede konstrukci formulí $\mathsf{FmBdd}_n(x)$ a $\mathsf{Fm}_n(x)$ představit a dovede také vyslovit jejich vlastnosti. Všechny jsou Δ_1 v PA. Formule FmBdd_0 je totožná s dříve užívanou formulí FmBdd. Bez formalizované definice Π_n^+-formulí se obejdeme.

Dále definujme pro každé n formuli $\mathsf{SatBdd}_n(x,e)$, která je definicí pravdy pro formule v $\Delta_0(\Sigma_n^+ \cup \Pi_n^+)$. Postupujme rekurzí podle n. SatBdd_0 je formule SatBdd. SatBdd_{n+1} je formule, která vznikne z formule $\mathsf{SatBdd}_n(x,e)$ nahrazením podformule FmBdd_n v prvním řádku formulí FmBdd_{n+1} a dále nahrazením pátého řádku, začínajícího „$\vee\,(\mathsf{FmAt}(y)$“, následujícími třemi novými řádky:

$$\begin{aligned}&\vee\ (\mathsf{FmBdd}_n(y)\ \&\ (\mathsf{B}(w,(y,d),\overline{1}) \equiv \mathsf{SatBdd}_n(y,d))),\\ &\vee\ \exists u(y = \ulcorner\exists uy'\urcorner\ \&\ (\mathsf{B}(w,(y,d),\overline{1}) \equiv \exists b\mathsf{SatBdd}_n(y', d(u/b)))),\\ &\vee\ \exists u(y = \ulcorner\forall uy'\urcorner\ \&\ (\mathsf{B}(w,(y,d),\overline{1}) \equiv \forall b\mathsf{SatBdd}_n(y', d(u/b)))).\end{aligned}$$

Formule SatBdd_{n+1} je utvořena z formule SatBdd_n zhruba stejně, jako byla formule SatBdd utvořena z formule SatAt. Formuli $\mathsf{SatBdd}_{n+1}(x,e)$ si můžeme představit jako „program“, který pracuje následovně. Nejprve zjistí syntaktickou složitost vstupu x a ověří, že je to formule v $\Delta_0(\Sigma_{n+1}^+ \cup \Pi_{n+1}^+)$. Pokud ano, stanoví číslo t dostatečně velké vzhledem k x a e a připraví si tabulku w s $x + \overline{1}$ řádky a t sloupci. V této tabulce nejprve vyplní pravdivostní hodnoty v řádcích, které příslušejí k formulím tvaru y', $\ulcorner\exists uy'\urcorner$ a $\ulcorner\forall uy'\urcorner$, kde $y' \in \Sigma_n^+ \cup \Pi_n^+$, a to tak, jak popsáno

v nových třech řádcích, s pomocí dříve sestrojeného „podprogramu“ SatBdd_n. Pak vyplní ostatní řádky příslušné k formulím vzniklým z formulí v $\Sigma^+_{n+1} \cup \Pi^+_{n+1}$ pomocí logických spojek a omezené kvantifikace.

V zápisu formule SatBdd_n jsme si dovolili další zkrácený zápis: $d(u/b)$ označuje ono ohodnocení, o kterém byla řeč v komentáři ke konstrukci formule SatBdd a které vzniklo z d změnou hodnoty v u na b. V následujícím lemmatu navíc $e(z)$ označuje hodnotu, kterou ohodnocení d přiřazuje proměnné z.

Lemma 4.4.19 *(a) Formule* SatBdd_n *je v* $\Delta_{n+1}(\mathsf{PA})$.

(b) $\mathsf{PA} \vdash \forall x \forall e(\mathsf{FmBdd}_m(x) \to (\mathsf{SatBdd}_m(x,e) \equiv \mathsf{SatBdd}_n(x,e)))$ *pro každou dvojici čísel* m *a* n *takových, že* $m \leq n$.

(c) V PA *lze dokázat sentence*

$$\forall x \forall y_1 \forall y_2 \forall e(\mathsf{FmBdd}_n(x) \;\&\; x = \ulcorner (y_1 \& y_2) \urcorner \to (\mathsf{SatBdd}_n(x,e) \equiv \equiv \mathsf{SatBdd}_n(y_1,e) \;\&\; \mathsf{SatBdd}_n(y_2,e))),$$

$$\forall x \forall y \forall e(\mathsf{FmBdd}_n(x) \;\&\; x = \ulcorner \neg y \urcorner \to (\mathsf{SatBdd}_n(x,e) \equiv \neg \mathsf{SatBdd}_n(y,e))),$$

$$\forall x \forall y \forall u \forall e(\mathsf{FmBdd}_n(x) \;\&\; x = \ulcorner \exists u y \urcorner \to (\mathsf{SatBdd}_n(x,e) \equiv \exists b \mathsf{SatBdd}_n(y, e(u/b)))),$$

$$\forall x \forall y \forall z \forall u \forall e(\mathsf{FmBdd}_n(x) \;\&\; x = \ulcorner \forall u {\leq} z y \urcorner \to (\mathsf{SatBdd}_n(x,e) \equiv \equiv \forall b {\leq} e(z)\, \mathsf{SatBdd}_n(y, e(u/b)))),$$

a také analogické sentence týkající se ostatních spojek a ostatních kvantifikátorů.

(d) $\mathsf{PA} \vdash \forall x \forall y \forall u(\mathsf{FmBdd}_n(x) \;\&\; x = \ulcorner \forall u y \urcorner \;\&\; \forall e \mathsf{SatBdd}_n(y,e) \to \to \forall e \mathsf{SatBdd}_n(x,e))$.

(e) $\mathsf{PA} \vdash \forall x \forall e \forall d(\mathsf{FmBdd}_n(x) \;\&\; \forall v(\mathsf{OccF}(u,x) \to d(v) = e(v)) \to \to (\mathsf{SatBdd}_n(x,d) \equiv \mathsf{SatBdd}_n(x,e)))$.

(f) $\mathsf{PA} \vdash \forall x \forall e(\mathsf{FmBdd}_n(x) \;\&\; \mathsf{LogAx}(x) \to \mathsf{SatBdd}_n(x,e))$.

Důkaz Všechna tvrzení se dokazují metamatematickou indukcí podle n. Číslu w, o kterém je řeč ve formuli $\mathsf{SatBdd}_n(x,e)$ a které je posloupností délky $x+1$, jejíž všechny členy jsou posloupnosti délky t dostatečné vzhledem k x a e, říkejme *pravdivostní relace pro* x, e *a* t (a pro formule splňující $\mathsf{FmBdd}_n(x)$, tj. pro formule v $\Delta_0(\Sigma^+_n \cup \Pi^+_n)$). V PA lze dokázat, že je-li t dostatečně velké vzhledem k x a e, pak pro x, e a t existuje pravdivostní relace. A navíc, její hodnoty pro dvojice (y,d), kde $\mathsf{FmBdd}_n(y)$ a d je ohodnocení přípustné vzhledem k x a e, jsou jednoznačně určeny. V důkazu tvrzení (b)–(d) lze pokračovat ve stejném duchu, jako jsme to udělali již vícekrát, celkem podrobně například v důkazu tvrzení 4.2.10 (c) a (d).

V důkazech tvrzení (e) a (f) se v PA postupuje stejně jako ve skutečnosti. Tvrzení (e) je formalizací důkazu lemmatu 3.1.11. V (f) je nejsložitější ten případ, kdy x je axiom tvaru B1 nebo B2. Postupuje se stejně jako v lemmatech 3.1.14 a 3.1.20.

Podívejme se ještě na tvrzení (a). Je-li SatBdd_n v $\Delta_{n+1}(\mathsf{PA})$, pak podformule formule SatBdd_{n+1}, které začínají kvantifikátory „$\exists b$“ a „$\forall b$“, jsou v $\Sigma_{n+1}(\mathsf{PA})$

resp. v $\Pi_{n+1}(\mathsf{PA})$. Obě podformule jsou tedy v $\Delta_{n+2}(\mathsf{PA})$. Celá formule SatBdd_{n+1} je z těchto podformulí utvořena pomocí logických spojek, kvantifikátorů, které lze omezit, a pomocí kvantifikátoru „$\exists w$“, o kterém bylo před chvílí zdůrazněno, že je „obojetný“: celá formule $\mathsf{SatBdd}_{n+1}(x,e)$ by se dala ekvivalentně psát ve tvaru

$$\mathsf{FmBdd}_{n+1}(x)\ \&\ \mathsf{Seq}(e)\ \&\ \forall w(\text{když } t \text{ je dostatečně velké vzhledem k } x \text{ a } e \text{ a když } w \text{ je pravdivostní relace pro } x,\ e \text{ a } t, \text{ pak } \mathsf{B}(w,(x,e),\overline{1})).$$

Tím je ověřeno, že formule SatBdd_{n+1} je Δ_{n+2} v PA za předpokladu, že formule SatBdd_n je Δ_{n+1} v PA. Formule SatBdd_0 je utvořena z $\Delta_1(\mathsf{PA})$-formulí pomocí logických spojek, kvantifikátorů, které lze omezit, a jednoho obojetného kvantifikátoru, a je tedy Δ_1 v PA. QED

Z definice pravdy pro $\Delta_0(\Sigma_n^+ \cup \Pi_n^+)$-formule nyní utvoříme formuli $\mathsf{Sat}_n(x,e)$, která je definicí pravdy pro Σ_n^+-formule. Formuli Sat_n budeme v další práci upřednostňovat před formulí SatBdd_n. Množinu Σ_n^+ totiž považujeme za přirozenější než množinu $\Delta_0(\Sigma_n^+ \cup \Pi_n^+)$. Líbí se nám také to, že syntaktická složitost formule $\mathsf{Sat}_n(x,e)$ pro $n \geq 1$ vyjde jen $\Sigma_n(\mathsf{PA})$. Pravdivostí Π_n^+-formulí se nezabýváme, protože to není třeba. Šlo by to ale snadno a také by to dopadlo příznivě: Π_n^+-formule mají definici pravdy, která je $\Pi_n(\mathsf{PA})$. Definujme tedy formule $\mathsf{Sat}_n(x,e)$ a $\mathsf{Tr}_n(x)$ pro $n \geq 1$:

$$\begin{aligned}\mathsf{Sat}_n(x,e) &\equiv \mathsf{SatBdd}_{n-1}(x,e) \vee \exists y \exists u(x = \ulcorner \exists u y \urcorner\ \&\ \exists b \mathsf{SatBdd}_{n-1}(y, e(u/b))),\\ \mathsf{Tr}_n(x) &\equiv \mathsf{Sent}_n(x)\ \&\ \exists e \mathsf{Sat}_n(x,e).\end{aligned}$$

Formule $\mathsf{Tr}_n(x)$ říká číslo x je pravdivá Σ_n^+-sentence. Formule $\mathsf{Sent}_n(x)$ je ovšem definována jako konjunkce $\mathsf{Sent}(x)\ \&\ \mathsf{Fm}_n(x)$. Víme ze 4.4.19, že sentence je splněna některým ohodnocením, právě když je splněna každým ohodnocením. Je tedy jedno, zda ve formuli $\mathsf{Tr}_n(x)$ stojí „$\exists e$“ nebo „$\forall e$“. Kvantifikátoru „$\exists e$“ jsme dali přednost proto, abychom nezvyšovali složitost formule.

Lemma 4.4.20 *(a) Pro $n \geq 1$, formule Sat_n a Tr_n jsou Σ_n v PA.*

(b)–(f) Všechna tvrzení (b)–(f) lemmatu 4.4.19 platí pro $n \geq 1$, nahradíme-li v nich formuli SatBdd_n formulí Sat_n.

(g) Nechť $n \geq 1$, nechť $\varphi(x_1,\ldots,x_r)$ je Σ_n^+-formule, $k_1,\ldots,k_r$ jsou přirozená čísla a nechť q je posloupnost, jejíž hodnoty v $x_1,\ldots,x_r$ jsou $k_1,\ldots,k_r$. Pak v PA lze dokázat sentenci $\varphi(\overline{k_1},\ldots,\overline{k_r}) \equiv \mathsf{Sat}_n(\overline{\varphi},\overline{q})$.

(h) Je-li $\varphi \in \Sigma_n^+$ a φ je sentence, pak $\mathsf{PA} \vdash \varphi \equiv \mathsf{Tr}_n(\overline{\varphi})$.

Důkaz Formule Sat_n je utvořena z formule SatBdd_{n-1}, která je Δ_n v PA, tedy Σ_n v PA, a to pomocí konjunkce, disjunkce a existenční kvantifikace. Z tvrzení (c) a (d) lemmatu 4.3.4 plyne (a).

Všechna tvrzení (b)–(f) plynou z definice formulí Sat_n a z příslušných tvrzení lemmatu 4.4.19. Tvrzení (c) lze dokázat indukcí podle složitosti formule φ. Je-li φ

atomická, uplatní se 4.4.17(c). V ostatních případech se použijí tvrzení o logických spojkách a kvantifikátorech uvedená v (b). Tvrzení (h) plyne okamžitě z (g) volbou $r = 0$. QED

Tvrzení (h) (případně též tvrzení (g)) se někdy nazývá *dekvotační schéma* (anglicky *dequotation scheme*). Mnozí je také znají a citují jako „lemma sněží-sněží“, protože vyjadřuje tento fakt: sentence „sněží“ je pravdivá, právě když sněží. Na dekvotačním schématu je důležité, že podobně jako věta o formalizované Σ-úplnosti platí pro *všechny* sentence bez ohledu na to, jsou-li dokazatelné, vyvratitelné nebo nezávislé.

Definujme v PA *důkazy omezené složitosti*. Nechť $\tau(z)$ je formule a nechť m je přirozené číslo. Definujme formule $\mathsf{Proof}_{m,\tau}(x,w)$ a $\mathsf{Pr}_{m,\tau}(x)$:

$$\begin{aligned}\mathsf{Proof}_{m,\tau}(x,w) &\equiv \mathsf{Proof}_{\tau}(x,w)\ \&\ \forall w_1 \forall z(\mathsf{Beg}(w_1,w)\ \&\ \mathsf{Ends}(w_1,z) \to \mathsf{Fm}_m(z)),\\ \mathsf{Pr}_{m,\tau}(x) &\equiv \exists w \mathsf{Proof}_{m,\tau}(x,w).\end{aligned}$$

Formule $\mathsf{Pr}_{m,\tau}(x)$ tedy říká, že formuli x lze dokázat důkazem, v němž všechny formule jsou v Σ^+_m. Je-li x dokazatelná takovým důkazem, pak ovšem x sama musí být v Σ^+_m, tj. musí o ní platit $\mathsf{Fm}_m(x)$. Je-li τ v $\Delta_1(\mathsf{PA})$, pak formule $\mathsf{Proof}_{m,\tau}$ je v $\Delta_1(\mathsf{PA})$, protože kvantifikátory „$\forall w_1 \forall z$“ lze psát jako omezené. Je-li τ v $\Sigma_1(\mathsf{PA})$, pak formule $\mathsf{Proof}_{m,\tau}$ a $\mathsf{Pr}_{m,\tau}$ jsou v $\Sigma_1(\mathsf{PA})$.

Od oddílu 4.2 pracujeme s formalizovanou definicí důkazu, pro kterou jsme si vybrali hilbertovský kalkulus HK. Stejně dobře lze ale v PA formalizovat i gentzenovský kalkulus GK. Znamená to k seznamu symbolů potřebných k zapisování důkazů přidat tři symboly „$\langle$“, „$\rangle$“ a „$\Rightarrow$“ pro zapisování sekventů. Řekněme, že tam, kde bychom chtěli zdůraznit, že jde o symboly, zejména ve výrazech tvaru $\ulcorner(..)\urcorner$, bychom užívali jejich strojopisné verze `[`, `]` a `=>`. Všechna tvrzení kapitoly 3 o gentzenovském kalkulu GK, která mají ryze syntaktický důkaz, lze formalizovat v PA. Budeme potřebovat větu o eliminovatelnosti řezů, tvrzení o vzájemné simulovatelnosti kalkulů HK a GK a větu 3.3.4.

Věta 4.4.21 *Nechť F je konečná množina aritmetických sentencí, nechť φ je aritmetická sentence. Pak existuje číslo m takové, že* $\mathsf{PA} \vdash \mathsf{Pr}_F(\overline{\varphi}) \to \mathsf{Pr}_{m,F}(\overline{\varphi})$.

Důkaz Máme množinu sentencí F a sentenci φ. Vezměme číslo m_0 tak velké, že φ i všechny sentence v F jsou v $\Sigma^+_{m_0}$. Protože pracujeme s aritmetickým jazykem, množina axiomů rovnosti má osm prvků (axiomy E1–E3, tři instance axiomu E4 a dvě instance axiomu E5). Označme tuto množinu E. Lze ověřit, že všechny prvky množiny E jsou sentence v Π^+_4, tedy v Σ^+_5. Označme $\mathcal{S}$ sekvent $\langle F, E \Rightarrow \varphi \rangle$. Všechny formule sekventu $\mathcal{S}$ jsou v $\Sigma^+_{\max\{5,m_0\}}$. Položme $m_1 = \max\{5, m_0\}$. Tvrdíme, že číslo $m = 1 + m_1$ vyhovuje, protože:

> Nechť sentence $\overline{\varphi}$ je v kalkulu HK dokazatelná z množiny předpokladů $\overline{F}$. Pak sekvent $\overline{\mathcal{S}}$ je dokazatelný v kalkulu GK. Podle věty 3.3.13 o eliminovatelnosti řezů má sekvent $\overline{\mathcal{S}}$ i bezřezový důkaz w_1. Podle věty 3.3.4 každá formule v důkazu w_1 je s-podformulí některé formule sekventu $\overline{\mathcal{S}}$. Je jasné, že je-li formule z

s-podformulí formule y a je-li $\mathsf{Fm}_{m_1}(y)$, pak $\mathsf{Fm}_{m_1}(z)$. Z toho plyne, že pro každou formuli z v důkazu w_1 platí $\mathsf{Fm}_{m_1}(z)$. Podle věty o simulovatelnosti kalkulu GK kalkulem HK, viz 3.3.2, má sentence $\overline{\varphi}$ důkaz w_2 z množiny předpokladů $\overline{F} \cup \overline{E}$ v kalkulu HK, tj. důkaz w_2 z množiny předpokladů $\overline{F}$ v kalkulu HK_e. Prohlédnutím konstrukce důkazu w_2 v důkazu věty 3.3.2 lze ověřit, že důkaz w_2 obsahuje pouze formule utvořené z formulí v důkazu w_1 pomocí logických spojek. Všechny takové formule z splňují podmínku $\mathsf{Fm}_m(z)$.

QED

Věta 4.4.22 *(a) Nechť F je konečná množina aritmetických sentencí. Pak implikace $\bigwedge F \to \mathsf{Con}(F)$ je dokazatelná v* PA.
(b) Nechť F je konečná množina axiomů Peanovy aritmetiky. Pak $\mathsf{PA} \vdash \mathsf{Con}(F)$.

Důkaz Nechť $F = \{\psi_1, \ldots, \psi_k\}$ je dána. Vzpomeňme si, jak je sentence $\mathsf{Con}(F)$ definována pomocí formule Pr_F, a užijme předchozí větu na množinu F a na sentenci $\varphi := (0 = \mathrm{S}(0))$: pro jisté m platí $\mathsf{PA} \vdash \neg\mathsf{Con}(F) \to \mathsf{Pr}_{m,F}(\overline{0 = \mathrm{S}(0)})$. Zbývá zdůvodnit $\mathsf{PA} \vdash \bigwedge F \to \neg\mathsf{Pr}_{m,F}(\overline{0 = \mathrm{S}(0)})$:

Dokazujme sporem. Nechť ψ_1, ψ_2, .. a ψ_k. Nechť zároveň existuje číslo w tvaru $\ulcorner x_1 \# x_2 \# \ldots \# x_t \urcorner$ takové, že pro každé l, kde $1 \leq l \leq t$, platí $\mathsf{Fm}_m(x_l)$, a w je důkaz sentence $\overline{0 = \mathrm{S}(0)}$ z množiny předpokladů $\overline{F}$. Ověříme indukcí podle l, že $\forall e \mathsf{Sat}_m(x_l, e)$. Je-li x_l jeden z předpokladů, tj. jedna ze sentencí $\overline{\psi_1}, \ldots, \overline{\psi_k}$, pak $\exists e \mathsf{Sat}_m(x_l, e)$ dle 4.4.20(h), a také $\forall e \mathsf{Sat}_m(x_l, e)$ dle 4.4.20(e). Je-li x_l logický axiom, uplatní se 4.4.20(f). A je-li x_l odvozena z předchozích členů pomocí pravidel generalizace nebo pomocí pravidla MP, uplatní se tvrzení z 4.4.20(b) týkající se kvantifikátorů a implikace.

Tím jsme dospěli ke sporu. Sentence $\overline{0 = \mathrm{S}(0)}$ je jednou z formulí x_l, a platí o ní tedy $\forall e \mathsf{Sat}_m(\overline{0 = \mathrm{S}(0)}, e)$. Díky 4.4.20(h) o ní platí také $\neg\forall e \mathsf{Sat}_m(\overline{0 = \mathrm{S}(0)}, e)$.

Tvrzení (b) plyne bezprostředně z (a): obsahuje-li F pouze axiomy Peanovy aritmetiky, pak $\mathsf{PA} \vdash \bigwedge F$. QED

Věta 4.4.22 dává odpověď na jednu z otázek ze závěru oddílu 4.2. Jedna z konečných množin F axiomů Peanovy aritmetiky je Q, a platí tedy $\mathsf{PA} \vdash \mathsf{Con}(\mathsf{Q})$.

Tomu, abychom mohli tvrdit $\mathsf{PA} \vdash \mathsf{Con}(\pi)$, brání rozdíl mezi obraty „pro každou F, která je konečná, PA ví, že ...“ a „PA ví, že pro každou konečnou F ...“. Kdybychom měli (jeden) důkaz tvrzení, že každá konečná část množiny $\{\, z \,;\, \pi(z) \,\}$ je bezesporná, znamenalo by to i důkaz bezespornosti celé množiny $\{\, z \,;\, \pi(z) \,\}$. Takový důkaz ale (zatím?) nemáme. Máme pouze nekonečně mnoho různých důkazů různých formulí tvaru $\mathsf{Con}(F)$ a není zřejmé, jak z nich utvořit společný důkaz tvrzení, že každá konečná část množiny $\{\, z \,;\, \pi(z) \,\}$ je bezesporná.

Pomohlo by, kdybychom místo dílčích definicí pravdy Sat_n mohli sestrojit jednu společnou (*uniformní*) *definici pravdy* pro všechny aritmetické formule najednou. Fakt, že aritmetická klasifikace formulí Sat_n (na rozdíl od formulí Fm_n) vzrůstá se vzrůstajícím n, ale naznačuje, že to možná nepůjde.

Konstatujme, že sentence $\mathsf{Con}(\pi)$, přes dílčí úspěchy v dokazování bezespornosti, zůstává kandidátem na konkrétní tvrzení, které je nezávislé na PA.

Cvičení

1. Dokažte v Q sentence $\forall x \forall y(x \leq y \leq \overline{n} \rightarrow x \leq \overline{n})$, $\forall x \forall y(x \leq \overline{n} \leq y \rightarrow x \leq y)$ a $\forall x(\mathrm{S}(x) + \overline{n} = x + \overline{n+1})$.

2. Dokažte, že sentence $\forall x(\mathrm{S}(x) + 0 = x + \overline{1})$ a $\forall x \exists v(0 + v = x)$ nejsou v Q dokazatelné. To znamená, že tvrzení (e) věty 4.4.1 by neplatilo, kdybychom v axiomu Q8 zaměnili pořadí sčítanců.

3. Dokažte, že (a)–(d) ve větě 4.4.1 by bylo možno dokázat i v případě, kdybychom v axiomech Q8 a Q9 zaměnili pořadí sčítanců.

4. Dokažte, že každá Σ-korektní teorie je bezesporná.

5. Rozhodněte, zda platí
   (a) Jsou-li φ a ψ aritmetické sentence takové, že $\mathsf{PA} \vdash \varphi \vee \psi$, pak platí $\mathsf{PA} \vdash \varphi$ nebo $\mathsf{PA} \vdash \psi$.
   (b) Jsou-li φ a ψ aritmetické Σ-sentence takové, že $\mathsf{PA} \vdash \varphi \vee \psi$, pak platí $\mathsf{PA} \vdash \varphi$ nebo $\mathsf{PA} \vdash \psi$.

   Návod k (b). Použijte Σ-korektnost na disjunkci $\varphi \vee \psi$ a Σ-úplnost zvlášť na φ a na ψ.

6. Rozhodněte, zda platí
   (a) Je-li $\exists x \varphi(x)$ aritmetická sentence taková, že $\mathsf{PA} \vdash \exists x \varphi(x)$, pak existuje číslo n takové, že $\mathsf{PA} \vdash \varphi(\overline{n})$.
   (b) Je-li $\exists x \varphi(x)$ aritmetická sentence taková, že φ je omezená a $\mathsf{PA} \vdash \exists x \varphi(x)$, pak existuje číslo n takové, že $\mathsf{PA} \vdash \varphi(\overline{n})$.

   Návod. V případě (a) vezměte omezenou formuli $\psi(y)$ splňující podmínky $\mathbf{N} \models \forall y \psi(y)$ a $\mathsf{PA} \nvdash \forall y \psi(y)$. Existenci takové sentence zaručuje věta 4.3.12. Dále uvažujte sentenci $\exists x \forall y(\psi(y) \vee \neg \psi(x))$.

7. Dokažte, že množina všech logicky platných formulí v jazyce aritmetiky je Σ_1-kompletní.

8. Dokažte, že splňuje-li Σ_1-formule $\varphi(x, y)$ podmínku $(*)$ z věty 4.4.14, pak φ definuje v $\mathbf{N}$ graf funkce f a všechny sentence tvaru $\exists y \varphi(\overline{n}, y)$ jsou v Q dokazatelné.

9. Vyvoďte z lemmatu 4.4.10, že ke každé rekurzívní množině $A \subseteq \mathrm{N}$ existuje formule $\varphi(x) \in \Sigma_1$ taková, že $\mathsf{Q} \vdash \varphi(\overline{n})$ pro všechna $n \in A$ a $\mathsf{Q} \vdash \neg \varphi(\overline{n})$ pro všechna $n \notin A$.

10. Vyvoďte totéž tvrzení z věty 4.4.14.

11. Dokažte, že splňuje-li teorie T předpoklady Rosserovy věty 4.4.11, pak každá z množin $\Sigma_1 \cap \mathrm{Thm}(T)$ i $\Pi_1 \cap \mathrm{Thm}(T)$ je Σ_1-kompletní.

12. Zdůvodněte, že relace $\{\, [\varphi, e]\,;\, \varphi \in \Delta_0 \ \&\ \mathbf{N} \models \varphi[e]\,\}$ je *PR*. Z toho plyne, že i relace $\{\, [\varphi(x), n]\,;\, \varphi(x) \in \Delta_0 \ \&\ \mathbf{N} \models \varphi(\overline{n})\,\}$ je *PR*. Jinými slovy, úloha rozhodnout, zda daná formule je Δ_0-formulí s jednou volnou proměnnou, která je v $\mathbf{N}$ splněna daným číslem n, je primitivně rekurzívní. Zdůvodněte dále, že množina $\{\, \varphi(x)\,;\, \varphi(x) \in \Delta_0 \ \&\ \mathbf{N} \not\models \varphi(\overline{\varphi})\,\}$ je příklad množiny, která je primitivně rekurzívní, není ale Δ_0-definovatelná.

    Návod. Analyzujte konstrukci formule SatBdd a důkaz lemmatu 4.4.19. Podmínka „φ je Δ_0-formule a e je ohodnocení proměnných takové, že (některá nebo každá) pravdivostní relace m pro φ, e a k, kde k je dost velké vzhledem k φ a e, přiřazuje dvojici $[\varphi, e]$ hodnotu 1“ je primitivně rekurzívní, neboť velikost pravdivostní relace lze odhadnout primitivně rekurzívní funkcí ve φ a e.

13. Nechť $\mathbf{M}$ je struktura pro aritmetický jazyk a $\mathbf{A}$ je její podstruktura. Řekneme, že $\mathbf{A}$ splňuje *Tarského-Vaughtovu podmínku* pro Γ-formule, jestliže pro každou formuli $\varphi(x, \underline{y}) \in \Gamma$ a pro každou r-tici $b_1, \ldots, b_r$ prvků množiny A platí implikace $\mathbf{M} \models (\exists x \varphi)[\underline{b}] \Rightarrow \exists a \in A(\mathbf{M} \models \varphi[a, \underline{b}])$. Řekneme, že struktura $\mathbf{A}$ je Γ-*elementární*, jestliže všechny Γ-formule jsou absolutní pro podstrukturu $\mathbf{A}$. Dokažte, že když $\mathbf{A}$ splňuje Tarského-Vaughtovu podmínku pro Π_m-formule, pak $\mathbf{A}$ je Σ_{m+1}-elementární.

14. Dokažte, že když $\mathbf{A}$ je Σ_{m+1}-elementární podstruktura struktury $\mathbf{M}$ a $\mathbf{M} \models \mathsf{PA}$, pak $\mathbf{A} \models \mathrm{I}\Sigma_m$.

    Návod. Dokažte indukcí dle k, že $\mathbf{A} \models \mathrm{I}\Sigma_k$ pro každé $k \leq m$. Zdůvodněte úvahami podobnými jako v cvičení 5 oddílu 4.2, že máte-li Σ_{k-1}-indukci a je-li $\varphi(x, \underline{y}) \in \Sigma_k$, pak formule $\varphi(0, \underline{y}) \,\&\, \forall x(\varphi(x, \underline{y}) \to \varphi(\mathrm{S}(x), \underline{y}))$ je ekvivalentní s Π_{k+1}-formulí, a je tedy absolutní pro podstrukturu $\mathbf{A}$ vzhledem k předpokladu, že $\mathbf{A}$ je Σ_{m+1}-elementární.

15. Nechť $\mathbf{M} \models \mathsf{PA}$. Řekneme, že prvek a modelu $\mathbf{M}$ je Γ-*definovatelný*, jestliže existuje formule $\psi(x) \in \Gamma$, která jej v $\mathbf{M}$ definuje. Zdůvodněte využitím věty 4.3.12, že existuje model Peanovy aritmetiky, který má nestandardní Δ_0-definovatelné prvky.

16. Nechť $\mathbf{M} \models \mathsf{PA}$ a nechť D_n označuje množinu všech Σ_{n+1}-definovatelných prvků modelu $\mathbf{M}$. Zdůvodněte, že množina D_n je podstruktura modelu $\mathbf{M}$, tj. že obsahuje nulu a je uzavřená na sčítání, násobení a přičítání jedničky.

17. Nechť D_n a $\mathbf{M}$ jsou jako v předchozím cvičení. Dokažte užitím cvičení 13 a 14, že D_n je Σ_{n+1}-elementární podstruktura modelu $\mathbf{M}$, která je modelem teorie $\mathrm{I}\Sigma_n$.

18. Nechť $\alpha(x,y)$ označuje formuli

    > číslo x je formule s jednou volnou proměnnou, platí $\mathsf{Fm}_{n+1}(x)$ a přitom pro (některé nebo každé) ohodnocení e přiřazující číslo y oné jediné volné proměnné formule x platí $\mathrm{Sat}_{n+1}(x,e)$.

    Stručněji řečeno, formule $\alpha(x,y)$ říká číslo x je Σ^+_{n+1}-formule s jedinou volnou proměnnou, která je (n+1)-splněná číslem y. Zdůvodněte, že formule α je $\Sigma_{n+1}(\mathsf{PA})$. Nechť dále $\beta(x,y)$ je formule $\alpha(x,y)\,\&\,\forall v(\alpha(x,v)\to v=y)$. Zdůvodněte, že jsou-li D_n a $\mathbf{M}$ jako v předchozích cvičeních, pak formule β je absolutní pro podstrukturu D_n. Vysvětlete, jak se přitom uplatní vědomost, že $D_n\models \mathrm{I}\Sigma_n$. Zdůvodněte, že $\forall b\in D_n\exists m\in \mathrm{N}(\mathbf{M}\models\beta(\overline{m},y)[b])$. Nakonec dokažte, že formule $\forall y\exists x{<}t\,\beta(x,y)$ je v D_n splněna právě těmi ohodnoceními, která proměnné t přiřazují nestandardní prvek. Z toho plyne, že obsahuje-li D_n nějaké nestandardní prvky, pak $D_n\not\models\mathsf{PA}$.

19. Dokažte užitím předchozího cvičení (a cvičení 15), že žádná z teorií $\mathrm{I}\Sigma_n$ není ekvivalentní s PA. Z toho plyne, že Peanova aritmetika není konečně axiomatizovatelná.

20. Formulujte schémata podobná tvrzením 4.4.17(c) a 4.4.20(g), ve kterých by se jako hodnoty proměnných připouštěla libovolná (formální) přirozená čísla, ne jen (standardní) numerály. Naznačte důkaz a zdůvodněte, že k důkazu všech instancí obou schémat v PA stačí jen konečně mnoho axiomů.

21. Zdůvodněte, že existuje $n_0\geq 1$ takové, že každá teorie $\mathrm{I}\Sigma_n$ pro $n\geq n_0$ je konečně axiomatizovatelná.

    Návod. Užitím dílčí definice pravdy Sat_n a předchozího cvičení lze indukci pro všechny Σ_n-formule formulovat pomocí jediné formule. Číslo n_0 zvolte tak, že všechny axiomy PA nutné v předchozím cvičení jsou v Σ_{n_0}.

4.5 Autoreference, Druhá Gödelova věta

Uvažujme aritmetickou formuli $\psi(x)$ s jednou volnou proměnnou x. Formule $\psi(x)$ může být libovolná, ale představujme si ji nějak jako $\mathsf{Tr}_n(x)$ nebo $\neg\mathsf{Pr}_{\mathsf{Q}}(x)$, tj. jako formuli, která vyjadřuje nějakou vlastnost formálních formulí x. Položme si otázku, zda za proměnnou x lze do formule $\psi(x)$ dosadit nějaký numerál tvaru $\overline{\varphi}$, kde φ je sentence, tak, aby výsledná sentence $\psi(\overline{\varphi})$ byla (dokazatelně například v PA) ekvivalentní se sentencí φ. Tutéž otázku lze také vyjádřit v terminologii řešení rovnic: má každá rovnice tvaru $\mathsf{PA}\vdash\varphi\equiv\psi(\overline{\varphi})$ nebo $\mathsf{Q}\vdash\varphi\equiv\psi(\overline{\varphi})$ pro neznámou sentenci φ řešení? Na první pohled to možná vypadá, že sotva, a navíc, že odpověď může záviset na tom, jak přesně bylo zvoleno kódování (konečných množin a posloupností), tj. přiřazení přirozených čísel formulím. Uvidíme, že tomu tak není. Rovnice $\mathsf{Q}\vdash\varphi\equiv\psi(\overline{\varphi})$ (a tedy i rovnice $\mathsf{PA}\vdash\varphi\equiv\psi(\overline{\varphi})$) má vždy řešení a důkaz nevyužívá žádné zvláštní vlastnosti kódování.

Ekvivalenci $\varphi \equiv \psi(\overline{\varphi})$ lze číst sentence φ tvrdí, že $\overline{\varphi}$ má vlastnost ψ. Lze také říci, že φ tvrdí o sobě já mám vlastnost ψ. Z tohoto důvodu se věta, která zaručuje existenci řešení rovnic tvaru $T \vdash \varphi \equiv \psi(\overline{\varphi})$, kde T je vhodná teorie, nazývá věta o autoreferenci. Věta o autoreferenci umožňuje psát výroky „v první osobě“.

Věta 4.5.1 (o autoreferenci) *Ke každé aritmetické formuli $\psi(x)$ existuje aritmetická sentence φ taková, že $\mathsf{Q} \vdash \varphi \equiv \psi(\overline{\varphi})$.*

Důkaz obsahuje také určitý „samovztažný“ motiv. Budeme se totiž zabývat situací, kdy do nějaké formule $\alpha(x)$ je za její jedinou volnou proměnnou dosazen její vlastní číselný kód, tj. numerál $\overline{\alpha}$. Definujme aritmetickou funkci f tímto předpisem:

$$f(\alpha) = \begin{cases} \alpha(\overline{\alpha}) & \text{když } \alpha(x) \text{ je formule s jednou volnou proměnnou} \\ 0 & \text{jinak.} \end{cases}$$

Funkce f je (primitivně) rekurzívní. Podle věty 4.4.14 k funkci f existuje Σ_1-formule $\gamma(x, y)$, která ji reprezentuje v Q. To znamená, že podmínka

$$\mathsf{Q} \vdash \forall y\big(\gamma(\overline{\alpha}, y) \;\equiv\; y = \overline{\alpha(\overline{\alpha})}\,\big) \tag{1}$$

platí pro každou formuli $\alpha(x)$ s jednou volnou proměnnou. Nechť aritmetická formule $\psi(x)$ je dána. Označme $\chi(x)$ formuli $\exists y(\gamma(x, y) \;\&\; \psi(y))$ a označme φ sentenci $\chi(\overline{\chi})$. Vztáhneme-li (1) na formuli $\chi(x)$, dostaneme

$$\mathsf{Q} \vdash \forall y(\gamma(\overline{\chi}, y) \;\equiv\; y = \overline{\varphi}). \tag{2}$$

Ověřme dokazatelnost ekvivalence $\varphi \equiv \psi(\overline{\varphi})$ v Q:

Nechť $\psi(\overline{\varphi})$. Z implikace $\leftarrow$ v (2) máme $\gamma(\overline{\chi}, \overline{\varphi})$. Existuje tedy číslo y, totiž $\overline{\varphi}$, takové, že $\gamma(\overline{\chi}, y)$ a zároveň $\psi(y)$. Tedy $\chi(\overline{\chi})$.

Nechť naopak $\chi(\overline{\chi})$. Existuje tedy y splňující současně podmínky $\gamma(\overline{\chi}, y)$ a $\psi(y)$. Implikace $\rightarrow$ v (2) ale říká, že první z těchto podmínek splňuje jediné y, totiž $\overline{\varphi}$. Tedy $\psi(\overline{\varphi})$.

QED

Větu o autoreferenci není ani tak těžké dokázat. Spíš je těžké ji netriviálním způsobem použít, čili zvolit formuli $\psi(x)$ tak, aby rovnice $\vdash \varphi \equiv \psi(\overline{\varphi})$ neměla žádná nezajímavá řešení typu $0 = 0$ nebo $0 = \overline{1}$. Autoři netriviálních užití věty o autoreferenci jsou zpravidla známi a sentence φ splňující nějakou zajímavou rovnici se citují jako něčí autoreferenční formule.

V tomto oddílu si postupně ukážeme několik příkladů na užití věty o autoreferenci. Začněme nápadem, který se připisuje Alfredu Tarskému: co dostaneme, pokusíme-li se v aritmetice reprodukovat paradox lháře, tj. napsat sentenci já jsem nepravdivá?

Věta 4.5.2 *Pro žádnou bezespornou teorii T obsahující Q neexistuje aritmetická formule $\mathsf{Tr}(x)$ taková, že pro každou aritmetickou sentenci φ platí $T \vdash \varphi \equiv \mathsf{Tr}(\overline{\varphi})$.*

Důkaz Nechť taková formule $\mathsf{Tr}(x)$ existuje. Podle věty o autoreferenci k formuli $\neg\mathsf{Tr}(x)$ existuje sentence ω taková, že $\mathsf{Q} \vdash \omega \equiv \neg\mathsf{Tr}(\overline{\omega})$. Protože T obsahuje Q, máme $T \vdash \omega \equiv \neg\mathsf{Tr}(\overline{\omega})$. Protože pro formuli $\mathsf{Tr}(x)$ platí dekvotační schéma, máme $T \vdash \omega \equiv \mathsf{Tr}(\overline{\omega})$. Z ekvivalencí $\omega \equiv \neg\mathsf{Tr}(\overline{\omega})$ a $\omega \equiv \mathsf{Tr}(\overline{\omega})$ lze v T dokázat $\omega \to \neg\omega$ i $\neg\omega \to \omega$. V T tedy lze dokázat ω i $\neg\omega$. To je spor s předpokladem, že T je bezesporná. QED

V předchozím oddílu jsme pro každé n sestrojili formuli $\mathsf{Tr}_n(x)$, která je dílčí definicí pravdy pro Σ_n^+-formule. V závěru jsme poznamenali, že k tomu, abychom dokázali sentenci $\mathsf{Con}(\pi)$ vyjadřující bezespornost Peanovy aritmetiky, by pomohla uniformní definice pravdy, tj. jedna definice pravdy pro všechny aritmetické formule najednou. Z věty 4.5.2 je jasné, že tento plán je neproveditelný: uniformní definice pravdy neexistuje.

Ve větě 4.5.2 se nepředpokládá, že T je rekurzívně axiomatizovatelná. Můžeme tedy volit $T := \mathrm{Th}(\mathbf{N})$: neexistuje formule $\mathsf{Tr}(x)$ taková, že $\mathbf{N} \models \varphi \equiv \mathsf{Tr}(\overline{\varphi})$ pro každou sentenci φ. To dále znamená, že neexistuje formule $\mathsf{Tr}(x)$ taková, že pro každou sentenci φ platí ekvivalence $\mathbf{N} \models \varphi \Leftrightarrow \mathbf{N} \models \mathsf{Tr}(\overline{\varphi})$. Tím jsme ověřili, že věta 4.5.2 poskytuje alternativní důkaz věty 4.3.10, tj. tvrzení, že množina $\mathrm{Th}(\mathbf{N})$ není v $\mathbf{N}$ definovatelná. Obě věty 4.3.10 a 4.5.2 se citují jako *Tarského věta o nedefinovatelnosti pravdy.*

V důkazu věty 4.5.2 jsme větu o autoreferenci použili na formuli $\psi(x)$, která neexistuje, a výsledkem byl důkaz, že opravdu neexistuje. Větu o autoreferenci lze ale samozřejmě použít i na takovou formuli $\psi(x)$, o které víme, že existuje, protože jsme ji dříve sestrojili. V následujících větách 4.5.3 a 4.5.6 pracujeme se sentencemi, které říkají něco o vlastních důkazech nebo o vlastní dokazatelnosti. *Gödelova sentence* říká já jsem nedokazatelná, *Rosserova sentence* říká před každým mým důkazem existuje menší důkaz mé negace.

V několika následujících tvrzeních předpokládáme, že T je teorie obsahující Peanovu aritmetiku a že $\tau(x)$ je Σ-formule, která definuje v $\mathbf{N}$ množinu T. Z věty 4.4.16 víme, že pro formuli $\mathsf{Pr}_\tau(x)$ platí podmínky D1–D3, tj. podmínky pro dokazatelnost. Dále víme z věty 4.2.13, že formule $\mathsf{Pr}_\tau(x)$ definuje v $\mathbf{N}$ množinu $\mathrm{Thm}(T)$. Tento fakt formulujme explicitně a označme si jej: ekvivalence

Def: $\quad T \vdash \varphi \Leftrightarrow \mathbf{N} \models \mathsf{Pr}_\tau(\overline{\varphi})$

platí pro každou sentenci v jazyce teorie T. Užitečná bude také vědomost, že $\mathsf{Pr}_\tau(x)$ je Σ-formule, viz 4.3.5. Ještě poznamenejme, že Σ-formule, která definuje v $\mathbf{N}$ množinu T, existuje k teorii T právě tehdy, když T je rekurzívně axiomatizovatelná.

Věta 4.5.3 (První Gödelova o neúplnosti) *Nechť T je Σ-korektní teorie obsahující Peanovu aritmetiku a nechť $\tau(z)$ je Σ-formule, která definuje v $\mathbf{N}$ množinu T. Platí-li $\mathsf{PA} \vdash \nu \equiv \neg\mathsf{Pr}_\tau(\overline{\nu})$, pak ν je sentence nezávislá na T.*

Důkaz Postupujme sporem. Nechť $T \vdash \nu$. Podmínka D1 dává $T \vdash \mathsf{Pr}_\tau(\overline{\nu})$. Z předpokladu $\mathsf{PA} \vdash \nu \equiv \neg\mathsf{Pr}_\tau(\overline{\nu})$ plyne $T \vdash \neg\mathsf{Pr}_\tau(\overline{\nu})$. Tedy T je sporná. To ale není, protože je Σ-korektní.

Víme už tedy $T \nvdash \nu$. Podmínka Def dává $\mathbf{N} \not\models \mathsf{Pr}_\tau(\overline{\nu})$. Dále postupujme opět sporem. Nechť $T \vdash \neg\nu$. Z předpokladu $\mathsf{PA} \vdash \nu \equiv \neg\mathsf{Pr}_\tau(\overline{\nu})$ plyne $T \vdash \mathsf{Pr}_\tau(\overline{\nu})$. Fakt, že T je Σ-korektní, dává $\mathbf{N} \models \mathsf{Pr}_\tau(\overline{\nu})$. QED

Předchozím důkazem jsme vlastně nezískali žádnou novou vědomost, ve větách 4.3.11, 4.3.12, 4.4.8 a 4.4.11 jsme už tvrdili víc. Jeho význam je jednak v tom, že jde o původní (klasický) důkaz První Gödelovy věty, a dále v tom, že jeho prodloužením získáme důkaz Druhé Gödelovy věty. Nejprve si ale rozmysleme jedno pomocné tvrzení.

Lemma 4.5.4 *Nechť T je teorie obsahující Peanovu aritmetiku a nechť $\tau(z)$ je Σ-formule, která definuje v $\mathbf{N}$ množinu T. Pak $\mathsf{Pr}_\tau(\overline{\varphi}) \to (\mathsf{Pr}_\tau(\overline{\neg\varphi}) \to \neg\mathsf{Con}(\tau))$ je sentence dokazatelná v PA pro každou volbu sentence φ.*

Důkaz Protože sentence $\varphi \to (\neg\varphi \to 0 = \mathrm{S}(0))$ je tautologie, víme

1: $\mathsf{PA} \vdash \varphi \to (\neg\varphi \to 0 = \mathrm{S}(0))$.

Dále platí

2: $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi \to (\neg\varphi \to 0 = \mathrm{S}(0))})$; 1, D1

3: $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi}) \to \mathsf{Pr}_\tau(\overline{\neg\varphi \to 0 = \mathrm{S}(0)})$; 2, D2

4: $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi}) \to (\mathsf{Pr}_\tau(\overline{\neg\varphi}) \to \mathsf{Pr}_\tau(\overline{0 = \mathrm{S}(0)}))$; 3, D2.

Nyní si stačí připomenout, že sentence $\mathsf{Con}(\tau)$ je definována jako $\neg\mathsf{Pr}_\tau(\overline{0 = \mathrm{S}(0)})$. QED

Vraťme se ještě k důkazu První Gödelovy věty. Podmínku Def, ve které je řeč o struktuře $\mathbf{N}$, a Σ-korektnost, v jejíž definici je také řeč o struktuře $\mathbf{N}$, jsme použili pouze v druhé části důkazu, kde jsme ověřili, že sentence ν je v T nevyvratitelná. V první části jsme Σ-korektnost použili pouze k tomu, abychom tvrdili, že teorie T je bezesporná. V první části důkazu jsem vlastně ověřili, že sentence ν je v T nedokazatelná, je-li T bezesporná, což je fakt, který za chvíli, v důkazu Druhé Gödelovy věty, ještě použijeme. Podstatnou částí důkazu Druhé Gödelovy věty bude formalizace první části důkazu První Gödelovy věty, tj. důkaz sentence $\mathsf{Pr}_\tau(\overline{\nu}) \to \neg\mathsf{Con}(\tau)$ v Peanově aritmetice.

Věta 4.5.5 (Druhá Gödelova o neúplnosti) *Nechť T je bezesporná teorie obsahující Peanovu aritmetiku a nechť $\tau(z)$ je Σ-formule, která definuje v $\mathbf{N}$ množinu T. Pak $T \nvdash \mathsf{Con}(\tau)$.*

Důkaz Vezměme sentenci ν, která splňuje podmínku

1: $\mathsf{PA} \vdash \nu \equiv \neg\mathsf{Pr}_\tau(\overline{\nu})$.

Jak jsme před chvílí poznamenali, předpoklad o bezespornosti teorie T stačí k tvrzení, že sentence ν je nedokazatelná v T:

2: $T \nvdash \nu$.

Vezměme z ekvivalence (1) jen jednu implikaci a uvažujme, co lze dále v PA, a tedy i v T, dokázat o sentenci ν a o případném důkazu sporu:

3:	$\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\nu \to \neg\mathsf{Pr}_\tau(\overline{\nu})})$	; 1, D1
4:	$\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\nu}) \to \mathsf{Pr}_\tau(\overline{\neg\mathsf{Pr}_\tau(\overline{\nu})})$	; 3, D2
5:	$\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\nu}) \to \mathsf{Pr}_\tau(\overline{\mathsf{Pr}_\tau(\overline{\nu})})$	; D3
6:	$\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\mathsf{Pr}_\tau(\overline{\nu})}) \to (\mathsf{Pr}_\tau(\overline{\neg\mathsf{Pr}_\tau(\overline{\nu})}) \to \neg\mathsf{Con}(\tau))$	; Lemma 4.5.4
7:	$\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\nu}) \to \neg\mathsf{Con}(\tau)$	; 4, 5, 6
8:	$\mathsf{PA} \vdash \mathsf{Con}(\tau) \to \nu$	; 7, 1
9:	$T \nvdash \mathsf{Con}(\tau)$	; 8, 2.

QED

Z předchozího výkladu je jasné, že definují-li dvě formule v $\mathbf{N}$ tutéž množinu, nemusí to znamenat, že v dané teorii T lze dokázat jejich ekvivalenci. Explicitně to bylo řečeno ve cvičení 3 oddílu 4.3. Tento fakt naznačuje, že formule tvaru $\mathsf{Pr}_\tau(x)$ a sentence tvaru $\mathsf{Con}(\tau)$ utvořené z různých formulí $\tau(z)$ mohou být v dané teorii T neekvivalentní, přestože ony různé formule $\tau(z)$ definují v $\mathbf{N}$ tutéž množinu T. Ve cvičení 6 je zdůvodněno, že toto se opravdu děje: existují formule $\tau_1(z)$ a $\tau_2(z)$ takové, že obě definují v $\mathbf{N}$ množinu PA (tj. každá z nich je Σ-definicí množiny všech axiomů Peanovy aritmetiky), ale v PA nelze dokázat sentenci $\mathsf{Con}(\tau_1) \equiv \mathsf{Con}(\tau_2)$. Tím vším chceme říci, že dané teorii T lze více způsoby popsat její vlastní množinu axiomů a v dané teorii lze také více způsoby vyjádřit její vlastní bezespornost. Věta 4.5.5 tvrdí, že sentence $\mathsf{Con}(\tau)$ vyjadřující bezespornost teorie T je v T *vždy* nedokazatelná, pokud ovšem dodržíme podmínku, že τ je Σ-definicí množiny T. Pro jistotu znovu připomeňme, že Σ-definice množiny T existuje právě tehdy, je-li T rekurzívně axiomatizovatelná.

Druhou Gödelovu větu lze stručně formulovat takto: v žádné dostatečně silné rekurzívně axiomatizovatelné teorii nelze dokázat její vlastní bezespornost. Přitom „dostatečně silná“ pro náš text znamená „obsahující Peanovu aritmetiku“. Je známo, že Druhou Gödelovu větu lze v tomto ohledu značně zobecnit. Například pouhým prověřením příslušných partií této kapitoly lze zjistit, že věta 4.5.5 platí pro všechny teorie T obsahující teorii $\mathrm{I}\Sigma_1$, o které jsme mluvili ve cvičeních oddílů 4.3 a 4.4. Zájemce o zobecnění Druhé Gödelovy věty odkazujeme na tytéž zdroje, o kterých jsme se už zmínili na konci oddílu 4.2, tj. na články Pudláka, Wilkieho a Parise, případně na Hájkovu a Pudlákovu monografii [31].

Mezi více Σ-formulemi, které definují v $\mathbf{N}$ množinu všech axiomů Peanovy aritmetiky, je i formule $\pi(z)$, která axiomy Peanovy aritmetiky popisuje jako devět axiomů Robinsonovy aritmetiky plus všechny instance schématu indukce a které můžeme říkat *přirozená definice* množiny všech axiomů Peanovy aritmetiky. Na formuli $\pi(z)$ se ovšem věta 4.5.5 vztahuje také. Platí tedy $\mathsf{PA} \nvdash \mathsf{Con}(\pi)$. To je odpověď na otázku, kterou jsme od konce oddílu 4.2 opakovaně připomínali. Věta 4.5.2 vylučuje možnost dokázat sentenci $\mathsf{Con}(\pi)$ pomocí uniformní definice

pravdy. Věta 4.5.5 tuto možnost vylučuje absolutně, tj. bez ohledu na to, jaké prostředky bychom v důkazu snad použili.

Z věty 4.2.13 víme, že sentence $\neg\mathsf{Con}(\pi)$ není dokazatelná v PA. Věta 4.5.5 tedy poskytuje odpověď na otázku, kterou jsme v závěru oddílu 4.3 formulovali trochu jinak a která zní: je-li Peanova aritmetika neúplná, kde je tedy nějaký zajímavý příklad nezávislé sentence? Teorie, jejímiž axiomy jsou Q1–Q9 a všechny instance schématu indukce, je bezesporná, je příkladem takové sentence.

Lze namítnout, že ještě zajímavější než sentence o důkazech sporu by byla nezávislá sentence o přirozených číslech. Podrobněji lze tuto námitku formulovat následovně. Přirozená čísla jsou pro logiky zajímavá nikoliv jako čísla, nýbrž především jako kódy syntaktických objektů. Logikové vlastně přirozená čísla tak trochu zneužívají. Lze nezávislost na Peanově aritmetice dokázat pro nějakou sentenci, která je zajímavá i pro nelogiky? Odpověď zní ano. V kapitole [63] knihy [4] je nezávislost na Peanově aritmetice dokázána pro kombinatorické tvrzení, které je zobecněním Ramseyovy věty. Termín „matematický“ v názvu práce [63] je myšlen jako protiklad k „logický“. Později vznikla celá řada výsledků tohoto druhu. Některé jsou reprodukovány v knihách [47] a [31], tam lze nalézt i další odkazy. Obzvláště zajímavé příklady tvrzení nezávislých na PA, jejichž obsah (nikoliv ale důkaz nezávislosti) lze snadno vysvětlit a pochopit, se studují v článku [48]. Jeden z těchto příkladů je také vyložen v knize [85].

Vzpomeňme si, že věty o neúplnosti jsme nejprve (viz 4.3.11 a 4.3.12) formulovali pro teorii T s aritmetickým jazykem splňující předpoklad $\mathbf{N} \models T$. Později jsme předpoklad $\mathbf{N} \models T$ nahradili Σ-korektností nebo bezesporností a uvědomili jsme si, že nevadí, obsahuje-li jazyk L teorie T kromě šesti symbolů aritmetického jazyka ještě další symboly. V tom případě můžeme totiž definovat aritmetické formule jazyka L jako formule jazyka L neobsahující žádný z těchto dalších symbolů. K důkazu neúplnosti teorie T pak stačí ukázat nezávislou aritmetickou sentenci, v definici Σ-korektnosti (a vlastně i bezespornosti) stačí mluvit jen o aritmetických sentencích a v úvahách o m-převeditelnosti lze také vystačit s funkcemi, jejichž všechny hodnoty jsou aritmetické sentence. Nejdůležitější věty (zejména 4.4.11 a 4.5.5) se pak vztahují na teorie, které jsou dostatečně silnými (ve smyslu „bohatství jazyka“ a „síla axiomů“) *teoriemi univerza přirozených čísel*.

Věty 4.4.11 a 4.5.5 lze snadno zobecnit ještě dále. Stejně jako nevadí, jsou-li v jazyce teorie T nějaké další symboly, nevadí ani, jsou-li v jejím univerzu kromě přirozených čísel ještě další objekty. Stačí, máme-li v jazyce L teorie T formuli $\delta(x)$, kterou můžeme číst objekt x je přirozené číslo, neboli můžeme-li ze všech objektů teorie T přirozená čísla vyčlenit pomocí vhodné formule $\delta(x)$. Aritmetické formule pak můžeme definovat jako formule jazyka L, které s užitím pouze aritmetických symbolů mluví pouze o objektech splňujících podmínku $\delta(x)$. Jinak řečeno, s užitím terminologie z oddílu 3.6, máme-li formuli $\delta(x)$ a překlad symbolů $\sharp$ z aritmetického jazyka do jazyka L, můžeme aritmetické formule jazyka L definovat jako všechny formule tvaru φ^*, kde $*$ je příslušný překlad formulí. Tím jsme zdůvodnili, že Rosserova věta a všechny naše varianty První Gödelovy věty platí pro všechny teorie T, ve kterých je interpretovatelná Robinsonova aritmetika, kdežto Druhá

Gödelova věta platí pro všechny teorie T, ve kterých je interpretovatelná Peanova aritmetika.

Protože v ZF nebo v GB lze z univerza všech množin resp. tříd vyčlenit přirozená čísla formulí množina (resp. třída) x je ordinální číslo menší než první limitní číslo a operace a relace aritmetického jazyka lze interpretovat jako ordinální operace a relace na takto vyčleněných objektech, vztahují se Rosserova věta i Gödelovy věty i na teorie ZF a GB a také na další varianty teorie množin. Tyto teorie jsou tedy podstatně nerozhodnutelné a nezúplnitelné pomocí rekurzívní množiny dodatečných axiomů. Z nerozhodnutelnosti a konečné axiomatizovatelnosti teorie GB plyne postupem stejným jako v důkazu věty 4.4.9, že množina všech logicky platných formulí v jazyce $\{\in\}$ je algoritmicky nerozhodnutelná. Platí $\mathsf{GB} \nvdash \mathsf{Con}(\mathsf{GB})$; definujeme-li *přirozenou definici* $\mathsf{zf}(z)$ teorie ZF jako formuli, která axiomy teorie ZF popisuje jako několik jednotlivých axiomů a všechny instance schématu vydělení a schématu nahrazení, platí také $\mathsf{ZF} \nvdash \mathsf{Con}(\mathsf{zf})$. Z toho a z (důkazu) věty 3.6.19 je jasné, že $\mathsf{PA} \nvdash \mathsf{Con}(\mathsf{GB})$ a $\mathsf{PA} \nvdash \mathsf{Con}(\mathsf{zf})$. Na druhé straně, uvnitř ZF i GB víme, že každá teorie, která má model, je bezesporná, a také že struktura sestávající ze všech ordinálních čísel menších než první limitní ordinální číslo splňuje axiomy Q1–Q9 a všechny instance schématu indukce. To znamená, že sentence $\mathsf{Con}(\pi)$ vyjadřující bezespornost Peanovy aritmetiky je dokazatelná v ZF i v GB. Bez důkazu uveďme, že Gödelova-Bernaysova teorie množin je vůči aritmetickým (i vůči množinovým) sentencím konzervativní nad Zermelovou-Fraenkelovou teorií množin a že existují důkazy tohoto faktu, které lze formalizovat v PA. Platí tedy $\mathsf{PA} \vdash \mathsf{Con}(\mathsf{zf}) \to \mathsf{Con}(\mathsf{GB})$.

Všimněme si, že ordinální čísla menší než první limitní číslo hrála v předchozím odstavci dvojí úlohu. Jednak tvořila obor interpretace (díky níž jsme mohli tvrdit, že každá sentence dokazatelná v PA je dokazatelná i v ZF či v GB) a dále tvořila nosnou množinu modelu (formalizované) teorie $\{\, z\,;\, \pi(z)\,\}$ (díky němuž jsme uvnitř teorie množin mohli tvrdit, že formalizovaná Peanova aritmetika popsaná formulí π je bezesporná).

V oddílu 3.2 jsme v souvislosti s tzv. Skolemovým paradoxem poznamenali, že není známa žádná přímá konstrukce modelu teorie množin. Druhá Gödelova věta (spolu s faktem, že věta o silné úplnosti je formalizovatelná v teorii množin) vysvětluje, proč tomu tak je: pokud „přímá“ znamená „formalizovatelná v teorii množin“, pak taková konstrukce určitě neexistuje, neboť by znamenala důkaz bezespornosti teorie množin uvnitř teorie množin.

Ještě se zmiňme o tom, jak Druhá Gödelova věta souvisí s *Hilbertovým programem*. Následující odstavce jsou založeny hlavně na úvodní části kapitoly [78] a na článku [81]. Čtenáři s hlubším zájmem o Hilbertův program a historii logiky článek [81] vřele doporučujeme; je psán velmi čtivě a jsou v něm uvedeny další užitečné odkazy.

Některé z mnoha pěkných důkazů, které objevil D. Hilbert, byly ve své době kritizovány jako takzvaně nefinitní či nekonstruktivní. O Hilbertově řešení Gordanova problému v teorii invariantů Gordan sám prohlásil, že je to teologie, což pravděpodobně myslel pejorativně. Hilberta tato kritika mrzela a snažil se (úspěšně) napadené důkazy nahradit (většinou pracnějšími) finitními. Protože ale myslel dál

než jen na jednotlivé případy a také proto, že aktivity svých kritiků pravděpodobně (viz [81]) pokládal za nebezpečí pro matematiku, kterému je třeba čelit, uvažoval o možnosti dokázat, že takové nahrazení nekonstruktivního důkazu důkazem finitním je vždy možné. Podrobněji řečeno, v matematice lze rozlišit tvrzení *reálná* či *finitní* od tvrzení *ideálních* (která například mluví o nekonečných mohutnostech nebo obsahují střídající se kvantifikátory). Hilbert soudil, že ideální tvrzení představují zbytečné, avšak zpravidla pohodlné a účinné okliky. Podobně jako nemůžeme počítáním s komplexními čísly odvodit žádnou novou rovnost týkající se reálných čísel, nemůžeme ani pomocí ideálních tvrzení dokázat žádná nová finitní tvrzení. Transfinitní matematika, tj. matematika, v níž máme co dělat s ideálními tvrzeními, je konzervativním rozšířením finitní matematiky.

První verze Hilbertova programu byla formulována v Hilbertově přednáškovém cyklu v Hamburku v červenci 1921 a zněla *dokázat bezespornost aritmetiky finitními prostředky*. Aritmetikou se přitom mínila veškerá tehdejší matematika zahrnující i teorii množin („aritmetika“ tedy rozhodně neznamenalo „Peanova aritmetika“), kdežto finitní prostředky zahrnovaly indukci a můžeme si je dnes představit jako Peanovu aritmetiku nebo některý její fragment. Hilbertův program tedy můžeme chápat jako plán dokázat bezespornost teorie množin v Peanově aritmetice. Za součást Hilbertova programu lze pokládat i zpřesnění pojmu důkazu tak, aby se dosáhlo kontrolovatelnosti výsledků matematických úvah, čili aby se pojem důkazu stal finitním pojmem. Hilbert sám nazýval svůj plán *teorie důkazů*.

Není úplně jasné, proč konzervativnost transfinitní matematiky nad finitní matematikou byla ve formulaci Hilbertova programu nahrazena pouhou bezesporností (aritmetiky neboli) transfinitní matematiky. Jedno možné vysvětlení je takové, že Hilbert přikládal důkazům bezespornosti velký význam, neboť byl přesvědčen, že důkaz bezespornosti nějaké teorie T je zároveň důkazem, že objekty popsané axiomy teorie T existují. Bezespornost pokládal za kritérium existence. Druhý možný důvod naznačuje cvičení 9: pokud se rozhodneme, že finitní tvrzení jsou přesně ta, která lze vyjádřit aritmetickými Π_1-sentencemi, pak důkaz v PA, že nějaké rozšíření T Peanovy aritmetiky je bezesporné, je zároveň důkazem, že teorie T je nad PA konzervativní vůči finitním tvrzením. Toto cvičení má ovšem smysl pouze v situaci, kdy ještě nevíme o platnosti Druhé Gödelovy věty, jinak je triviální.

Hilbertův program pozitivně ovlivnil rozvoj logiky a o té jeho části, která požadovala zpřesnění a formalizaci pojmu důkazu, lze říci, že se úspěšně podařila. Teorie důkazů (v [94] se říká *strukturální teorie důkazů*) je dnes uznávanou logickou disciplínou. Na druhé straně, pokud Hilbertův program chápeme tak, jak bylo vysvětleno, čili jako plán dokázat v Peanově aritmetice bezespornost teorie množin, pak Druhá Gödelova věta znamená, že Hilbertův program je neproveditelný. Nejenže v PA nelze dokázat bezespornost teorie množin, nelze v ní dokázat dokonce ani bezespornost samotné Peanovy aritmetiky. Nejenže v PA nelze dokázat bezespornost teorie množin, ale ani veškerý aparát teorie množin nestačí k důkazu bezespornosti teorie množin. Teorie množin není konzervativním rozšířením Peanovy aritmetiky, neboť sentence $\mathsf{Con}(\pi)$ je dokazatelná v teorii množin, ale nikoliv v Peanově aritmetice (a přitom navíc vyjadřuje finitní tvrzení). Druhá Gödelova

věta ale znamená více než neproveditelnost Hilbertova programu. Domníváme se, že Druhá Gödelova věta také ruší či alespoň velmi problematizuje pojem finitního tvrzení a finitního důkazu. Ať bychom finitní důkazy definovali jakkoliv, pravděpodobně by je bylo možné ztotožnit s důkazy formalizovatelnými v nějaké (představujme si slabé) axiomatické teorii. Když ale taková teorie T splňuje známé a nepříliš náročné podmínky, je podezřelá z toho, že je sporná. Jinak řečeno, pokud obrat „finitní důkazové prostředky“ má znamenat něco, co je ne zcela triviální a přitom nezpochybnitelné čili jistě bezesporné, pak nic takového neexistuje. Snad kdybychom klasickou logiku nahradili nějakou jinou ... Vraťme se ale raději na zem, logika — ani klasická — nekončí Druhou Gödelovou větou.

Aplikujme větu 4.4.14 na funkci $\alpha \mapsto \neg\alpha$: existuje Σ_1-formule $\gamma(x,y)$ taková, že

$$\mathsf{Q} \vdash \forall y\big(\gamma(\overline{\alpha},y) \;\equiv\; y = \overline{\neg\alpha}\,\big) \qquad (*)$$

pro každou aritmetickou formuli α. Nechť jako obvykle $\tau(z)$ je Σ-definice nějakého rozšíření Peanovy aritmetiky. Vezměme za $\psi(x)$ formuli

$$\forall z(\mathsf{Proof}_\tau(x,z) \to \exists v{\le}z\,\exists y(\gamma(x,y)\;\&\;\mathsf{Proof}_\tau(y,v)))$$

a užijme na ni větu o autoreferenci: existuje sentence ρ taková, že

$$\mathsf{Q} \vdash \rho \;\equiv\; \forall z(\mathsf{Proof}_\tau(\overline{\rho},z) \to \exists v{\le}z\,\exists y(\gamma(\overline{\rho},y)\;\&\;\mathsf{Proof}_\tau(y,v))). \qquad (**)$$

Z podmínek $(*)$ a $(**)$ plyne

$$\mathsf{Q} \vdash \rho \;\equiv\; \forall z(\mathsf{Proof}_\tau(\overline{\rho},z) \to \exists v{\le}z\,\mathsf{Proof}_\tau(\overline{\neg\rho},v)).$$

Platí $\rho \in \Pi_1(\mathsf{PA})$. Sentenci ρ říkejme *Rosserova sentence* příslušná k formuli $\tau(z)$ resp. k teorii T. Než vyslovíme vlastnosti sentence ρ, všimněme si ještě, že předchozí úvaha o funkci $\alpha \mapsto \neg\alpha$ a formuli γ znamená, že větu o autoreferenci lze trochu zobecnit. Nejenže každá rovnice tvaru $\mathsf{Q} \vdash \varphi{\equiv}\psi(\overline{\varphi})$ má řešení, ale i všechny rovnice tvaru $\mathsf{Q} \vdash \varphi \equiv \psi(\overline{\varphi},\overline{\neg\varphi})$ či $\mathsf{Q} \vdash \varphi \equiv \psi(\overline{\neg\varphi})$ mají řešení pro každou volbu formule ψ.

Věta 4.5.6 (Rosserova) *Nechť T je bezesporná teorie obsahující Peanovu aritmetiku a nechť $\tau(z)$ je Σ-formule, která definuje v $\mathbf{N}$ množinu T. Nechť ρ je sentence splňující podmínku $\mathsf{Q} \vdash \rho \equiv \forall z(\mathsf{Proof}_\tau(\overline{\rho},z) \to \exists v{\le}z\,\mathsf{Proof}_\tau(\overline{\neg\rho},v))$. Pak ρ je nezávislá na T. Navíc platí $\mathsf{PA} \vdash \mathsf{Con}(\tau) \to \neg\mathsf{Pr}_\tau(\overline{\rho})\;\&\;\neg\mathsf{Pr}_\tau(\overline{\neg\rho})$.*

Důkaz Nechť T je bezesporná, a přitom některá ze sentencí ρ a $\neg\rho$ je v T dokazatelná. Vezměme nejmenší číslo m, které je důkazem kterékoliv ze sentencí ρ a $\neg\rho$. Je-li m důkazem sentence ρ, platí

$$\mathbf{N} \models \exists z(\mathsf{Proof}_\tau(\overline{\rho},z)\;\&\;\forall v{\le}z\,\neg\mathsf{Proof}_\tau(\overline{\neg\rho},v)), \qquad (1)$$

v opačném případě platí naopak

$$\mathbf{N} \models \exists v(\mathsf{Proof}_\tau(\overline{\neg\rho},v)\;\&\;\forall z{<}v\,\neg\mathsf{Proof}_\tau(\overline{\rho},z)). \qquad (2)$$

Sentence v (1) je sentence $\neg\rho$. Sentenci v (2) označme σ. Obě sentence $\neg\rho$ i σ jsou Σ-sentence. Platí-li (1), čili při probírání přirozených čísel jedno po druhém je dřív nalezen důkaz sentence ρ než důkaz sentence $\neg\rho$ (přičemž druhý z nich možná ani neexistuje), pak $T \vdash \rho$. Na druhé straně Σ-úplnost užitá na (1) dává $T \vdash \neg\rho$. Dále si všimněme, že platí

$$\mathsf{PA} \vdash \sigma \to \rho. \tag{3}$$

Platí-li (2), pak $T \vdash \neg\rho$, ale Σ-úplnost užitá na (2) a podmínka (3) dávají $T \vdash \rho$. Alternativa „(1) nebo (2)“, tj. předpoklad, že některá ze sentencí ρ a $\neg\rho$ je v T dokazatelná, je tedy ve sporu s předpokladem, že teorie T je bezesporná. Tím je dokončen důkaz první části věty. Důkaz druhé části je formalizací důkazu první části. Použijeme podmínky

$$\mathsf{PA} \vdash \neg\rho \to \mathsf{Pr}_\tau(\overline{\neg\rho}), \qquad \mathsf{PA} \vdash \sigma \to \mathsf{Pr}_\tau(\overline{\sigma}) \quad \text{a} \quad \mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\sigma \to \rho}). \tag{4}$$

Přitom první dvě podmínky platí díky větě o formalizované Σ-úplnosti, přesněji řečeno díky podobné úvaze, jako když jsme v důkazu věty 4.4.16 dokazovali platnost podmínky D3, třetí plyne z (3) užitím podmínky D1. Uvažujme v PA:

> Nechť $\mathsf{Pr}_\tau(\overline{\rho})$ nebo $\mathsf{Pr}_\tau(\overline{\neg\rho})$, tj. některá ze sentencí $\overline{\rho}$ a $\overline{\neg\rho}$ má důkaz. Je-li některý důkaz sentence $\overline{\rho}$ menší než jakýkoliv důkaz sentence $\overline{\neg\rho}$, pak $\neg\rho$. Z $\neg\rho$ na jedné straně plyne $\mathsf{Pr}_\tau(\overline{\rho})$, na druhé straně první podmínka v (4) dává $\mathsf{Pr}_\tau(\overline{\neg\rho})$. Tedy $\neg\mathsf{Con}(\tau)$. Je-li naopak některý důkaz sentence $\overline{\neg\rho}$ menší než jakýkoliv důkaz sentence $\overline{\rho}$, pak σ. Ze σ na jedné straně plyne $\mathsf{Pr}_\tau(\overline{\neg\rho})$, na druhé straně zbývající dvě podmínky v (4) a podmínka D2 dávají $\mathsf{Pr}_\tau(\overline{\rho})$. Tedy opět $\neg\mathsf{Con}(\tau)$.

QED

Rosserova věta stejně jako První Gödelova věta poskytuje konstrukci nezávislé sentence. Přitom jde o konstrukci, která funguje i pro nekorektní teorie, a navíc důkazy obou faktů $T \nvdash \rho$ a $T \nvdash \neg\rho$ lze formalizovat v PA. Vzpomeňme si, že v případě Gödelovy sentence ν to bylo trochu jinak. Tam jsme formalizovali důkaz faktu, že $T \nvdash \nu$, a tím jsme vlastně dokázali Druhou Gödelovu větu. Důkaz faktu „když T je Σ-korektní, pak $T \nvdash \neg\nu$“ jsme se formalizovat nepokusili. Avšak ve cvičení 16 je alespoň ukázáno, jak lze předpoklad o Σ-korektnosti vyslovit v aritmetickém jazyce.

Věta 4.5.7 *Peanova aritmetika není konečně axiomatizovatelná.*

Důkaz Nechť $F \subseteq \mathsf{PA}$ je konečná množina sentencí a přitom F a PA jsou ekvivalentní teorie. Pak formule $[F](z)$ a teorie F splňují předpoklady Druhé Gödelovy věty. Tedy $F \nvdash \mathsf{Con}(F)$. Protože F a PA jsou ekvivalentní, máme $\mathsf{PA} \nvdash \mathsf{Con}(F)$. To je ale ve sporu s tvrzením 4.4.22. QED

Větu 4.5.7 dokázal Ryll-Nardzewski. Připomeňme, že ve cvičeních oddílu 4.4 jsme uvedli jiný důkaz tohoto tvrzení. Důkaz, který jsme uvedli nyní, ukazuje, že Druhá Gödelova věta je nejen „finálním produktem“, tj. poučným a nečekaným

výsledkem, který zajímá i nelogiky, ale také užitečným technickým prostředkem, který lze použít v některých důkazech. Tohoto aspektu se ještě chvíli přidržme. Následující věta je uvedena v článku [20].

Věta 4.5.8 *(a) Nechť T a S jsou rekurzívně axiomatizovatelné teorie obsahující Peanovu aritmetiku a nechť T je interpretovatelná v S. Pak ke každé Σ-definici σ teorie S existuje Σ-definice τ teorie T taková, že $\mathsf{PA} \vdash \mathsf{Con}(\sigma) \to \mathsf{Con}(\tau)$.*
(b) Nechť T je bezesporná teorie obsahující Peanovu aritmetiku a nechť τ je její Σ-definice. Pak teorie $(T + \mathsf{Con}(\tau))$ není interpretovatelná v T.

Důkaz Budeme v PA formalizovat důkaz věty 3.6.19. Nechť $\sigma(z)$ je daná Σ-definice teorie S. Nechť je dána interpretace teorie T v teorii S a nechť $*$ je příslušný překlad formulí. Nechť $\gamma(y,x)$ je Σ-formule, která reprezentuje funkci $\varphi \mapsto \varphi^*$:

$$\mathsf{PA} \vdash \forall x\big(\gamma(\overline{\varphi},x) \;\equiv\; x = \overline{\varphi^*}\big) \tag{1}$$

pro každou formuli φ v jazyce teorie T. Stejným právem jako v 4.2.11(c) můžeme předpokládat, že formule γ navíc splňuje podmínku

$$\mathsf{PA} \vdash \forall y \exists! x \gamma(y,x). \tag{2}$$

Stejně jako v důkazu věty 3.6.19 (tj. přeříkáním uvnitř PA) lze ověřit, že

$$\mathsf{PA} \vdash \forall z \forall y \forall x(\mathsf{LogAx}(z) \,\&\, \mathsf{UnivClo}(z,y) \,\&\, \gamma(y,x) \to \mathsf{Pr}_\sigma(x)). \tag{3}$$

Uvnitř PA tedy víme, že univerzální uzávěry všech logických axiomů se překladem $*$ přeloží na formule dokazatelné v teorii σ. Totéž bychom chtěli tvrdit o vlastních axiomech teorie T. S vlastními axiomy teorie T ale máme tuto potíž: fakt, že všechny axiomy teorie T se překladem $*$ přeloží na formule dokazatelné v teorii S, je dán podmínkou věty a nemáme k němu žádný důkaz, který bychom mohli formalizovat uvnitř PA. To je mimochodem také důvod, proč netvrdíme $\mathsf{PA} \vdash \mathsf{Con}(\sigma) \to \mathsf{Con}(\tau)$ pro *libovolnou* Σ-definici τ teorie T, tvrdíme pouze, že existuje taková Σ-definice τ. Protože teorie T je rekurzívně axiomatizovatelná, můžeme zvolit její Σ-definici $\tau_0(z)$. Formuli $\tau(z)$ definujme takto:

$$\tau_0(z) \,\&\, \exists x \exists y(\mathsf{UnivClo}(z,y) \,\&\, \gamma(y,x) \,\&\, \mathsf{Pr}_\sigma(x)).$$

To je evidentně Σ-formule. Když φ je axiom teorie T, pak platí $\mathbf{N} \models \mathsf{UnivClo}(\overline{\varphi},\overline{\varphi})$, a také $\mathbf{N} \models \gamma(\overline{\varphi},\overline{\varphi^*})$. Navíc z předpokladu $S \vdash \varphi^*$ plyne $\mathbf{N} \models \mathsf{Pr}_\sigma(\overline{\varphi^*})$. To znamená, že formule $\tau(z)$ stejně jako formule $\tau_0(z)$ definuje v $\mathbf{N}$ množinu T. Uvnitř PA jsme se tedy rozhodli, že připustíme pouze takové axiomy, jejichž překlad je dokazatelný z množiny předpokladů $\{\, z \,;\, \mathsf{Sent}(z) \,\&\, \sigma(z) \,\}$. Tím jsme sice možná vyloučili některé z prvků množiny $\{\; z \;;\; \mathsf{Sent}(z) \;\&\; \tau_0(z) \;\}$, nikoliv ale sentence $\overline{\varphi}$ takové, že $\varphi \in T$. Z tvrzení 4.2.11(c) týkajícího se formule UnivClo a z podmínky (2) plyne

$$\mathsf{PA} \vdash \forall z \forall y \forall x(\mathsf{Sent}(z) \,\&\, \tau(z) \,\&\, \mathsf{UnivClo}(z,y) \,\&\, \gamma(y,x) \to \mathsf{Pr}_\sigma(x)). \tag{4}$$

Podmínky (3) a (4) říkají, že univerzální uzávěry všech logických axiomů i všech vlastních axiomů teorie τ se přeloží na formule dokazatelné v teorii σ. V PA lze

dále snadno ověřit, že množina všech formulí, jejichž univerzální uzávěry se přeloží na formule dokazatelné v teorii σ, je uzavřená na odvozovací pravidla. To vše znamená, že univerzální uzávěry všech formulí dokazatelných v teorii τ se přeloží na formule dokazatelné v teorii σ a také že případný spor v teorii τ se přeloží na spor v teorii σ. Opravdu tedy platí, že je-li τ sporná, pak i σ je sporná.

V (b) postupujme sporem. Nechť τ je Σ-definice teorie T obsahující PA a nechť teorie $(T + \mathsf{Con}(\tau))$ je interpretovatelná v teorii T. Dle již dokázaného tvrzení (a) k formuli τ existuje formule $\theta(z)$, která je Σ-definicí teorie $(T+\mathsf{Con}(\tau))$ a pro kterou platí $\mathsf{PA} \vdash \mathsf{Con}(\tau) \to \mathsf{Con}(\theta)$, tedy $(T + \mathsf{Con}(\tau)) \vdash \mathsf{Con}(\theta)$. Je-li teorie $(T + \mathsf{Con}(\tau))$ bezesporná, máme spor s Druhou Gödelovou větou pro teorii $(T + \mathsf{Con}(\tau))$ a formuli θ. Je-li sporná, máme spornou teorii, která je interpretovatelná v bezesporné, čili spor s větou 3.6.19. QED

Tvrzení (b) předchozí věty lze chápat jako zesílení Druhé Gödelovy věty. Nejen že sentence teorie T je bezesporná je v teorii T nedokazatelná. Přidáme-li ji k T jako nový axiom, dostaneme teorii, která je o dost silnější než původní teorie T v tom smyslu, že pomocí interpretace nelze dokázat její relativní bezespornost vůči teorii T.

Nechť $\mathbf{M}$ je struktura pro libovolný jazyk L. Řekneme, že množina $A \subseteq M$ je *parametricky definovatelná* ve struktuře $\mathbf{M}$, jestliže existuje formule $\varphi(x, y_1, \ldots, y_r)$ v L a prvky $b_1, \ldots, b_r$ struktury $\mathbf{M}$ takové, že $A = \{\, a \in M \,;\, \mathbf{M} \models \varphi[a, \underline{b}] \,\}$. Protože tato definice připouští i případ $r = 0$, je jasné, že každá množina definovatelná v $\mathbf{M}$ je současně také parametricky definovatelná v $\mathbf{M}$. Snadno lze ověřit (cvičení), že pro strukturu $\mathbf{N}$ (a obecně pro každou strukturu $\mathbf{M}$, jejíž každý prvek je v $\mathbf{M}$ definovatelný) naopak platí, že každá množina, která je v ní parametricky definovatelná, je v ní i definovatelná.

Nechť $\mathbf{M}$ je model Peanovy aritmetiky. Řekneme, že množina $A \subseteq \mathrm{N}$ je *standardní množinou* modelu $\mathbf{M}$, jestliže existuje aritmetická formule $\varphi(x, \underline{y})$ a prvky $b_1, \ldots, b_r$ modelu $\mathbf{M}$ takové, že $A = \{\, n \,;\, \mathbf{M} \models \varphi(\overline{n}, \underline{y})[\underline{b}] \,\}$. Jinými slovy, množina A je standardní množinou modelu $\mathbf{M}$, je-li průnikem nějaké množiny parametricky definovatelné v $\mathbf{M}$ se standardní částí modelu $\mathbf{M}$. Množinu všech standardních množin modelu $\mathbf{M}$ značíme $\mathrm{SSy}(\mathbf{M})$. Množině $\mathrm{SSy}(\mathbf{M})$ se říká *standardní systém* modelu $\mathbf{M}$ nebo také *Scottova množina* modelu $\mathbf{M}$. Je zřejmé, že standardní množiny struktury $\mathbf{N}$ jsou přesně ty, které jsou v $\mathbf{N}$ (parametricky nebo neparametricky) definovatelné, čili přesně ty, které jsou aritmetické. Více nás ale budou zajímat standardní množiny nestandardních modelů Peanovy aritmetiky.

V kapitole 2 jsme pracovali s posloupností p všech prvočísel. Nyní budeme potřebovat formalizovanou posloupnost všech prvočísel, čili Σ-formuli, která říká číslo y je x-té prvočíslo a která má vlastnost, že utvoříme-li s její pomocí a s pomocí formule $\mathsf{Prime}(x)$ sentence číslo $\overline{2}$ je 0-tým prvočíslem a pro každé x je (x+1)-ní prvočíslo nejmenším prvočíslem větším než x-té prvočíslo, obě tyto sentence jsou dokazatelné v PA. Pišme $\mathsf{p}(x)$ pro x-té (formální) prvočíslo. V PA je jasné, že funkce p souhlasí s funkcí p na standardních argumentech, což lze schematicky vyjádřit podmínkou $\forall n(\mathsf{PA} \vdash \mathsf{p}(\overline{n}) = \overline{\mathrm{p}(n)})$. Schematicky proto, že v aritmetickém jazyce nemáme

term $\mathsf{p}(x)$. Takto jsme ale už postupovali mnohokrát, viz komentář za větou 4.2.5. Následující lemma tvrdí mimo jiné, že v definici standardní množiny lze vystačit s počtem parametrů r rovným jedné, a dokonce lze vystačit s jedinou formulí $\varphi(x,y)$ společnou pro všechny standardní množiny, totiž s formulí když u je x-té prvočíslo, pak $u \mid y$, kterou schematicky zapisujeme $\mathsf{p}(x) \mid y$.

Lemma 4.5.9 *Nechť* $\mathbf{M}$ *je nestandardní model Peanovy aritmetiky. Pak*
(a) Pro každou množinu $A \in \mathrm{SSy}(\mathbf{M})$ *existuje formule* $\varphi(x,y)$ *a prvek* $b \in M$ *takové, že* $A = \{\, n \,;\, \mathbf{M} \models \varphi(\overline{n},y)[b] \,\}$.
(b) Množina $\mathrm{SSy}(\mathbf{M})$ *je uzavřena na sjednocení, průnik a komplement.*
(c) Když $A \in \mathrm{SSy}(\mathbf{M})$*, pak existuje* $b \in M$ *takový, že* $A = \{\, n ; \mathbf{M} \models (\mathsf{p}(\overline{n}) \mid y)[b] \,\}$.
(d) Množina $\mathrm{SSy}(\mathbf{M})$ *obsahuje i (nějaké) nerekurzívní množiny.*

Důkaz Platí-li $A = \{\, n \,;\, \mathbf{M} \models \varphi(\overline{n},\underline{y})[b_1,..,b_r] \,\}$, pak místo formule φ lze vzít formuli $\exists v_1 \,..\, \exists v_r (y = \langle v_1,..,v_r\rangle \;\&\; \varphi(x,\underline{v}))$ s volnými proměnnými x a y a místo r parametrů $b_1,..,b_r$ lze vzít jeden parametr $b = \langle b_1,..,b_r\rangle$. Lomené závorky v obou případech odkazují k formalizovanému kódování posloupností. Tím je dokázáno tvrzení (a).

V (c) předpokládejme, že standardní množina $A = \{\, n \,;\, \mathbf{M} \models \varphi(\overline{n},z)[b_1] \,\}$ je dána formulí $\varphi(x,z)$ a ohodnocením b_1 proměnné z. Indukcí podle t lze ověřit, že

$$\mathbf{M} \models \forall t \exists y \forall x (\mathsf{p}(x) \mid y \;\equiv\; \varphi(x,z) \;\&\; x < t)[b_1].$$

To znamená, že pro každé ohodnocení a proměnné t existuje ohodnocení b_2 proměnné y tak, že

$$\mathbf{M} \models \forall x (\mathsf{p}(x) \mid y \;\equiv\; \varphi(x,z) \;\&\; x < t)[a,b_1,b_2].$$

Zvolíme-li a nestandardní, čili větší než všechna x tvaru $\overline{n}$, a zvolíme-li k němu příslušné b_2, máme

$$\forall n (\mathbf{M} \models (\mathsf{p}(\overline{n}) \mid y \;\equiv\; \varphi(\overline{n},z))[b_1,b_2]),$$

a také

$$\forall n (\mathbf{M} \models (\mathsf{p}(\overline{n}) \mid y)[b_2] \;\Leftrightarrow\; \mathbf{M} \models \varphi(\overline{n},z)[b_1]).$$

Opravdu tedy platí $A = \{\, n \,;\, \mathbf{M} \models (\mathsf{p}(\overline{n}) \mid y)[b_2] \,\}$ pro vhodné ohodnocení b_2 proměnné y.

V (d) postupujme podobně jako v důkazu věty 4.4.11. Vezměme dvě disjunktní rekurzívně spočetné množiny A a B takové, že každá rekurzívně spočetná nadmnožina jedné z nich disjunktní s druhou je Σ_1-kompletní. Stejně jako v důkazu věty 4.4.11 k množinám A a B existuje formule $\theta(x)$ taková, že $\mathsf{PA} \vdash \theta(\overline{n})$ pro všechna $n \in A$ a $\mathsf{PA} \vdash \neg\theta(\overline{n})$ pro všechna $n \in B$. Pak množina $\{\, n \,;\, \mathbf{M} \models \theta(\overline{n}) \,\}$ je standardní množina modelu $\mathbf{M}$, která je nadmnožinou množiny A disjunktní s množinou B. Netvrdíme o ní, že je rekurzívně spočetná. Určitě je ale nerekurzívní. QED

V následující větě uvažujeme o tom, zda operace $+^{\mathbf{M}}$ a $\cdot^{\mathbf{M}}$ nějakého nestandardního modelu $\mathbf{M}$ Peanovy aritmetiky mohou být rekurzívní. Protože otázka po rekurzívnosti má smysl pouze pro množiny přirozených čísel a relace na přirozených číslech, uvažujeme o nestandardních modelech, jejichž nosná množina je množina N všech přirozených čísel. Množina N tedy ve větě 4.5.10 hraje dvojí roli: jednak je nosnou množinou modelu $\mathbf{M}$, jednak ji lze homomorfismem $n \mapsto \overline{n}^{\mathbf{M}}$ izomorfně zobrazit na podstrukturu (standardní část) modelu $\mathbf{M}$. Je-li N nosnou množinou modelu $\mathbf{M}$, pak operace $+^{\mathbf{M}}$ a $\cdot^{\mathbf{M}}$ nemusí mít nic společného s obvyklými operacemi $+$ a $\cdot$ na přirozených číslech, tj. s operacemi $+^{\mathbf{N}}$ a $\cdot^{\mathbf{N}}$ struktury $\mathbf{N}$. V důkazu věty 4.5.10 budeme kromě formalizované posloupnosti všech prvočísel potřebovat ještě jednu formalizovanou funkci, totiž mocninu. Pišme $\mathsf{exp}(y,x)$ tam, kde bychom ve skutečnosti (na metamatematické úrovni) psali y^x. Z vlastností funkce exp budeme potřebovat zejména tuto: $\mathsf{PA} \vdash \forall x_1 \forall x_2 \forall y(\mathsf{exp}(y, x_1 \cdot x_2) = \mathsf{exp}(\mathsf{exp}(y,x_1),x_2)$.

Věta 4.5.10 (Tennenbaumova) *Nechť* $\mathbf{M} = \langle \mathrm{N}, +^{\mathbf{M}}, \cdot^{\mathbf{M}}, 0^{\mathbf{M}}, \mathrm{S}^{\mathbf{M}}, \leq^{\mathbf{M}}, <^{\mathbf{M}} \rangle$ *je nestandardní model Peanovy aritmetiky. Pak každá z operací* $+^{\mathbf{M}}$ *a* $\cdot^{\mathbf{M}}$ *je nerekurzívní.*

Důkaz Předpokládejme, že $+^{\mathbf{M}}$ je rekurzívní. Zdůvodníme, že v tom případě každá množina $A \in \mathrm{SSy}(\mathbf{M})$ je rekurzívně spočetná. Vzhledem k uzavřenosti množiny $\mathrm{SSy}(\mathbf{M})$ na komplement (viz 4.5.9(b)) a Postově větě to znamená, že každá množina $A \in \mathrm{SSy}(\mathbf{M})$ je rekurzívní. To je ale spor s tvrzením 4.5.9(d). Nechť tedy $A \in \mathrm{SSy}(\mathbf{M})$ je dána. Podle tvrzení 4.5.9(c) existuje prvek b modelu $\mathbf{M}$ takový, že $A = \{\, n \,;\, \mathbf{M} \models (\mathsf{p}(\overline{n}) \mid y)[b] \,\}$. Protože funkce p souhlasí na standardních argumentech se skutečnou posloupností p všech prvočísel, máme

$$\begin{aligned} n \in A &\Leftrightarrow \mathbf{M} \models (\mathsf{p}(\overline{n}) \mid y)[b] \\ &\Leftrightarrow \exists d(\overline{\mathrm{p}(n)}^{\mathbf{M}} \cdot^{\mathbf{M}} d = b) \\ &\Leftrightarrow \exists d(\underbrace{d +^{\mathbf{M}} d +^{\mathbf{M}} \ldots +^{\mathbf{M}} d}_{\mathrm{p}(n) \text{ sčítanců}} = b). \end{aligned} \qquad (*)$$

Je-li funkce $+^{\mathbf{M}}$ rekurzívní, pak podmínka uvedená v závorce v posledním řádku ekvivalencí $(*)$ je rekurzívní, a množina A je tedy rekurzívně spočetná vzhledem k implikaci $\Leftarrow$ ve větě 2.2.25.

Uvažujme o násobení $\cdot^{\mathbf{M}}$ modelu $\mathbf{M}$. Nemůžeme jednoduše říci, že je-li $\cdot^{\mathbf{M}}$ rekurzívní, pak podmínka uvedená v závorce v prostředním řádku ekvivalencí $(*)$ je rekurzívní. K tomu bychom potřebovali vědět, že funkce $n \mapsto \overline{\mathrm{p}(n)}^{\mathbf{M}}$ je rekurzívní. Postupujme tedy trochu jinak. Vezměme $c \in \mathrm{N}$ takové, že $c = \mathsf{exp}^{\mathbf{M}}(\overline{2}, b)$. Platí

$$\begin{aligned} n \in A &\Leftrightarrow \exists d(\mathsf{exp}^{\mathbf{M}}(\overline{2}, \overline{\mathrm{p}(n)}^{\mathbf{M}} \cdot^{\mathbf{M}} d) = c) \\ &\Leftrightarrow \exists d(\mathsf{exp}^{\mathbf{M}}(\mathsf{exp}^{\mathbf{M}}(\overline{2}, d), \overline{\mathrm{p}(n)}^{\mathbf{M}}) = c) \\ &\Leftrightarrow \exists d(\mathsf{exp}^{\mathbf{M}}(d, \overline{\mathrm{p}(n)}^{\mathbf{M}}) = c) \\ &\Leftrightarrow \exists d(\underbrace{d \cdot^{\mathbf{M}} d \cdot^{\mathbf{M}} \ldots \cdot^{\mathbf{M}} d}_{\mathrm{p}(n) \text{ činitelů}} = c). \end{aligned}$$

Přitom za zmínku stojí implikace $\Leftarrow$ ve třetím řádku. Ta platí vzhledem k faktu, který v modelu $\mathbf{M}$ nemůže být popřen: každý dělitel mocniny dvojky je opět mocnina dvojky. Je-li násobení $\cdot^{\mathbf{M}}$ modelu $\mathbf{M}$ rekurzívní, opět jsme dospěli k závěru, že množina A je rekurzívně spočetná. QED

Tennenbaumovu větu lze vyslovit také takto: je-li $\mathbf{M}$ spočetný model Peanovy aritmetiky a zobrazíme-li jej na množinu N všech přirozených čísel nějakou vzájemně jednoznačnou funkcí, pak ať to uděláme jakkoliv, operace $+^{\mathbf{M}}$ a $\cdot^{\mathbf{M}}$ modelu $\mathbf{M}$ se zobrazí na nerekurzívní množiny. Tennenbaumova věta dává odpověď na otázku uvedenou v závěru oddílu 4.1. Nestandardní model Peanovy aritmetiky nelze sestrojit tak jednoduše, jako jsme sestrojili model Robinsonovy aritmetiky z obrázku 4.1.1 na str. 284. Tento model má totiž rekurzívní sčítání i násobení.

Následující věta je věta o autoreferenci v množném čísle. Budeme ji potřebovat v oddílu 5.3. Tvrzení 4.5.11(b) lze označit jako autoreferenci v čísle množném konečném, nebo také jako větu o řešitelnosti n rovnic pro n neznámých sentencí. Tvrzení (a) je autoreference v čísle množném nekonečném, neboť numerál $\overline{\varphi}$ ve formuli ψ reprezentuje nekonečně mnoho neznámých sentencí $\varphi(\overline{0})$, $\varphi(\overline{1})$, $\varphi(\overline{2})$, ...

Věta 4.5.11 *(a) Ke každé aritmetické formuli $\psi(x,z)$ existuje aritmetická formule $\varphi(z)$ taková, že $\forall k(\mathsf{Q} \vdash \varphi(\overline{k}) \equiv \psi(\overline{\varphi},\overline{k}))$.*
(a) Ke každé n-tici aritmetických formulí $\psi_1(x_1,..,x_n),..,\psi_n(x_1,..,x_n)$ existují aritmetické sentence $\lambda_1,..,\lambda_n$ takové, že ekvivalence

$$\lambda_1 \equiv \psi_1(\overline{\lambda_1},..,\overline{\lambda_n}), \quad \lambda_2 \equiv \psi_2(\overline{\lambda_1},..,\overline{\lambda_n}), \quad .., \quad \lambda_n \equiv \psi_n(\overline{\lambda_1},..,\overline{\lambda_n})$$

jsou dokazatelné v Q.

Důkaz K důkazu tvrzení (a) stačí projít důkaz věty 4.5.1 a zkontrolovat, že volná proměnná z nijak nevadí: vezmeme funkci $\alpha(x,z) \mapsto \alpha(\overline{\alpha},z)$ a formuli $\gamma(x,y)$ která ji reprezentuje, označíme $\chi(x,z)$ formuli $\exists y(\gamma(x,y) \,\&\, \psi(y,z))$ a za $\varphi(z)$ vezmeme formuli $\chi(\overline{\chi},z)$. Platí $\mathsf{Q} \vdash \forall z(\varphi(z) \equiv \psi(\overline{\varphi},z))$, tedy také $\forall k(\mathsf{Q} \vdash \varphi(\overline{k}) \equiv \psi(\overline{\varphi},\overline{k}))$.

Tvrzení (b) převedeme na tvrzení (a). Nechť formule $\psi_1(\underline{x}),..,\psi_n(\underline{x})$ jsou dány. Definujme funkce f_k pro $1 \le k \le n$:

$$f_k(\alpha) = \begin{cases} \alpha(\overline{k}) & \text{když } \alpha(x) \text{ je formule s jednou volnou proměnnou} \\ 0 & \text{jinak,} \end{cases}$$

a vezměme formule $\gamma_1(x,y),..,\gamma_n(x,y)$, které reprezentují funkce $f_1,..,f_n$. To znamená, že pro každou formuli $\alpha(x)$ s jednou volnou proměnnou a pro $1 \le k \le n$ platí

$$\mathsf{Q} \vdash \forall y\big(\gamma_k(\overline{\alpha},y) \;\equiv\; y = \overline{\alpha(\overline{k})}\,\big).$$

Dále označme $\psi(x,z)$ formuli

$$\exists y_1\,..\,\exists y_n(\gamma_1(x,y_1) \,\&\, ..\,\&\, \gamma_n(x,y_n) \,\& \\ \& \,((z=\overline{1} \,\&\, \psi_1(\underline{y})) \vee\, ..\, \vee\, (z=\overline{n} \,\&\, \psi_n(\underline{y})))).$$

Dle tvrzení (a) k formuli $\psi(x,z)$ existuje formule $\varphi(z)$ taková, že

$$\forall k(\mathsf{Q} \vdash \varphi(\overline{k}) \equiv \psi(\overline{\varphi},\overline{k})).$$

Snadno lze ověřit, že sentence $\varphi(\overline{k}) \equiv \psi_k(\overline{\varphi(\overline{1})},\ldots,\overline{\varphi(\overline{n})})$ je pro $1 \leq k \leq n$ dokazatelná v Q. Za hledané sentence $\lambda_1,\ldots,\lambda_n$ lze tedy vzít sentence $\varphi(\overline{1}),\ldots,\varphi(\overline{n})$. QED

Cvičení

1. Nechť Γ je rekurzívní množina aritmetických sentencí, která obsahuje všechny Σ_1- i Π_1-sentence dokazatelné v Q a která je bezesporná v tom smyslu, že nemá žádnou podmnožinu tvaru $\{\alpha,\neg\alpha\}$. Pak existuje Σ_1-sentence φ taková, že $\varphi \notin \Gamma$ a $\neg\varphi \notin \Gamma$. Dokažte.

   Návod. Vezměte formuli $\psi(x)$, která množinu Γ reprezentuje ve smyslu cvičení 9 z oddílu 4.4. Zdůvodněte, že sentence φ, která je řešením rovnice $\vdash \varphi \equiv \neg\psi(\overline{\varphi})$, má požadované vlastnosti.

2. Zdůvodněte převedením na předchozí cvičení, že pro každou rekurzívně axiomatizovatelnou a bezespornou teorii T obsahující Q existují Σ_1- a Π_1-sentence nezávislé na T.

   Návod. Nechť ne. Pak lze využitím Postovy věty zdůvodnit, že množina $\Gamma = (\Sigma_1 \cup \Pi_1) \cap \mathrm{Thm}(T)$ je rekurzívní. Na množinu Γ lze pak užít tvrzení z předchozího cvičení.

3. Nechť T je (ne nutně bezesporná či Σ-korektní) teorie s alespoň aritmetickým jazykem, která obsahuje Peanovu aritmetiku, a nechť $\tau(z)$ je Σ-formule, která definuje v $\mathbf{N}$ množinu T. Zdůvodněte, že implikace $\Rightarrow$ v podmínce Def plyne z podmínky D1. Zdůvodněte užitím podmínky Def, že pro každou sentenci φ platí implikace $\mathsf{PA} \vdash \mathsf{Pr}_\tau(\overline{\varphi}) \;\Rightarrow\; T \vdash \varphi$.

4. Přidáním ještě několika kroků k důkazu Druhé Gödelovy věty zdůvodněte, že v PA lze dokázat sentence $\nu \to \mathsf{Con}(\tau)$ a $\mathsf{Con}(\tau) \equiv \neg\mathsf{Pr}_\tau(\overline{\mathsf{Con}(\tau)})$.

5. Vyvoďte z Druhé Gödelovy věty pro teorii $(\mathsf{PA} + \mathsf{Con}(\pi))$ a z tvrzení 4.2.14(h), že v PA nelze dokázat implikaci $\mathsf{Con}(\pi) \to \neg\mathsf{Pr}_\pi(\overline{\neg\mathsf{Con}(\pi)})$.

6. Nechť $\tau(z)$ je formule $\pi(z) \vee \exists y{\leq}z\,\mathsf{Proof}_\pi(\overline{\neg\mathsf{Con}(\pi)},y)$. Zdůvodněte, že formule $\tau(z)$ je Σ-definice Peanovy aritmetiky. Formule $\tau(z)$ popisuje axiomy Peanovy aritmetiky jako axiomy Robinsonovy aritmetiky a všechny instance schématu indukce, plus všechny sentence větší než první důkaz sentence $\overline{\neg\mathsf{Con}(\pi)}$, pokud nějaké takové důkazy existují. Dokažte sentenci $\mathsf{Pr}_\pi(\overline{\neg\mathsf{Con}(\pi)}) \to \neg\mathsf{Con}(\tau)$ v PA. Vyvoďte z toho a z předchozího cvičení, že $\mathsf{PA} \nvdash \mathsf{Con}(\pi) \to \mathsf{Con}(\tau)$.

7. Nechť $\tau \restriction y$, kde $\tau(z)$ je aritmetická formule, označuje formuli $\tau(z)\ \&\ z \leq y$. Dokažte pomocí věty 4.4.22, že všechny sentence tvaru $\mathsf{Con}(\pi \restriction \overline{n})$ jsou v PA dokazatelné.

8. Nechť $\pi^*(z)$ je formule $\pi(z)\&\mathsf{Con}(\pi\restriction z)$. Zdůvodněte, že formule $\pi^*(z)$ definuje v $\mathbf{N}$ množinu PA a že platí $\mathsf{PA}\vdash\mathsf{Con}(\pi^*)$. Vysvětlete, proč tento fakt není ve sporu s Druhou Gödelovou větou.

9. Zapomeňte na chvíli na Druhou Gödelovu větu a dokažte, že když τ je Σ-definice teorie T, která je rozšířením Peanovy aritmetiky, a platí $\mathsf{PA}\vdash\mathsf{Con}(\tau)$, pak každá Π_1-sentence dokazatelná v T je dokazatelná už v PA.

   Návod. Nechť $\eta\in\Pi_1$ a $T\vdash\eta$. Užijte podmínku D1 na sentenci η a formalizovanou Σ-úplnost na sentenci $\neg\eta$.

10. Řekneme, že sentence φ je Γ-konzervativní nad teorií T, kde Γ je některá z množin Σ_n či Π_n, jestliže každá sentence $\eta\in\Gamma$ dokazatelná v $(T+\varphi)$ je dokazatelná už v T. Zdůvodněte, že sentence φ dokazatelná v T je Γ-konzervativní pro každou třídu Γ. Dále zdůvodněte, že když φ je Γ-konzervativní nad T, pak $\varphi\notin\Gamma(T)$.

11. Dokažte, že když T je Σ-korektní teorie, která obsahuje Robinsonovu aritmetiku, pak každá Π_1-sentence bezesporná s T (tj. nevyvratitelná v T) je Σ_1-konzervativní nad T.

12. Nechť ρ je Rosserova sentence příslušná k přirozené definici π Peanovy aritmetiky. Zdůvodněte, že sentence ρ a $\mathsf{Con}(\pi)$ jsou Σ_1-konzervativní nad PA. Dále zdůvodněte, že sentence $\neg\rho$ není Π_1-konzervativní nad PA.

13. Dokažte, že sentence $\neg\mathsf{Con}(\pi)$ je Π_1-konzervativní nad PA.

    Návod. Nechť $(\mathsf{PA}+\neg\mathsf{Con}(\pi))\vdash\eta$ a $\eta\in\Pi_1$. Pomocí formalizované Σ-úplnosti užité na sentenci $\neg\eta$ a pomocí ekvivalence ze cvičení 4 dokažte v PA implikaci $\mathsf{Con}(\pi)\to\eta$. Tedy $\mathsf{PA}\vdash\eta$.

14. Dokažte, že rekurzívně axiomatizovatelná teorie T obsahující Robinsonovu aritmetiku je Σ-korektní, právě když neexistuje $\Delta_1(T)$-sentence nezávislá na T.

    Návod. Nechť teorie T není Σ-korektní. Vezměte Σ-definici τ teorie T a formuli $\delta(v)\in\Delta_0$ takovou, že $T\vdash\exists v\delta(v)$, ale $\mathbf{N}\not\models\exists v\delta(v)$. Dále pracujte se sentencí φ, která splňuje podmínku $T\vdash\varphi\equiv\forall z(\mathsf{Proof}_\tau(\overline{\varphi},z)\to\exists v{\leq}z\,\delta(v))$.

15. Nechť π je přirozená definice PA a nechť sentence $\mathsf{Con}^n(\pi)$ jsou pro $n\geq 0$ definovány rekurzí: $\mathsf{Con}^0(\pi)$ je sentence $0=0$, a dále $\mathsf{Con}^{n+1}(\pi)$ je sentence $\neg\mathsf{Pr}_\pi(\overline{\neg\mathsf{Con}^n(\pi)})$. Zdůvodněte, že všechny sentence $\mathsf{Con}^n(\pi)$ platí v $\mathbf{N}$ a že sentence $\mathsf{Con}^1(\pi)$ a $\mathsf{Con}(\pi)$ jsou ekvivalentní. Jaké implikace mezi sentencemi $\mathsf{Con}^n(\pi)$ lze dokázat v PA? Pro které dvojice čísel n a m je teorie $(\mathsf{PA}+\mathsf{Con}^n(\pi))$ intepretovatelná v teorii $(\mathsf{PA}+\mathsf{Con}^m(\pi))$?

16. Označme $\mathsf{1Con}(\pi)$ sentenci $\forall z(\mathsf{Fm}_1(z)\,\&\,\mathsf{Pr}_\pi(z)\to\mathsf{Tr}_1(z))$. Zdůvodněte, že sentence $\mathsf{1Con}(\pi)$ je v $\Pi_2(\mathsf{PA})$. Dokažte, že je-li η libovolná Π_1-sentence taková, že $\mathsf{PA}\vdash\mathsf{1Con}(\pi)\to\eta$, pak platí i $\mathsf{PA}\vdash\mathsf{1Con}(\pi)\to\mathsf{Con}(\pi+\overline{\eta})$. Vyvoďte z toho, že

sentence $\mathsf{1Con}(\pi)$ není v $\Pi_1(\mathsf{PA})$ a že z předpokladu $\mathsf{1Con}(\pi)$ lze v PA dokázat všechny sentence $\mathsf{Con}^n(\pi)$ z předchozího cvičení.

Návod. Užijte implikaci $\neg\sigma \to \neg\mathsf{Tr}_1(\overline{\sigma})$ na sentenci σ ekvivalentní s $\neg\eta$.

17. Dokažte, že Peanova aritmetika není interpretovatelná v žádné své konečné podteorii.

18. Dokažte využitím cvičení 1, že je-li $\mathbf{M} \models \mathsf{Q}$, pak $(\Sigma_1 \cup \Pi_1) \cap \mathrm{Th}(\mathbf{M})$ je nerekurzívní množina. Také každá z množin $\Sigma_1 \cap \mathrm{Th}(\mathbf{M})$ a $\Pi_1 \cap \mathrm{Th}(\mathbf{M})$ je nerekurzívní.

19. Dokažte využitím cvičení 9 z oddílu 4.4, že je-li $\mathbf{M} \models \mathsf{PA}$ nestandardní, pak $\mathrm{SSy}(\mathbf{M})$ obsahuje všechny rekurzívní množiny.

20. Vyvoďte z cvičení 18 a z tvrzení 4.4.20(h), že je-li $\mathbf{M} \models \mathsf{PA}$ nestandardní, pak formule $\mathsf{Tr}_1(x)$ kóduje v $\mathbf{M}$ nerekurzívní množinu. Neplatí tedy $\mathrm{SSy}(\mathbf{M}) \subseteq \mathit{OR}$ (to jsme už tvrdili v 4.5.9(d)).

21. Je-li $\mathbf{M} \models \mathrm{Th}(\mathbf{N})$ nestandardní, pak $\mathrm{SSy}(\mathbf{M})$ obsahuje všechny aritmetické množiny. Dokažte. Vyvoďte z toho, že každá z operací $+^{\mathbf{M}}$ a $\cdot^{\mathbf{M}}$ je v tom případě nearitmetická množina.

22. Užijte větu 3.6.9 k důkazu, že existuje model $\mathbf{M} \models \mathsf{PA}$ nestandardní takový, že $\mathrm{SSy}(\mathbf{M}) \subseteq \mathit{\Sigma}_2 \cup \mathit{\Pi}_2$.

23. Dokažte, že rovnice $\mathsf{Q} \vdash \varphi(z) \equiv \psi(\ulcorner\varphi(\dot{z})\urcorner, z)$ pro neznámou formuli $\varphi(z)$ má řešení pro libovolnou aritmetickou formuli $\psi(x, z)$. Vyvoďte z toho, že také rovnice $\mathsf{Q} \vdash \varphi(\overline{n}) \equiv \psi(\overline{\varphi(\overline{n})}, \overline{n})$ pro neznámou formuli $\varphi(z)$ má vždy řešení.

5

Některé neklasické logiky

Comparison between Reflexion and Löb's Principle seems a potent antidote to the misguided impression that (. . .) Gödel Theorem means that Human Mental Powers exceed what formal systems can do, the Myth of the Mental Muscles.

(A. Visser, [96])

V dosavadním textu jsme se zabývali výhradně *klasickou logikou*. Její sémantika je ve výrokové logice založena na představě *dvou pravdivostních hodnot*, v predikátové logice máme Tarského definici, která dvouhodnotovou sémantiku zobecňuje na predikátové formule. Existuje ale celá řada logik, kterým se říká *neklasické* a které jsou založeny na jiných východiscích. Neklasické logiky často nacházejí různé aplikace, a to i v oblastech mimo logiku. A některé z nich skutečně aspirují na roli nové metody usuzování, alternativní vůči klasické logice. Tři z neklasických logik se čtenáři pokusíme přiblížit v této kapitole. Uznáváme, že jejich výběr je do značné míry subjektivní. Nicméně doufáme, že mnohé z úvah a metod zde uvedených jsou pro neklasické logiky typické.

5.1 Intuicionistická logika

Předpokládejme, že máme sentenci φ a predikátovou formuli $\psi(x)$ s jednou volnou proměnnou x, a uvažujme formuli

$$(\varphi \to \exists x \psi(x)) \to \exists x(\varphi \to \psi(x)). \qquad (*)$$

To je logicky platná formule; setkali jsme se s ní například v souvislosti s prenexními operacemi. Zdůvodnění, že formule $(*)$ opravdu je logicky platnou formulí, je lehké; doporučujeme čtenáři, aby si je před další četbou uvědomil nebo i napsal. Konstatujme rovnou, že toto zdůvodnění není z hlediska intuicionistické logiky korektní, a pokusme se vysvětlit, proč není.

Pro „klasickou“ matematiku jsou matematické objekty něčím, co je dáno a co někde a nějak existuje bez ohledu na lidskou aktivitu. Tady parafrázujeme vysvětlení v [45]. Každé tvrzení o matematických objektech je platné, nebo neplatné a úkolem matematika je zjistit, který z obou případů je pravdivý. Naproti tomu z hlediska intuicionismu neexistují matematické objekty a priori, nezávisle na lidské

aktivitě, nýbrž nové a nové objekty jsou vytvářeny pomocí *konstrukcí*. A o vlastnostech zkonstruovaných objektů se přesvědčujeme pomocí *konstruktivních důkazů*. Konstrukce a konstruktivní důkaz jsou pro intuicionismus[1] klíčové pojmy; od nich je totiž odvozeno intuicionistické chápání logických symbolů. Přesný význam logických spojek a kvantifikátorů v intuicionistické matematice je dán následujícími podmínkami:

- konstruktivní důkaz konjunkce $\varphi \,\&\, \psi$ sestává z konstruktivního důkazu tvrzení φ a dále z konstruktivního důkazu tvrzení ψ,
- konstruktivní důkaz disjunkce $\varphi \vee \psi$ sestává z ukazatele na jedno z tvrzení φ, ψ a z konstruktivního důkazu tohoto tvrzení,
- konstruktivní důkaz implikace $\varphi \to \psi$ sestává z konstrukce, která každý konstruktivní důkaz tvrzení φ převede na konstruktivní důkaz tvrzení ψ,
- $\bot$ (spor) nemá žádný konstruktivní důkaz,
- negace $\neg\varphi$ je chápána jako implikace $\varphi \to \bot$; konstruktivní důkaz tvrzení $\neg\varphi$ je tedy konstrukce, která každý důkaz tvrzení φ převede na důkaz sporu,
- konstruktivní důkaz tvrzení $\exists x \varphi(x)$ sestává z konstrukce, která nalezne objekt a a konstruktivní důkaz faktu, že a má vlastnost φ,
- konstruktivní důkaz tvrzení $\forall x \varphi$ je konstrukce, která ke každému objektu a nalezne důkaz tvrzení, že a má vlastnost φ.

Těmto podmínkám se říká *podmínky BHK* (anglicky *BHK-explanation*). BHK je zkratka jmen Brouwer, Heyting, Kolmogorov. Lze najít i zdroje (např. [95]), které interpretují „K“ jako Kreisel.

Vraťme se nyní k formuli $(\varphi \to \exists x \psi(x)) \to \exists x (\varphi \to \psi(x))$ a analyzujme ji využitím podmínek BHK. Platnost implikace $\varphi \to \exists x \psi(x)$ znamená, že máme proceduru, která každý konstruktivní důkaz tvrzení φ přepracuje na konstruktivní důkaz tvrzení $\exists x \psi(x)$. Konstruktivní důkaz tvrzení $\exists x \psi(x)$ znamená konstrukci, která nalezne objekt s vlastností ψ. Dohromady tedy máme konstrukci, která z každého konstruktivního důkazu tvrzení φ vytvoří objekt a s vlastností ψ. To ale neznamená, že máme a priori konstrukci objektu a s nějakou vlastností, byť bychom se spokojili se slabší vlastností vyjádřenou implikací $\varphi \to \psi(x)$.

Tím jsme zdůvodnili, proč formule $(*)$ není intuicionisticky logicky platnou formulí. Na druhé straně ale lze snadno postupně zdůvodnit, že následující tři formule jsou intuicionisticky logicky platnými formulemi:

$$\neg\varphi \to (\varphi \to \psi(x)),$$
$$\neg\varphi \to \exists x (\varphi \to \psi(x)),$$
$$(\varphi \to \exists x \psi(x)) \to (\varphi \vee \neg\varphi \to \exists x (\varphi \to \psi(x))).$$

[1] Ve stejném nebo podobném smyslu jako intuicionismus se užívá také termín *konstruktivismus*, někdy spíš ve spojitosti s ruskou matematickou školou.

Nemá-li přesto formule $(\varphi \to \exists x \psi(x)) \to \exists x(\varphi \to \psi(x))$ být intuicionisticky logicky platnou formulí, znamená to, že ani $\varphi \vee \neg\varphi$ nemůže být intuicionisticky logicky platnou formulí. To ostatně je v souladu s BHK-podmínkou pro disjunkci: $\varphi \vee \neg\varphi$ můžeme tvrdit až poté, kdy jsme konstruktivně dokázali φ nebo jsme konstruktivně dokázali $\neg\varphi$. *Tertium non datur*, princip vyloučeného třetího, není intuicionisticky přijatelným logickým principem.

Fakt, že princip vyloučeného třetího není intuicionisticky korektní, by ale neměl být chápán tak, že v intuicionistické logice jsou možné více než dvě logické hodnoty. Brzy uvidíme, že každý předpoklad tvaru $\neg(\varphi \vee \neg\varphi)$ vede v intuicionistické logice ke sporu. Z toho, že nějaké tvrzení, v našem případě $\varphi \vee \neg\varphi$, není intuicionisticky logicky platné, nelze usoudit, že za nějakých okolností by mohl platit jeho opak.

Podmínky BHK nepovažujeme za závaznou definici, ale spíše za heuristiku, důležitou pro intuicionismus jako filozofické stanovisko. Vzhledem k tomuto přístupu nemusíme diskutovat fakt, že podmínka pro symbol $\bot$ má možná trochu jiný charakter než podmínky pro ostatní logické symboly. Neuvažujeme ani o tom, zda s užitím podmínek BHK lze zdůvodnit intuicionistickou logickou platnost principu *ex falso*, ze sporu plyne cokoliv, vyjádřeného schématem $\bot \to \psi$ nebo $\varphi \to (\neg\varphi \to \psi)$. Spokojme se s prohlášením, že ano, princip ex falso je intuicionistickou tradicí přijímán jako korektní. Jsou ale myslitelné logiky ještě slabší než intuicionistická, ve kterých se tento princip nepovažuje za automaticky korektní. O tom si lze přečíst například v [94]. Několik zmínek spolu s úvahami o modifikacích podmínek BHK je také v [14]. Van Dalenovu kapitolu [14] doporučujeme jako úvodní četbu o intuicionistické logice a její historii.

K pojmu konstruktivního důkazu je nutno poznamenat, že se jím nemá rozumět důkaz v logickém smyslu, tj. formální posloupnost symbolů. Konstruktivní důkaz je mentální operací, která je korektní, pokud je v souladu s lidskou intuicí. Někde tady je třeba hledat původ termínu intuicionismus.

Vznik intuicionismu je spjat s pracemi L. E. J. Brouwera z počátku 20. století. Brouwer formuloval intuicionistickou filozofii matematiky, nikoliv ale logický systém. O otázky jazyka se prý (viz [45]) Brouwer vůbec nezajímal. Později vznikla rozsáhlá intuicionistická literatura; různé oblasti matematiky byly revidovány a znovu vystavěny na intuicionistických základech.

V našem textu nepůjde o revizi matematiky ani o intuicionismus jako filozofické stanovisko. Půjde nám o vlastnosti intuicionistické logiky jako jednoho z formálně logických systémů, o její vztah ke klasické logice a případně o její aplikace. Nepokoušíme se zavádět intuicionistickou logiku na metamatematickou úroveň. Na přímou otázku bychom odpověděli, že v úvahách o kalkulech a sémantice intuicionistické logiky užíváme logiku klasickou.

Intuicionistickou logiku jako formální systém formuloval A. Heyting, který tím zpřístupnil Brouwerovy práce širšímu okruhu zájemců. Čitelné a dosud čtené pojednání o kalkulech pro intuicionistickou logiku je v Kleeneho knize [49] z r. 1952. My začneme výklad od sémantiky, kterou vytvořil S. Kripke v r. 1965. Užití kripkovské sémantiky se neomezuje jen na intuicionistickou logiku. Je v neklasických logikách široce aplikovatelná a v oddílu 5.3 této kapitoly se s ní také setkáme.

5.1.1 Sémantika intuicionistické výrokové logiky

Formule intuicionistické výrokové logiky jsou sestaveny z výrokových atomů pomocí čtyř logických spojek $\&, \vee, \rightarrow, \neg$. Jsou to tedy tytéž formule jako v klasické výrokové logice. Důležitý rozdíl je v tom, že nelze například implikaci ekvivalentně vyjádřit pomocí disjunkce a negace. Žádnou ze spojek nelze vyjádřit pomocí ostatních, a přítomnost všech čtyř je tedy nutná. Ekvivalenci $\equiv$ nepovažujeme za základní spojku, nýbrž stejně jako v klasické výrokové logice za konjunkci dvou implikací.

Definice 5.1.1 *O trojici $\langle W, \leq, \Vdash \rangle$, kde $\leq$ je uspořádání na neprázdné množině W a relace $\Vdash$ je podmnožinou kartézského součinu množiny W s množinou všech výrokových formulí, řekneme, že je* kripkovským modelem *pro intuicionistickou logiku, jestliže pro libovolné prvky x a y množiny W, pro libovolné formule A a B a pro libovolný výrokový atom p platí:*

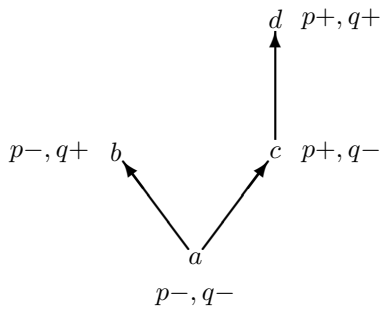
- *když $x \leq y$ a $x \Vdash p$, pak $y \Vdash p$,*
- *$x \Vdash A \,\&\, B$, právě když $x \Vdash A$ a $x \Vdash B$,*
- *$x \Vdash A \vee B$, právě když $x \Vdash A$ nebo $x \Vdash B$,*
- *$x \Vdash A \rightarrow B$, právě když $\forall y \geq x (y \Vdash A \Rightarrow y \Vdash B)$,*
- *$x \Vdash \neg A$, právě když $\forall y \geq x (y \nVdash A)$.*

Termín uspořádání má obvyklý význam: $\leq$ je reflexivní, tranzitivní a slabě antisymetrická relace na množině W. Prvkům množiny W říkejme jednoduše *vrcholy*. Zápis $x \leq y$ čteme „vrchol y je dosažitelný z vrcholu x“ nebo také „vrchol y je viditelný z vrcholu x“. Relaci $\leq$ říkáme *relace dosažitelnosti*. Relace dosažitelnosti nemusí být lineární. Dvojice $\langle W, \leq \rangle$ je *(kripkovský) rámec* modelu $\langle W, \leq, \Vdash \rangle$. Zápis $x \Vdash A$ čteme „formule A je splněna ve vrcholu x“ nebo též „vrchol x splňuje formuli A“. Relace $\Vdash$ je *pravdivostní relace*. Množina W může mít libovolnou (konečnou nebo nekonečnou) mohutnost, musí ale být neprázdná.

Prvkům kripkovského rámce se v literatuře obecně (tj. v souvislosti s kripkovskou sémantikou pro různé logiky) říká *stavy* nebo také *možné světy* (possible worlds). Můžeme si totiž představovat, že mezi výroky o světě nás obklopujícím některé jsou specifické (pro tento svět), kdežto některé jsou nutné (zákonité, logicky platné), neboť platí ve všech možných světech. Tato představa stejně jako termín „možné světy“ pochází od Leibnize. V intuicionistické logice lze prvky kripkovského rámce považovat za *informační stavy*; podmínka $x \Vdash A$ znamená, že stav informace x umožňuje tvrdit, že platí A. Přechod ze stavu x do stavu y dosažitelného z x lze chápat tak, že uplynul čas, během kterého byly získány (konstruktivně dokázány) nové informace. Naše definice požaduje, aby v tom případě nepřestal být splněn žádný výrokový atom, který byl splněn už v x. Tomuto požadavku se říká *podmínka perzistence*. Brzy uvidíme (viz 5.1.3), že pro ostatní formule (jiné než atomy) podmínka perzistence platí také.

Sémantika intuicionistické výrokové logiky zobecňuje sémantiku klasické výrokové logiky. V klasické logice přidělujeme výrokovým atomům libovolné pravdi-

vostní hodnoty. V intuicionistické logice je třeba nejprve (libovolně) zvolit kripkovský rámec a pak teprve přidělovat pravdivostní hodnoty atomům v jeho prvcích. Jsou-li dány pravdivostní hodnoty výrokových atomů ve všech vrcholech nějakého rámce, definice 5.1.1 jednoznačně určuje pravdivostní hodnoty všech ostatních formulí. Pravdivostní hodnota implikace $A \to B$ a negace $\neg A$ v nějakém vrcholu x závisí na pravdivostních hodnotách formulí A a B resp. formule A ve vrcholech dosažitelných z x. K určení pravdivostní hodnoty formulí $A \,\&\, B$ a $A \vee B$ v x stačí znát pravdivostní hodnoty formulí A a B jen v samotném vrcholu x.



Obrázek 5.1.1: Kripkovský model pro intuicionistickou logiku

Příklad 5.1.2 Na obrázku 5.1.1 je příklad kripkovského modelu $\langle W, \leq, \Vdash \rangle$. Množina stavů W obsahuje čtyři vrcholy a, b, c a d, relace dosažitelnosti $\leq$ je znázorněna šipkami. Na obrázku nejsou znázorněny „automatické“ prvky relace $\leq$: vzhledem k definici uspořádání je také vrchol d dosažitelný z vrcholu a a každý ze čtyř prvků množiny W je dosažitelný sám ze sebe. Znaménka $+$ a $-$ označují, ve kterých prvcích množiny W atomy jsou a nejsou splněny. O atomech různých od p a q si můžeme myslet, že nikde splněny nejsou. V tomto modelu platí $b \Vdash \neg p$, protože atom p není splněn v žádném vrcholu dosažitelném z b. Ze všech ostatních vrcholů je ale viditelný vrchol d, ve kterém je splněn atom p. Tedy $x \nVdash \neg p$ pro $x \in \{a, c, d\}$. Podobně lze zjistit, že také formule $q \to \neg p$ je splněna v b a není splněna v a, c ani v d. Její negace $\neg(q \to \neg p)$ je splněna ve vrcholech x s vlastností, že v x ani nikde dál formule $q \to \neg p$ splněna není, což jsou vrcholy c a d. Formule $p \vee \neg p$ je splněna v b, c a v d, není splněna v a.

Lze dokázat, že bychom mohli vystačit s rámci, které z hlediska teorie grafů jsou stromy; nebudeme to ale potřebovat. Přesto si dovolme nejmenší vrchol rámce nazvat *kořenem*. Naopak vrchol s, z kterého nejsou dosažitelné žádné vrcholy různé od s, nazvěme *listem*. Samozřejmě ne každý rámec musí mít kořen nebo listy.

Lemma 5.1.3 *Nechť $\langle W, \leq, \Vdash \rangle$ je kripkovský model, nechť x a y jsou jeho vrcholy takové, že $x \leq y$, nechť A je výroková formule. Když $x \Vdash A$, pak $y \Vdash A$.*

Důkaz ponecháváme za cvičení.

Definice 5.1.4 Sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ platí *v modelu* $\langle W, \leq, \Vdash \rangle$*, jestliže v každém vrcholu* $x \in W$*, ve kterém jsou splněny všechny formule z* Γ*, je splněna také některá formule z* Δ. Sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ *je* intuicionisticky tautologický*, jestliže platí v každém kripkovském modelu.* Formule A platí *v modelu* $\langle W, \leq, \Vdash \rangle$*, jestliže v modelu* $\langle W, \leq, \Vdash \rangle$ *platí sekvent* $\langle\, \Rightarrow\; A \,\rangle$*. Formule* A *je* intuicionistická tautologie*, jestliže sekvent* $\langle\, \Rightarrow\; A \,\rangle$ *je intuicionisticky tautologický, tj. jestliže formule* A *je splněna v každém vrcholu každého kripkovském modelu. Množinu všech intuicionistických tautologií označme* Int-Taut.

Není-li formule A intuicionistickou tautologií, znamená to, že existuje kripkovský model, ve kterém A neplatí. Takový model nazvěme *kripkovským protipříkladem* na formuli A. Podobně *protipříkladem na sekvent* $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je model $\langle W, \leq, \Vdash \rangle$ a jeho vrchol a takový, že v a jsou splněny všechny formule z Γ a nesplněny všechny formule z Δ.

Příklad 5.1.5 Z podmínky pro negaci v definici kripkovského modelu a z reflexivity relace dosažitelnosti plyne, že pro žádný vrchol z libovolného kripkovského modelu a žádnou formuli A neplatí současně $z \Vdash A$ a $z \Vdash \neg A$. Jsou-li x a y vrcholy nějakého kripkovského modelu takové, že $x \leq y$ a $x \Vdash A$, pak z tranzitivity relace $\leq$, z lemmatu 5.1.3 a z předchozí úvahy plyne $z \nVdash \neg A$ pro libovolný vrchol z dosažitelný z y. To dále znamená $y \Vdash \neg A \to B$ pro libovolnou formuli B. Tím je ověřeno, že $x \Vdash A \to (\neg A \to B)$. Protože x byl libovolný vrchol libovolného kripkovského modelu, dokázali jsme, že $A \to (\neg A \to B)$ je intuicionistická tautologie. Podobně lze ověřit, že také každá formule tvaru $A \to \neg\neg A$ je intuicionistická tautologie. Další příklady intuicionistických tautologií jsou $\neg\neg\neg A \to \neg A$ a $\neg\neg(A \vee \neg A)$, a ještě další příklady intuicionistických tautologií jsou uvedeny ve cvičeních. Na druhé straně formule $\neg\neg A \to A$, $A \vee \neg A$ a $(\neg\neg A \to A) \to A \vee \neg A$ nejsou intuisticionistickými tautologiemi: v modelu z obrázku 5.1.1 neplatí formule $\neg\neg q \to q$, $p \vee \neg p$ ani $(\neg\neg p \to p) \to p \vee \neg p$.

Lemma 5.1.6 *Nechť formule* A *není intuicionistickou tautologií. Pak existuje kripkovský model* $\langle W, \leq, \Vdash \rangle$ *a vrchol* $r \in W$ *takové, že* r *je kořenem v rámci* $\langle W, \leq \rangle$ *a* $r \nVdash A$.

Důkaz Není-li formule A intuicionistickou tautologií, existuje model $\langle W', \leq', \Vdash' \rangle$ a vrchol $r \in W'$ takový, že $r \nVdash' A$. Položme $W = \{\, y \in W' \,;\, r \leq' y \,\}$. Relace $\leq$ a $\Vdash$ definujme jako restrikce relací $\leq'$ a $\Vdash'$ na množinu W. Snadno lze ověřit, že konstrukce je korektní a že libovolná formule je v libovolném vrcholu y nového modelu splněna, právě když je v y splněna ve smyslu původního modelu. QED

Předchozí lemma by pochopitelně zůstalo v platnosti, kdybychom místo o formuli mluvili o sekventu. Model vzniklý odstraněním všech vrcholů nedosažitelných z jistého vrcholu r, jehož konstrukce je popsána v předchozím důkazu, se nazývá *model generovaný vrcholem* r.

Je-li *s listem* nějakého kripkovského modelu, pak pravdivostní hodnoty formulí se v *s* vyčíslují „klasicky“. Například implikace $A \to B$ je splněna, právě když B je v s splněna nebo A je v s nesplněna. Z toho plyne, že jednoprvkové kripkovské modely jednoznačně korespondují s pravdivostními ohodnoceními ve smyslu klasické výrokové logiky. Každá intuicionistická tautologie platí ve všech kripkovských modelech, takže i ve všech jednoprvkových modelech, a je tedy tautologií ve smyslu klasické výrokové logiky. Tím jsme zdůvodnili inkluzi Int-Taut $\subseteq$ Taut. Z příkladu 5.1.5 je jasné, že tato inkluze je ostrá. Zatím nevíme, zda Int-Taut je jednodušší nebo složitější úloha než Taut. Nevíme ani, zda je rozhodnutelná. Tím se budeme zabývat v následujícím pododdílu.

5.1.2 Rozhodnutelnost, úplnost, složitost

Podobně jako v sémantice klasické predikátové logiky nenaznačuje definice intuicionistické tautologie žádný algoritmus, který by zjistil, zda daná formule platí ve všech modelech. Kripkovské modely mohou být neomezeně velké nebo i nekonečné. Ukážeme si, že takový algoritmus přesto — a na rozdíl od klasické predikátové logiky — existuje. Algoritmus sestavíme tak, aby rozhodoval o sekventech, ne pouze o jednotlivých formulích. Analýza našeho algoritmu nám pak umožní definovat gentzenovský kalkulus pro intuicionistickou logiku a dokázat jeho úplnost.

Lemma 5.1.7 *V každém řádku následující tabulky:*

$\langle\, \Gamma, A \,\&\, B \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma, A \,\&\, B, A, B \Rightarrow \Delta \,\rangle$
$\langle\, \Gamma, A \vee B \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma, A \vee B, A \Rightarrow \Delta \,\rangle, \quad \langle\, \Gamma, A \vee B, B \Rightarrow \Delta \,\rangle$
$\langle\, \Gamma \Rightarrow \Delta, A \,\&\, B \,\rangle$	$\langle\, \Gamma \Rightarrow \Delta, A \,\&\, B, A \,\rangle, \quad \langle\, \Gamma \Rightarrow \Delta, A \,\&\, B, B \,\rangle$
$\langle\, \Gamma \Rightarrow \Delta, A \vee B \,\rangle$	$\langle\, \Gamma \Rightarrow \Delta, A \vee B, A, B \,\rangle$
$\langle\, \Gamma, A \to B \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma, A \to B \Rightarrow \Delta, A \,\rangle, \quad \langle\, \Gamma, A \to B, B \Rightarrow \Delta \,\rangle$
$\langle\, \Gamma, \neg A \Rightarrow \Delta \,\rangle$	$\langle\, \Gamma, \neg A \Rightarrow \Delta, A \,\rangle$
$\langle\, \Gamma \Rightarrow \Delta, A \to B \,\rangle$	$\langle\, \Gamma \Rightarrow \Delta, A \to B, B \,\rangle$

je sekvent v levém sloupci intuicionisticky tautologický, právě když sekvent v pravém sloupci je intuicionisticky tautologický, resp. když oba sekventy v pravém sloupci jsou intuicionisticky tautologické.

Důkaz Podívejme se například na poslední řádek. Není-li $\langle\, \Gamma \Rightarrow \Delta, A \to B \,\rangle$ intuicionisticky tautologický sekvent, znamená to, že existuje kripkovský model K, v jehož kořenu jsou splněny všechny formule z Γ a není splněna formule $A \to B$ ani žádná z formulí z Δ. Není-li splněna formule $A \to B$, není splněna ani formule B, a K je tedy protipříkladem i na sekvent $\langle\, \Gamma \Rightarrow \Delta, A \to B, B \,\rangle$. Naopak, každý protipříklad na sekvent $\langle\, \Gamma \Rightarrow \Delta, A \to B, B \,\rangle$ je zároveň automaticky protipříkladem na sekvent $\langle\, \Gamma \Rightarrow \Delta, A \to B \,\rangle$. Stejná úvaha platí i pro ostatních šest případů: libovolný kripkovský model je protipříkladem na sekvent v levém sloupci, právě když je protipříkladem na (některý) sekvent v pravém sloupci. QED

Vícenásobným užitím právě dokázaného lemmatu lze otázku, zda daný sekvent je intuicionisticky tautologický, převést na tutéž otázku týkající se sekventů, které jsou uzavřené ve smyslu následující definice. Pak se budeme zabývat uzavřenými sekventy.

Definice 5.1.8 *Sekvent* $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ *je* uzavřený, *jestliže*

- *když* $A \,\&\, B \in \Gamma$ *(resp.* $A \vee B \in \Delta$*), pak* A *i* B *jsou v* Γ *(resp. v* Δ*),*
- *když* $A \vee B \in \Gamma$ *(resp.* $A \,\&\, B \in \Delta$*), pak* A *nebo* B *je v* Γ *(resp. v* Δ*),*
- *když* $A \to B \in \Gamma$*, pak* $B \in \Gamma$ *nebo* $A \in \Delta$*,*
- *když* $\neg A \in \Gamma$*, pak* $A \in \Delta$*,*
- *když* $A \to B \in \Delta$*, pak* $B \in \Delta$*.*

Příklad 5.1.9 Sekvent $\langle\, \Rightarrow \neg\neg p \to p \,\rangle$ není uzavřený, sekventy $\langle\, \Rightarrow \neg\neg p \to p, p \,\rangle$ a $\langle\, p \to q \Rightarrow p, \neg q \,\rangle$ jsou uzavřené. Definice neříká nic o negaci v sukcedentu ani o premise implikace v sukcedentu.

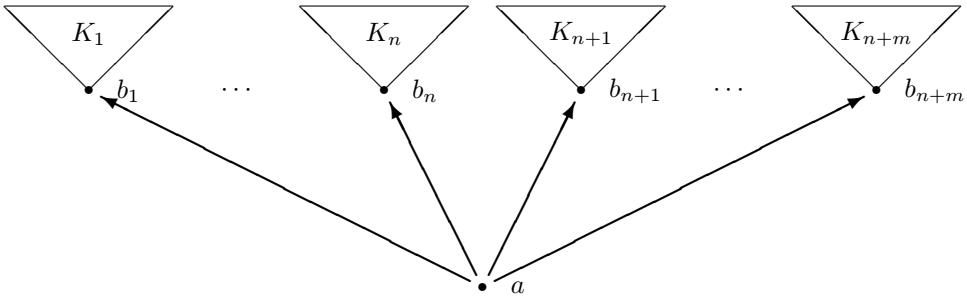
Lemma 5.1.10 *Nechť* $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ *je uzavřený sekvent. Pak* $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ *je intuicionisticky tautologický, právě když je splněna* některá *z následujících podmínek:*

- $\Gamma \cap \Delta \neq \emptyset$*,*
- *existuje formule* $A \to B \in \Delta$ *taková, že* $A \notin \Gamma$ *a sekvent* $\langle\, \Gamma, A \Rightarrow B \,\rangle$ *je intuicionisticky tautologický,*
- *existuje formule* $\neg A \in \Delta$ *taková, že* $A \notin \Gamma$ *a sekvent* $\langle\, \Gamma, A \Rightarrow \,\rangle$ *je intuicionisticky tautologický.*

Důkaz Když $\Gamma \cap \Delta \neq \emptyset$, pak $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je intuicionisticky tautologický sekvent. Zabývejme se podmínkou týkající se implikace, úvaha pro poslední podmínku týkající se negace je podobná. Nechť tedy $A \to B \in \Delta$ a $\langle\, \Gamma, A \Rightarrow B \,\rangle$ je intuicionisticky tautologický sekvent. Ověříme, že sekvent $\langle\, \Gamma \Rightarrow A \to B \,\rangle$ je intuicionisticky tautologický. To bude samozřejmě znamenat, že i sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je intuicionisticky tautologický. Nechť tedy a je libovolný vrchol libovolného kripkovského modelu takový, že $a \Vdash \Gamma$, tj. v a jsou splněny všechny formule z Γ. Máme ověřit $a \Vdash A \to B$, což podle definice znamená ověřit, že B je splněna ve všech vrcholech b dosažitelných z a, ve kterých je splněna formule A. Nechť tedy $a \leq b$ a $b \Vdash A$. Lemma 5.1.3 říká, že v b jsou splněny všechny formule z množiny Γ. Každý vrchol splňující všechny formule z množiny $\Gamma \cup \{A\}$ musí splňovat i formuli B, protože $\langle\, \Gamma, A \Rightarrow B \,\rangle$ je intuicionisticky tautologický sekvent. Tedy $b \Vdash B$.

Uvažujme o implikaci $\Rightarrow$. Předpokládejme, že $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je uzavřený sekvent, který nesplňuje žádnou ze tří podmínek lemmatu. Tedy $\Gamma \cap \Delta = \emptyset$, pro žádnou implikaci $A \to B \in \Delta$ takovou, že $A \notin \Gamma$, sekvent $\langle\, \Gamma, A \Rightarrow B \,\rangle$ není intuicionisticky tautologický a pro žádnou negaci $\neg A \in \Delta$ takovou, že $A \notin \Gamma$, sekvent $\langle\, \Gamma, A \Rightarrow \,\rangle$ není intuicionisticky tautologický. Napišme si seznam

$$A_1 \to B_1, \ldots, A_n \to B_n, \neg C_1, \ldots, \neg C_m$$



Obrázek 5.1.2: Amalgamace kripkovských modelů

všech implikací $A \to B$ v sukcedentu Δ takových, že $A \notin \Gamma$, a všech negací $\neg C$ v Δ takových, že $C \notin \Gamma$. Protože příslušné sekventy nejsou intuicionisticky tautologické, pro každou z těchto formulí můžeme zvolit kripkovský model K_i s kořenem b_i, kde $1 \leq i \leq n+m$, tak, že pro $1 \leq i \leq n$ je model K_i protipříkladem na sekvent $\langle\, \Gamma, A_i \;\Rightarrow\; B_i \,\rangle$ a pro $n+1 \leq i \leq n+m$ je model K_i protipříkladem na sekvent $\langle\, \Gamma, C_{i-n} \;\Rightarrow\, \rangle$. Tedy ve všech kořenech b_i jsou splněny všechny formule z množiny Γ. Navíc pro $1 \leq i \leq m$ platí $b_i \Vdash A_i$ a $b_i \nVdash B_i$, kdežto pro $n+1 \leq i \leq n+m$ platí $b_i \Vdash C_{i-n}$.

Utvořme nyní ze všech modelů K_i a z jednoho nového vrcholu a nový model K tak, jak je znázorněno na obrázku 5.1.2. Vrchol a je v K novým kořenem. To znamená, že z a jsou dosažitelné všechny prvky všech K_i, každý z dosavadních kořenů b_i je dosažitelný jen sám ze sebe a z nového kořenu a. Pravdivostní relaci rozšíříme na nový model K tak, že v a prohlásíme za splněné ty atomy, které jsou v množině Γ, a za nesplněné všechny ostatní. Takováto volba pravdivostních hodnot neporuší podmínku perzistence, neboť všechny atomy v Γ — a vůbec všechny formule v Γ — jsou splněny ve všech vrcholech všech modelů K_i.

O pravdivostních hodnotách formulí $D \in \Gamma \cup \Delta$ v kořenu a platí: *jestliže* $D \in \Gamma$, *pak* $a \Vdash D$, *a jestliže* $D \in \Delta$, *pak* $a \nVdash D$. Toto tvrzení dokážeme indukcí podle složitosti formule D. Když D je atomem a $D \in \Delta$, pak $a \nVdash D$, protože $\Gamma \cap \Delta = \emptyset$ a všechny atomy, které nejsou v Γ, jsme prohlásili za nesplněné v a. Když D je tvaru $E \,\&\, F$ a $D \in \Delta$, pak díky uzavřenosti sekventu $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ jedna z formulí E a F je v Δ, a tedy podle indukčního předpokladu je nesplněna v a. Platí tedy $a \nVdash E \,\&\, F$. Je-li D tvaru $E \to F$ a $D \in \Gamma$, pak opět díky uzavřenosti sekventu $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ platí $F \in \Gamma$ nebo $E \in \Delta$. Podle indukčního předpokladu F je nebo E není splněna v a. Tedy pro $x = a$ platí podmínka $x \nVdash E$ nebo $x \Vdash F$. Je-li $x \in K$ a $x \neq a$, pak pro x tato podmínka platí rovněž, neboť x je dosažitelný z některého b_i a víme $b_i \Vdash E \to F$, model K_i je přece protipříkladem na sekvent obsahující formuli $E \to F$ v antecedentu. Tedy podmínka $x \nVdash E$ nebo $x \Vdash F$ je splněna úplně všude, tedy $a \Vdash E \to F$. Uvažme ještě případ, kdy D je $E \to F$ a $D \in \Delta$. Všechny zbývající případy jsou podobné právě probraným nebo jednodušší. Formule E může nebo nemusí být v Γ. Uvažme obě

možnosti. Nechť $E \in \Gamma$. Víme $F \in \Delta$, to plyne z uzavřenosti sekventu $\langle\, \Gamma \Rightarrow \Delta \,\rangle$. Z indukčního předpokladu plyne, že pro $x = a$ platí $x \Vdash E$ a $x \nVdash F$. Nechť $E \notin \Gamma$. Pak $E \to F$ musí být jedna z formulí $A_i \to B_i$ pro $1 \leq i \leq n$. Protože K_i je protipříklad na sekvent $\langle\, \Gamma, A_i \Rightarrow B_i \,\rangle$, pro $x = b_i$ víme $x \Vdash A_i$ a $x \nVdash B_i$. V obou případech existuje vrchol x dosažitelný z a takový, že $x \Vdash E$ a $x \nVdash F$. Takže $a \nVdash E \to F$.

Můžeme tedy konstatovat, že sestrojený model K je hledaným protipříkladem na sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$. QED

Konstrukce kripkovského modelu z konečně mnoha modelů a jednoho nového vrcholu, která je znázorněna na obrázku 5.1.2 a která se uplatnila v důkazu předchozího lemmatu, se (například v knize [38]) nazývá *amalgamace*.

Na obou předchozích lemmatech lze založit algoritmus, který o libovolném sekventu rozhodne, zda je intuicionisticky tautologický, tj. algoritmus, který rozhoduje úlohu Int-Taut. Důkaz následující věty stejně jako lemmata 5.1.7 a 5.1.10 vznikly přizpůsobením úvah v Ladnerově článku [54], který se zabývá složitostí rozhodovacích procedur pro různé modální logiky. Článek [54] se ale nezabývá intuicionistickou logikou ani sekventovými kalkuly. Připomeňme, že za délku sekventu pokládáme počet výskytů všech logických spojek a výrokových atomů v jeho zápisu.

Věta 5.1.11 *Úloha zjistit, zda daný sekvent je intuicionisticky tautologický, je rozhodnutelná v polynomiálním prostoru. Jinými slovy, platí* Int-Taut $\in$ *PSPACE*.

Důkaz Program rozhodující, zda daný sekvent je intuicionisticky tautologický, lze založit na podprogramu F z obrázku 5.1.3. Podprogram F očekává jako parametry dvě konečné množiny Γ a Δ výrokových formulí. Podprogram je deklarován jako booleovská funkce. To znamená, že výsledkem jeho činnosti je odpověď ano nebo ne. Tvrdíme, že podprogram se dopočítá na každém vstupu, při zpracování vstupu $[\Gamma, \Delta]$ vystačí s prostorem polynomiálním v délce vstupu a jeho odpověď je správnou odpovědí na otázku, zda $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je intuicionisticky tautologický sekvent.

Podprogram využívá rekurzívní volání sama sebe. Například v řádku L2 volá sám sebe dvakrát, pokaždé na jiná data, a výsledkem výpočtu je logický součin (konjunkce) obou odpovědí vyjádřený slovem `and`. Příkaz `return` V ovšem znamená „skonči a vydej výsledek V“.

Bez rekurzívního volání se podprogram obejde v řádku L8: je-li $\Gamma \cap \Delta \neq \emptyset$, pak výsledek je `true`, tj. ano, sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je intuicionisticky tautologický. Odpověď `false` v podprogramu vidět není, ale je skryta v důležitém řádku L9. Tam je výsledek výpočtu stanoven jako disjunkce (vyjádřená dvěma symboly $\bigvee$ a slovem `or`) dílčích výsledků, jejichž počet může být různý, a to i nulový (v případě, kdy pro všechny implikace $A \to B$ v Δ a pro všechny negace $\neg A$ v Δ platí $A \in \Gamma$). A disjunkce nulového počtu booleovských hodnot je `false`.

```
boolean function F(Γ, Δ)
    if  některá formule v Γ porušuje uzavřenost sekventu ⟨ Γ ⇒ Δ ⟩  then
      zvol formuli D ∈ Γ, která porušuje uzavřenost
L1:   if D = A & B  then return F(Γ ∪ {A, B}, Δ)
L2:   if D = A ∨ B  then return [F(Γ ∪ {A}, Δ) and F(Γ ∪ {B}, Δ)]
L3:   if D = A → B  then return [F(Γ, Δ ∪ {A}) and F(Γ ∪ {B}, Δ)]
L4:   if D = ¬A     then return F(Γ, Δ ∪ {A})
    endif
    if  některá formule v Δ porušuje uzavřenost sekventu ⟨ Γ ⇒ Δ ⟩  then
      zvol formuli D ∈ Δ, která porušuje uzavřenost
L5:   if D = A ∨ B  then return F(Γ, Δ ∪ {A, B})
L6:   if D = A & B  then return [F(Γ, Δ ∪ {A}) and F(Γ, Δ ∪ {B})]
L7:   if D = A → B  then return F(Γ, Δ ∪ {B})
    endif
L8: if  Γ ∩ Δ ≠ ∅  then return true
L9: return [⋁_{A→B∈Δ, A∉Γ} F(Γ ∪ {A}, {B}) or ⋁_{¬A∈Δ, A∉Γ} F(Γ ∪ {A}, ∅)]
endfunction
```

Obrázek 5.1.3: Rozhodnutelnost intuicionistické výrokové logiky

Podprogram tedy pracuje tak, že otázku týkající se daného sekventu převádí na tutéž otázku nebo otázky týkající se jiných sekventů, a to buď užitím lemmatu 5.1.7 (v řádcích L1–L7), nebo užitím lemmatu 5.1.10 (v řádcích L8 a L9). Celý výpočet si můžeme představit jako strom, jehož vrcholy jsou ohodnoceny různými daty tvaru $[\Gamma, \Delta]$. Vrchol s ohodnocením $[\Gamma, \Delta]$ reprezentuje kopii našeho podprogramu, která má rozhodnout o logické pravdivosti sekventu $\langle\, \Gamma \Rightarrow \Delta \,\rangle$. Udělá to tak, že aktivuje další — podřazené — kopie, a svůj výsledek, který předá nadřazené kopii nebo hlavnímu programu, získá jako logický součet nebo součin jejich výsledků.

Tvrdíme, že všechny větve výpočtu dospějí po konečném a předem odhadnutelném počtu kroků buď k uzavřenému sekventu $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ takovému, že $\Gamma \cap \Delta = \emptyset$ a pro všechny implikace $A \to B \in \Delta$ platí $A \in \Gamma$ a pro všechny negace $\neg C \in \Delta$ platí $C \in \Gamma$ (ten podle lemmatu 5.1.10 není intuicionisticky tautologický), nebo k sekventu $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ takovému, že $\Gamma \cap \Delta \neq \emptyset$ (ten je intuicionisticky tautologický).

Předpokládejme, že vstupní data podprogramu F mají délku n, a všimněme si, jak se mění obsah množin Γ a Δ podél jedné větve výpočtu. Množina Δ se cestou od kořene směrem do hloubi stromu může zvětšovat (před voláním podprogramu F do ní může být přidána jedna nebo dvě formule) nebo zmenšovat (před voláním podprogramu F v řádku L9 jsou z ní odstraněny všechny formule nebo všechny až na jednu). Žádný z řádků L1–L9 ale nikdy neodstraní žádnou formuli z množiny Γ. Ta se může pouze zvětšovat a určitě se zvětší, je-li použit řádek L9.

Všechny formule ve hře jsou podformulemi některé formule v původním sekventu a je jich nejvýše n. Z toho usuzujeme, že na každé větvi výpočtu je nejvýše n uzavřených sekventů, protože každý další má v Γ nejméně o jednu formuli více, a

že vzdálenost od jednoho uzavřeného sekventu k druhému je také nejvýše n, protože každý z řádků L1–L7 vždy přidá alespoň jednu formuli do množiny $\Gamma \cup \Delta$.

Tím jsme zdůvodnili, že podprogram F se na každém vstupu dopočítá, neboť každá větev výpočtu je konečná a má délku $\mathcal{O}(n^2)$, kde n je délka vstupních dat. Každá kopie podprogramu F vystačí s lokálními daty velikosti $\mathcal{O}(n^2)$, což je maximální možná délka seznamu všech podformulí nějakého sekventu délky n. Z oddílu 2.1 víme, že souhrnná velikost paměťového prostoru je dána souhrnnou velikostí lokálních dat všech kopií podprogramu podél jedné větve výpočtu. Tím je dokázáno, že podprogram F vystačí s paměťovým prostorem velikosti $\mathcal{O}(n^4)$. QED

$$\dfrac{\dfrac{\dfrac{\dfrac{\langle B \Rightarrow B\rangle}{\langle B \Rightarrow \neg A \vee B\rangle}}{\langle \neg(\neg A \vee B), B \Rightarrow \rangle}}{\langle \neg(\neg A \vee B) \Rightarrow \neg B\rangle} \qquad \dfrac{\dfrac{\langle A \Rightarrow A\rangle \quad \dfrac{\langle B \Rightarrow B\rangle}{\langle B, \neg B \Rightarrow \rangle}}{\langle A \to B, \neg B, A \Rightarrow \rangle}}{\langle A \to B, \neg B \Rightarrow \neg A\rangle} \qquad \dfrac{\dfrac{\langle \neg A \Rightarrow \neg A\rangle}{\langle \neg A \Rightarrow \neg A \vee B\rangle}}{\langle \neg(\neg A \vee B), \neg A \Rightarrow \rangle}}{\dfrac{\langle \neg(\neg A \vee B), A \to B, \neg B \Rightarrow \rangle}{\dfrac{\langle \neg(\neg A \vee B), A \to B \Rightarrow \rangle}{\langle \neg(\neg A \vee B) \Rightarrow \neg(A \to B)\rangle}}}$$

Obrázek 5.1.4: Důkaz v intuicionistickém gentzenovském kalkulu

Nyní jsme připraveni definovat *gentzenovský kalkulus* pro intuicionistickou výrokovou logiku. Některá z pravidel kalkulu GK pro klasickou výrokovou logiku uvedených v oddílu 1.4 jsou korektní i vůči kripkovské sémantice intuicionistické logiky (ověření ponecháváme jako cvičení) a můžeme je beze změny převzít i do kalkulu pro intuicionistickou logiku. Jsou to pravidla A, W, Cut, $\to$-l, $\neg$-l a všechna čtyři pravidla pro konjunkci a disjunkci. K nim přidáme modifikovaná pravidla pro zavedení implikace a negace do sukcedentu:

$\to$-rI: $\quad \langle \Gamma, A \Rightarrow B\rangle \;/\; \langle \Gamma \Rightarrow A \to B\rangle$,

$\neg$-rI: $\quad \langle \Gamma, A \Rightarrow \rangle \;/\; \langle \Gamma \Rightarrow \neg A\rangle$,

$\to$-w: $\quad \langle \Gamma \Rightarrow \Delta, B\rangle \;/\; \langle \Gamma \Rightarrow \Delta, A \to B\rangle$.

Pravidlo $\to$-w nazvěme *slabým pravidlem pro zavedení implikace*. Zbývající dvě pravidla jsou téměř shodná s pravidly pro klasickou výrokovou logiku až na důležitý rozdíl, že v sukcedentu se nepřipouštějí postranní formule. O těchto dvou pravidlech se někdy mluví jako o *kritických*. Jsou použitelná jen tak, že po jejich použití je sukcedent jednoprvkový. Ověření korektnosti těchto pravidel ponecháváme opět jako cvičení, ale důkazy korektnosti většiny pravidel jsou vlastně obsaženy v důkazech lemmat 5.1.7 a 5.1.10.

Kalkulus GJ, gentzenovský kalkulus pro intuicionistickou výrokovou logiku, tedy definujeme jako kalkulus s pravidly A, W, Cut, $\to$-l, $\neg$-l, &-l, $\vee$-l, &-r a $\vee$-r převzatými z kalkulu GK a s právě definovanými pravidly $\to$-w, $\to$-rI a $\neg$-rI.

Na obrázku 5.1.4 je uveden příklad důkazu v kalkulu GJ. Jsou v něm použity dva řezy, nejprve na formuli $\neg A$ a pak na formuli $\neg B$. Následující věta tvrdí, že týž sekvent má i bezřezový důkaz. A dále následující věta tvrdí, že sekvent, který má jakýkoliv kripkovský protipříklad, má i konečný protipříklad. Tato vlastnost se obecně, tj. v souvislosti s logikami připouštějícími kripkovskou sémantiku, nazývá vlastnost konečných modelů a označuje se zkratkou FMP, *finite model property*.

Věta 5.1.12 (úplnost kalkulu GJ) *Každý intuicionisticky tautologický sekvent délky n má bezřezový důkaz hloubky $\mathcal{O}(n^3)$. Každý sekvent délky n, který není intuicionisticky tautologický, má kripkovský protipříklad hloubky nejvýše n, v němž každý vrchol má nejvýše n následníků. Kalkulus GJ je tedy úplný vůči kripkovské sémantice intuicionistické logiky a platí pro něj věta o eliminovatelnosti řezů. Intuicionistická výroková logika má vlastnost FMP.*

Důkaz Vraťme se k důkazu věty 5.1.11. Víme, že výpočet, který má rozhodnout o sekventu $\langle\, \Sigma \;\Rightarrow\; \Omega \,\rangle$, si můžeme představit jako strom, jehož každý vrchol je ohodnocen daty tvaru $[\Gamma, \Delta]$, která reprezentují otázku, zda sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je intuicionisticky tautologický. Označme tento strom $\mathcal{T}$. Víme, že má-li sekvent $\langle\, \Sigma \;\Rightarrow\; \Omega \,\rangle$ délku n, pak strom $\mathcal{T}$ má hloubku $\mathcal{O}(n^2)$. Rozmysleme si, že strom $\mathcal{T}$ lze přepracovat buď na důkaz sekventu $\langle\, \Sigma \;\Rightarrow\; \Omega \,\rangle$ v kalkulu GJ, nebo na kripkovský protipříklad na sekvent $\langle\, \Sigma \;\Rightarrow\; \Omega \,\rangle$.

Rozdělme sekventy stromu $\mathcal{T}$ na pozitivní a negativní podle toho, zda podprogram F po jejich zpracování odpověděl ano nebo ne. Každý sekvent stromu $\mathcal{T}$ je nebo není uzavřený, přičemž všechny listy jsou uzavřené. Je-li sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ listem stromu $\mathcal{T}$, pak je pozitivní právě tehdy, když $\Gamma \cap \Delta \neq \emptyset$. Není-li uzavřený sekvent listem, pak je pozitivní právě tehdy, je-li *některý* z jeho následníků pozitivní. Neuzavřený sekvent má jednoho nebo dva následníky a je pozitivní právě tehdy, když *každý* z jeho následníků je pozitivní.

Předpokládejme, že výsledek celého výpočtu je ANO. Pak kořen $\langle\, \Sigma \;\Rightarrow\; \Omega \,\rangle$ stromu $\mathcal{T}$ je pozitivní, čili sekvent $\langle\, \Sigma \;\Rightarrow\; \Omega \,\rangle$ je intuicionisticky tautologický. Odstraňme ze stromu $\mathcal{T}$ každý podstrom, jehož kořen je negativní. Odstraňme případně ještě další podstromy tak, aby každý uzavřený sekvent, který není listem, měl právě jednoho následníka. Probráním všech případů lze ověřit, že každý vrchol stromu $\mathcal{T}$ lze nejvýše n kroky a bez užití řezů odvodit v kalkulu GJ z jeho následníků. To znamená, že strom $\mathcal{T}$ lze doplnit na bezřezový důkaz $\mathcal{P}$ sekventu $\langle\, \Sigma \;\Rightarrow\; \Omega \,\rangle$ v kalkulu GJ, jehož hloubka je $\mathcal{O}(n^3)$. Například je-li $\mathcal{S}$ neuzavřený sekvent tvaru $\langle\, \Gamma, \neg A \;\Rightarrow\; \Delta \,\rangle$ a $\neg A$ je ona formule D, kterou si podprogram F zvolil mezi formulemi porušujícími uzavřenost, pak sekvent $\langle\, \Gamma, \neg A \;\Rightarrow\; \Delta \,\rangle$ má jednoho následníka $\langle\, \Gamma, \neg A \;\Rightarrow\; \Delta, A \,\rangle$, a opravdu jej z tohoto následníka lze odvodit jedním užitím pravidla $\neg$-l. Je-li $\mathcal{S}$ uzavřený sekvent, který není listem, pak $\mathcal{S}$ má tvar $\langle\, \Gamma \;\Rightarrow\; A_1 \to B_1, \ldots, A_n \to B_n, \neg C_1, \ldots, \neg C_m, \Pi \,\rangle$, kde pro každou implikaci $E \to F \in \Pi$ platí $E \in \Gamma$ a pro každou negaci $\neg E \in \Pi$ platí $E \in \Gamma$. Sekvent $\mathcal{S}$ má jediného následníka $\mathcal{S}'$ tvaru $\langle\, \Gamma, A_i \;\Rightarrow\; B_i \,\rangle$ nebo $\langle\, \Gamma, C_j \;\Rightarrow\, \rangle$. V tom případě

můžeme sekvent $\mathcal{S}$ odvodit ze sekventu $\mathcal{S}'$ tak, že užijeme pravidlo $\to$-rI resp. $\neg$-rI, a zbývající formule pak do sukcedentu přidáme pomocí pravidla W.

Předpokládejme, že výsledek celého výpočtu je NE. Pak kořen $\langle\, \Sigma \Rightarrow \Omega \,\rangle$ stromu $\mathcal{T}$ je negativní, čili sekvent $\langle\, \Sigma \Rightarrow \Omega \,\rangle$ není intuicionisticky tautologický. Jestliže podprogram F vyhodnotil některý sekvent $\mathcal{S}$ stromu $\mathcal{T}$ jako negativní, znamená to, že při jeho zpracování buď dostal odpověď ne při některém volání sebe sama v řádcích L1–L7, nebo použil řádek L9 a při všech voláních sebe sama dostal odpověď ne. Libovolný kripkovský protipříklad na kterýkoliv ze sekventů, které jsou ve hře při volání podprogramu F v řádcích L1–L7, je zároveň kripkovským protipříkladem na sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$. Indukční předpoklad říká, že každý z těchto (nejvýše dvou) sekventů *má* kripkovský protipříklad. Tedy $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ má protipříklad, a to ne větší hloubky. Byl-li použit řádek L9 a všechny odpovědi byly ne, pak všechny sekventy ve hře mají protipříklad (to je indukční předpoklad), a z důkazu lemmatu 5.1.10 plyne, že sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ má protipříklad hloubky o jedna větší, než je maximální hloubka těchto protipříkladů. Dohromady to znamená, že sekvent $\langle\, \Sigma \Rightarrow \Omega \,\rangle$ má protipříklad, jehož hloubka je omezena maximálním počtem užití řádku L9 na jedné větvi výpočtu, což je nejvýše n. QED

Příklad 5.1.13 Vezměme sekvent $\langle\, (p \to q) \vee (q \to p) \to q \;\Rightarrow\; q \,\rangle$ a podívejme se, jak jej zpracuje podprogram z obrázku 5.1.3 a co to znamená z hlediska věty 5.1.12. Označme D formuli $(p \to q) \vee (q \to p)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots \qquad\qquad \vdots}{\langle\, D \to q, p \;\Rightarrow\; q \,\rangle^{(6)} \qquad \langle\, D \to q, q \;\Rightarrow\; p \,\rangle^{(7)}}}{\langle\, D \to q \;\Rightarrow\; q, D, p \to q, q \to p, p \,\rangle^{(5)}}}{\langle\, D \to q \;\Rightarrow\; q, D, p \to q, q \to p \,\rangle^{(4)}}}{\langle\, D \to q \;\Rightarrow\; q, D \,\rangle^{(3)}} \qquad \langle\, D \to q, q \;\Rightarrow\; q \,\rangle^{(2)}}{\langle\, D \to q \;\Rightarrow\; q \,\rangle^{(1)}}.$$

Podprogram nejprve uplatnil řádky L3, L5 a L7, a tím dospěl k uzavřeným sekventům (2) a (5). Sekvent (2) je pozitivní, neboť jeho antecedent a sukcedent mají neprázdný průnik. Při zpracování sekventu (5) podprogram uplatnil řádek L9 a získal sekventy (6) a (7). Snadno lze ověřit, že dalším zpracováním sekventu (6), tj. opětovným užitím řádků L3, L5, L7 a L9, se zjistí, že sekvent (6) je pozitivní. Řádek L9 tedy vyhodnotí sekvent (5) jako pozitivní, a to bez ohledu na to, jaký je sekvent (7) (je ale negativní). Takže i sekventy (5), (4) a (3) jsou pozitivní a řádek L3 vyhodnotí sekvent (1) jako pozitivní. Důkaz sekventu (1) v kalkulu GJ získáme tak, že odstraníme podstrom, v jehož kořenu je sekvent (7), mezi sekventy (4) a (3) přidáme jeden nový sekvent $\langle\, D \to q \;\Rightarrow\; q, D, p \to q \,\rangle$, protože k odstranění formulí $p \to q$ a $q \to p$ je třeba užít pravidlo $\vee$-r dvakrát, a mezi sekventy (6) a (5) přidáme několik dalších sekventů, protože sekvent (5) lze získat ze sekventu (6) jedním užitím pravidla $\to$-rI a čtyřnásobným užitím pravidla W. Podobné úpravy je ovšem třeba provést také v podstromu, v jehož kořenu je sekvent (6). Je jasné, že

kdybychom byli formulovali pravidlo W tak, aby umožňovalo přidat několik formulí najednou, odhad $\mathcal{O}(n^3)$ ve větě 5.1.12 bychom mohli nahradit odhadem $\mathcal{O}(n^2)$.

Příklad 5.1.14 Označme $\mathcal{S}$ sekvent $\langle \Rightarrow p \to q, q \to p, p, q \rangle$. Při zpracování sekventu $\mathcal{S}$ podprogram z obrázku 5.1.3 uplatní řádek L9, zavolá sám sebe na sekventy $\langle p \Rightarrow q \rangle$ a $\langle q \Rightarrow p \rangle$ a zjistí, že oba jsou negativní, takže i sekvent $\mathcal{S}$ vyhodnotí jako negativní. Všechny tři sekventy $\mathcal{S}$, $\langle p \Rightarrow q \rangle$ a $\langle q \Rightarrow p \rangle$ jsou uzavřené a dávají tříprvkový protipříklad na sekvent $\mathcal{S}$: kořen modelu má dva následníky, v jednom je splněna formule p a není splněna formule q, v druhém je naopak splněna formule q a není splněna formule p.

V knihách [91] a [49] se uvažuje kalkulus GJ^1, ve kterém se v sukcedentu nikdy (nejen u kritických pravidel) nepřipouští více než jedna formule a ve kterém není pravidlo $\to$-w. Lze dokázat (cvičení 15 a 16), že jakýkoliv důkaz v našem kalkulu je simulovatelný užitím řezů v kalkulu GJ^1. Kalkuly GJ a GJ^1 jsou ekvivalentní a navzájem polynomiálně simulovatelné. Protože v [91] i v [49] je dokázáno, že i pro kalkulus GJ^1 platí věta o eliminovatelnosti řezů, je jasné, že i bezřezové verze kalkulů GJ a GJ^1 jsou spolu ekvivalentní. Nevíme, zda kalkulus GJ bez pravidla Cut a bez pravidla $\to$-w polynomiálně simuluje kalkulus GJ bez pravidla Cut. Jinými slovy, nevíme, zda pravidlo $\to$-w, které jsme si vymysleli, může některé bezřezové důkazy nějak výrazněji zkrátit.

K volbě pravidel gentzenovského kalkulu ještě poznamenejme toto. Některá z pravidel se dvěma předpoklady, totiž pravidla $\vee$-l a &-r, jsme formulovali se dvěma množinami postranních formulí. Takto formulovaným pravidlům se v [94] říká *pravidla se sdíleným kontextem*. Takové pravidlo lze aplikovat na dvojici sekventů pouze tehdy, mají-li oba tutéž množinu postranních formulí v sukcedentu a současně tutéž množinu postranních formulí v antecedentu. Zbývající pravidla se dvěma předpoklady, totiž $\to$-l a Cut, jsme formulovali jako kontextově nezávislá, tj. se čtyřmi množinami postranních formulí. Nyní je jasné, proč je to užitečné. Kdybychom pravidlo $\to$-l formulovali jako pravidlo se sdíleným kontextem:

$$\to\text{-l:} \qquad \langle \Gamma \Rightarrow \Delta, A \rangle, \langle \Gamma, B \Rightarrow \Delta \rangle \;/\; \langle \Gamma, A \to B \Rightarrow \Delta \rangle,$$

nemohli bychom například sekvent $\langle p, p \to q \Rightarrow q \rangle$ odvodit bezřezovým důkazem, který v žádném sukcedentu nemá více než jednu formuli. Na druhé straně kdybychom se nechtěli zmínit i o kalkulu GJ^1, nevadilo by formulovat všechna pravidla jako pravidla se sdíleným kontextem.

Hilbertovský kalkulus HJ pro intuicionistickou výrokovou logiku lze získat tak (uvádíme verzi z knihy [49]), že schéma A3 kalkulu HK nahradíme následujícím schématem A3I a přidáme jedno nové schéma A8:

$$\text{A3I:} \qquad (A \to B) \to ((A \to \neg B) \to \neg A),$$

$$\text{A8:} \qquad A \to (\neg A \to B).$$

Kalkuly HK a HJ mají tedy společná schémata A1, A2 a A4–A7 (viz oddíl 1.3) a shodně mají jediné odvozovací pravidlo MP. Schéma A8 vyjadřuje princip „ze sporu

plyne cokoliv“, tj. princip ex falso, o kterém jsme se zmínili v úvodu. Schéma A3I říká, že pokud z A plyne spor, pak A neplatí, tj. platí $\neg A$. To je slabší princip, než „pokud z $\neg A$ plyne spor, pak A“, který je vyjádřen schématem A3 klasické výrokové logiky. Ze schématu A3I plyne pouze toto: pokud z $\neg A$ plyne spor, pak $\neg\neg A$.

Kalkuly GJ a HJ jsou ekvivalentní a vzájemně polynomiálně simulovatelné. Kalkulus HJ je tedy také úplný vůči kripkovské sémantice. Přidáme-li ke kalkulu HJ buď schéma $\neg\neg A \to A$, nebo schéma $A \vee \neg A$, dostaneme kalkulus ekvivalentní s kalkulem pro klasickou výrokovou logiku. Ověření těchto faktů ponecháváme za cvičení.

Vraťme se nyní ke kripkovské sémantice a uvažujme o vzájemném vztahu klasické a intuicionistické logiky.

Věta 5.1.15 *(a) Formule A je tautologie (klasické výrokové logiky), právě když formule $\neg\neg A$ je intuicionistická tautologie.*
(b) Formule $B \to A$ je tautologie, právě když formule $B \to \neg\neg A$ je intuicionistická tautologie.

Důkaz Samozřejmě (a) plyne z (b) a v obou tvrzeních platí implikace $\Leftarrow$: když například $\neg\neg A$ je intuicionistickou tautologií, pak je i klasickou tautologií, a v klasické logice je $\neg\neg A$ ekvivalentní s A. Soustřeďme se tedy na implikaci $\Rightarrow$ v (b). Nechť $B \to \neg\neg A$ není intuicionistickou tautologií. To znamená, že existuje kripkovský model $K = \langle W, \leq, \Vdash\rangle$ a jeho vrchol a takový, že $a \not\Vdash B \to \neg\neg A$. Podle věty o úplnosti vůči kripkovské sémantice můžeme předpokládat, že model K je konečný. Podmínka $a \not\Vdash B \to \neg\neg A$ znamená existenci vrcholu b takového, že $a \leq b$, $b \Vdash B$ a $b \Vdash \neg A$. To dále znamená, že pro každý vrchol $c \geq b$ platí $c \not\Vdash A$. Protože model je konečný, existuje vrchol $c \geq b$, který je v $\langle W, \leq, \Vdash\rangle$ listem, tj. z něhož není dosažitelný žádný vrchol kromě něj samého. Víme, že v listech se pravdivostní hodnoty formulí vyčíslují klasicky. To znamená, že pravdivostní hodnoty formulí ve vrcholu c určují pravdivostní ohodnocení e (ve smyslu klasické logiky) takové, že $e \not\models A$. Díky podmínce perzistence platí ovšem $c \Vdash B$ a $e \models B$. Formule $B \to A$ tedy opravdu není klasickou tautologií. QED

Na tvrzení z předchozí věty se můžeme dívat z hlediska algoritmů a úloh, nebo z hlediska logiky. Funkce $A \mapsto \neg\neg A$ je samozřejmě vyčíslitelná v logaritmickém prostoru. Ekvivalence

$$A \in \textsc{Taut} \Leftrightarrow \neg\neg A \in \textsc{Int-Taut}$$

tedy znamená, že $\textsc{Taut} \leq_{\mathrm{m}}^{\log} \textsc{Int-Taut}$, takže úloha Int-Taut je *coNP*-těžkou úlohou. V dalším dokážeme, že platí víc. Tvrzení, že Int-Taut je úloha rozhodnutelná v *PSPACE*, které jsme získali zároveň s větou o úplnosti pro kalkulus GJ, pravděpodobně nelze zlepšit, neboť úloha Int-Taut je *PSPACE*-kompletní.

Z logického hlediska lze předchozí větu chápat tak, že klasická logika je vlastně obsažena v intuicionistické: kdo ví, co jsou intuicionistické tautologie, má také

plnou informaci o tom, které formule jsou klasickými tautologiemi. Ze dvou logik slabší je vlastně bohatší a v uvedeném smyslu v sobě obsahuje tu silnější.

Vztah mezi klasickou logikou a intuicionistickou logikou se vyjadřuje slovy „klasická logika je *interpretovatelná* v intuicionistické“, funkce $A \mapsto \neg\neg A$ je *interpretace* nebo *překlad*. Není to jediný takový překlad, trochu jiný překlad budeme uvažovat ve cvičeních. V pododdílu o intuicionistické predikátové logice si ukážeme, že i klasická predikátová logika je interpretovatelná v intuicionistické, ale nikoliv prostřednictvím funkce $A \mapsto \neg\neg A$. V predikátové logice není pravda, že pouhým připsáním dvojné negace dostaneme z klasicky logicky platné formule formuli intuicionisticky logicky platnou.

Následující větu dokázal Statman, [87], v r. 1979. Uvádíme vlastní důkaz, který je inspirován Ladnerovým článkem [54], vznikl nezávisle na Statmanově důkazu, je mu ale v lecčem podobný. V [87] je navíc dokázáno, že Int-Taut zůstane *PSPACE*-kompletní úlohou i v případě, omezíme-li se jen na výrokové formule neobsahující jiné logické spojky než implikaci. Domněnka vyslovená v [54], že Int-Taut je v *coNP*, je tedy (za předpokladu, že $NP \neq PSPACE$) nesprávná.

Věta 5.1.16 *Úloha* Int-Taut *je PSPACE-kompletní.*

Důkaz Máme zvolit některou *PSPACE*-kompletní úlohu a logaritmickým převodem ji převést na úlohu Int-Taut. Z oddílu 2.3 víme, že úloha QBF i její komplement $\overline{\text{QBF}}$ jsou *PSPACE*-kompletními úlohami. Z cvičení 20 oddílu 2.3 dále víme, že stačí uvažovat pouze kvantifikované výrokové formule tvaru $Q_m p_m \,..\, Q_1 p_1 B$, kde každý ze symbolů $Q_1, \ldots, Q_m$ je jeden z kvantifikátorů $\forall$ nebo $\exists$ a formule B neobsahuje další výrokové kvantifikátory ani jiné atomy než $p_1, \ldots, p_m$. Každou formuli A tohoto tvaru máme tedy v logaritmickém prostoru přepracovat na výrokovou formuli A^* tak, aby platila podmínka, že A je logicky platná (v tom smyslu, že je splněna některým čili každým pravdivostním ohodnocením), právě když A^* *není* intuicionistická tautologie. Z cvičení 20 oddílu 2.3 také víme, že bychom navíc mohli předpokládat, že v kvantifikátorovém prefixu $Q_m p_m \,..\, Q_1 p_1$ formule A se střídají existenční a univerzální kvantifikátory, první z nich je existenční a jejich počet m je sudý. To ale nebudeme potřebovat.

Nechť je tedy dána kvantifikovaná výroková formule A tvaru $Q_m p_m \,..\, Q_1 p_1 B(\underline{p})$, kde každý ze symbolů $Q_1, \ldots, Q_m$ je jeden z kvantifikátorů $\forall$ nebo $\exists$ a formule B neobsahuje kvantifikátory ani jiné atomy než $p_1, \ldots, p_m$. Formule A_j^* a A^* sestrojíme následující rekurzí podle j:

$$\begin{aligned} A_0^* &= \neg B(\underline{p}) \\ A_j^* &= \begin{cases} (p_j \vee \neg p_j) \to A_{j-1}^* & \text{pokud } Q_j = \exists \\ (A_{j-1}^* \to q_j) \to ((p_j \to q_j) \vee (\neg p_j \to q_j)) & \text{pokud } Q_j = \forall \end{cases} \\ A^* &= A_m^*, \end{aligned}$$

kde prostřední řádek platí pro $1 \leq j \leq m$. Každá formule A_j^* je sestavena z atomů $p_1, \ldots, p_m$ a případně nových pomocných atomů $q_1, \ldots, q_j$. O atomu q_j

lze uvažovat jako o zkratce pro formuli A^*_{j-1}. Pro následující sublemma bychom mohli vystačit i s jednodušší definicí formule A^*_j, totiž

$$A^*_j \quad = \quad \begin{cases} (p_j \vee \neg p_j) \to A^*_{j-1} & \text{pokud } Q_j = \exists \\ (p_j \to A^*_{j-1}) \vee (\neg p_j \to A^*_{j-1}) & \text{pokud } Q_j = \forall. \end{cases}$$

Potíž je v tom, že dvojnásobný výskyt formule A^*_{j-1} v A^*_j by mohl znamenat, že délka formule A^*_j roste s j exponenciálně, a nemohli bychom tedy tvrdit, že $A \mapsto A^*$ je funkce počitatelná v logaritmickém prostoru (nebo v polynomiálním čase).

Sublemma *Nechť e je libovolné pravdivostní ohodnocení atomů $p_{j+1}, .., p_m$. Pak $e \models Q_j p_j \,..\, Q_1 p_1 B(\underline{p})$, právě když existuje kripkovský protipříklad na formuli A^*_j, ve kterém jsou atomy $p_{j+1}, .., p_m$ ohodnoceny (ve všech vrcholech shodně) podle e.*

Toto sublemma dokažme indukcí podle j. Je-li $j = 0$ a $e \models Q_j p_j \,..\, Q_1 p_1 B(\underline{p})$, tj. $e \models B(\underline{p})$, pak jednoprvkový kripkovský model, ve kterém atomy $p_1, .., p_m$ ohodnotíme dle e, bude protipříkladem na formuli $\neg B(\underline{p})$, tj. na formuli A^*_0. Nechť naopak $j = 0$ a K je protipříklad na formuli $\neg B(\underline{p})$, v němž všechny atomy $p_1, .., p_m$ jsou ohodnoceny všude shodně dle e. Model K sice nemusí být jednoprvkový, ale nic zajímavějšího než v jednoprvkovém modelu se v něm stát nemůže. Nejen atomy, ale ani žádné jiné formule v něm nemění pravdivostní hodnotu, formule $B(\underline{p})$ v modelu K platí a ohodnocení e ji (v klasickém smyslu) splňuje.

Nechť $j > 0$, pro $j - 1$ tvrzení platí a nechť e je ohodnocení atomů $p_{j+1}, .., p_m$ takové, že $e \models Q_j p_j \,..\, Q_1 p_1 B(\underline{p})$. Uvažujme nejprve případ $Q_j = \exists$. Podmínka $e \models \exists p_j \,..\, Q_1 p_1 B(\underline{p})$ znamená, že alespoň jedno z obou ohodnocení $1^\frown e$ a $0^\frown e$, která rozšiřují e na atom p_j, splňuje formuli $Q_{j-1} p_{j-1} \,..\, Q_1 p_1 B(\underline{p})$. Indukční předpoklad říká, že existuje kripkovský protipříklad K na formuli A^*_{j-1}, ve kterém jsou atomy $p_j, .., p_m$ ohodnoceny všude shodně dle $1^\frown e$ nebo dle $0^\frown e$. Označme b onen vrchol modelu K, pro který platí $b \nVdash A^*_{j-1}$. Atomy $p_{j+1}, .., p_m$ jsou všude ohodnoceny dle e. Atom p_j je ohodnocen nějak, ale všude shodně. Tedy $b \Vdash p_j \vee \neg p_j$ a $b \nVdash A^*_j$. Model K je hledaným protipříkladem na formuli A^*_j.

Nechť $j > 0$, $Q_j = \forall$ a nechť dále e je ohodnocení atomů $p_{j+1}, .., p_m$ takové, že $e \models \forall p_j \,..\, Q_1 p_1 B(\underline{p})$. Tedy obě rozšíření $1^\frown e$ a $0^\frown e$ ohodnocení e na atom p_j splňují formuli $Q_{j-1} p_{j-1} \,..\, Q_1 p_1 B(\underline{p})$. Indukční předpoklad říká, že existují kripkovské protipříklady K_1 a K_0 a jejich vrcholy b_1 a b_0 takové, že b_1 v K_1 nesplňuje formuli A^*_{j-1}, b_0 v K_0 nesplňuje A^*_{j-1}, atomy $p_{j+1}, .., p_m$ jsou ve všech vrcholech obou modelů ohodnoceny shodně dle e, atom p_j je v K_1 ohodnocen všude kladně a v K_0 všude záporně. Předpokládejme, že b_1 je kořenem v K_1, b_0 je kořenem v K_0, a utvořme nový model K přidáním nového kořenu a jako na obrázku 5.1.2. Musíme ještě stanovit pravdivostní hodnoty všech atomů vyskytujících se v A^*_j, tedy atomů $p_1, .., p_m$ a $q_1, .., q_j$, v novém kořenu a, a také pravdivostní hodnoty atomu q_j v celém modelu K. To udělejme takto:

- atomy $p_{j+1}, .., p_m$ ohodnoťme v a podle e,
- atomy $p_1, .., p_j$ a $q_1, .., q_{j-1}$ prohlašme v a za nesplněné,

- atomu q_j přidělme v každém vrcholu x modelu K tutéž pravdivostní hodnotu, kterou v x má formule A^*_{j-1}.

Je zřejmé, že při takovémto přidělení pravdivostních hodnot je v K splněna podmínka perzistence. Navíc $a \Vdash A^*_{j-1} \to q_j$ (protože q_j a A^*_{j-1} mají všude tutéž pravdivostní hodnotu), $a \nVdash p_j \to q_j$ (protože $b_1 \Vdash p_j$ a $b_1 \nVdash q_j$) a $a \nVdash \neg p_j \to q_j$ (protože $b_0 \Vdash \neg p_j$ a $b_0 \nVdash q_j$). Tedy $a \nVdash A^*_j$ a model K je hledaným protipříkladem na formuli A^*_j, ve kterém jsou atomy $p_{j+1}, \ldots, p_m$ ohodnoceny všude dle e.

Zmiňme se ještě o implikaci $\Leftarrow$ v případě, kdy $j > 0$. Snadno lze ověřit, že je-li model K protipříkladem na formuli $(p_j \vee \neg p_j) \to A^*_{j-1}$, ve kterém jsou $p_{j+1}, \ldots, p_m$ ohodnoceny všude dle e, pak K má podmodel K', ve kterém je atom p_j ohodnocen všude shodně a který je protipříkladem na formuli A^*_{j-1}. A je-li K protipříkladem na formuli $(A^*_{j-1} \to q_j) \to ((p_j \to q_j) \vee (\neg p_j \to q_j))$, pak K má dva disjunktní podmodely K_1 a K_0, oba jsou protipříklady na formuli A^*_{j-1}, přičemž p_j je v K_1 ohodnocen všude kladně a v K_0 všude záporně. Na modely K', K_1 a K_0 lze vztáhnout indukční předpoklad. Podrobnosti přenecháváme čtenáři a sublemma tím máme za dokázané.

Pro $j = m$ sublemma říká, že formule A je logicky platná, právě když formule A^* má kripkovský protipříklad. Funkce $A \mapsto A^*$ je tedy hledaným logaritmickým převodem. QED

5.1.3 Sémantika intuicionistické predikátové logiky

V intuicionistické predikátové logice máme co dělat s týmiž formulemi jako v klasické predikátové logice: jsou to formule sestavené z atomických formulí pomocí čtyř logických spojek &, $\vee$, $\to$, $\neg$ a dvou kvantifikátorů $\forall$ a $\exists$. Sémantika intuicionistické predikátové logiky je založena na pojmu kripkovské struktury pro daný jazyk. Protože malá latinská písmena chceme užívat pro prvky struktur, domluvme se, že vrcholy kripkovských rámců budeme v tomto pododdílu značit řeckými písmeny ze začátku abecedy.

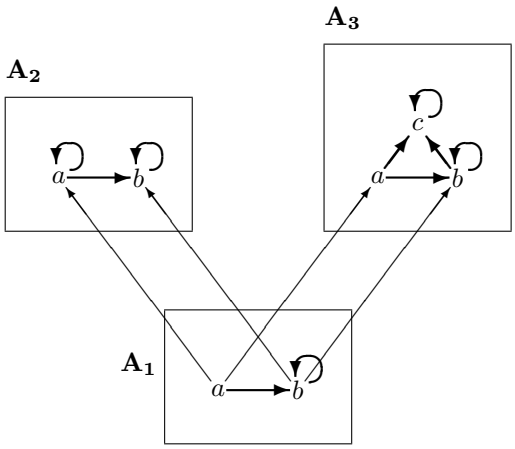
Definice 5.1.17 *Řekneme, že trojice* $\langle W, \leq, l\rangle$ *je* kripkovská (intuicionistická predikátová) struktura *pro jazyk* L*, jestliže relace* $\leq$ *je uspořádání na neprázdné množině* W *a* l *je funkce definovaná na množině* W*, která splňuje podmínky:*

- *všechny hodnoty* $l(\alpha)$ *funkce* l *jsou struktury pro jazyk* L *(ve smyslu klasické predikátové logiky bez rovnosti),*
- *jsou-li* A *a* B *nosné množiny struktur* $l(\alpha)$ *a* $l(\beta)$ *a platí-li* $\alpha \leq \beta$*, pak* $A \subseteq B$*,*
- *jsou-li* $s^{l(\alpha)}$ *a* $s^{l(\beta)}$ *realizace libovolného (funkčního nebo predikátového) symbolu* s *ve strukturách* $l(\alpha)$ *a* $l(\beta)$ *a platí-li* $\alpha \leq \beta$*, pak* $s^{l(\alpha)} \subseteq s^{l(\beta)}$*.*

Dvojici $\langle W, \leq\rangle$ *říkáme* (kripkovský) rámec *struktury* $\langle W, \leq, l\rangle$*.*

I v predikátové logice můžeme prvky množiny W chápat jako informační stavy. Podmínka $A \subseteq B$ pro nosné množiny struktur $l(\alpha)$ a $l(\beta)$ takových, že $\alpha \leq \beta$, říká,

že při přechodu ze stavu α do stavu β dosažitelného z α nemohou zmizet žádné objekty (univerza, o kterém se mluví). Podmínka $s^{l(\alpha)} \subseteq s^{l(\beta)}$ říká, že nemohou zmizet ani informace o vztazích mezi objekty. Může ale vyjít najevo existence nových objektů a nových vztahů.



Obrázek 5.1.5: Predikátová kripkovská struktura

Na obrázku 5.1.5 je příklad predikátové kripkovské struktury $\langle W, \leq, l\rangle$ pro jazyk s jedním binárním predikátovým symbolem R. Rámec $\langle W, \leq\rangle$ této struktury má tři prvky α_1, α_2 a α_3, které nejsou znázorněny a kterým funkce l přiřazuje struktury $\mathbf{A_1}$, $\mathbf{A_2}$ a $\mathbf{A_3}$. Relace $\leq$ je nejmenší (tranzitivní a) reflexivní relace na množině $\{\alpha_1, \alpha_2, \alpha_3\}$ obsahující množinu $\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3]\}$. Tenkými šipkami je znázorněna jak inkluze mezi nosnými množinami struktur, tak relace dosažitelnosti $\leq$. Silnější šipky znázorňují relaci R. Nová informace, která byla získána při přechodu ze stavu α_1 do stavu α_2, zní, že pro objekt a platí $a\ R\ a$. Nová informace, která byla získána při přechodu ze stavu α_1 do stavu α_3, zní, že kromě objektů a a b existuje také objekt c, pro který platí $a\ R\ c$, $b\ R\ c$ a $c\ R\ c$.

Je-li e ohodnocení proměnných v nějaké struktuře $l(\alpha)$ a platí-li $\alpha \leq \beta$, pak vzhledem k inkluzi, která platí pro nosné množiny struktur $l(\alpha)$ a $l(\beta)$, je ohodnocení e současně i ohodnocením proměnných ve struktuře $l(\beta)$. Snadno lze ověřit, že je-li t term jazyka L a je-li b jeho hodnota ve struktuře $l(\alpha)$, pak b je hodnota termu t i v každé struktuře $l(\beta)$ takové, že $\alpha \leq \beta$.

Definice 5.1.18 *Nechť $\langle W, \leq, \Vdash\rangle$ je kripkovská struktura pro jazyk L. Relace $\Vdash$ mezi prvky α množiny W, predikátovými formulemi φ a ohodnoceními e proměnných ve struktuře $l(\alpha)$ je definována podmínkami:*

- *je-li φ atomická formule jazyka L, pak $\alpha \Vdash \varphi[e]$, právě když $l(\alpha) \models \varphi[e]$ (ve smyslu klasické predikátové logiky),*
- *$\alpha \Vdash (\varphi\ \&\ \psi)[e]$, právě když $\alpha \Vdash \varphi[e]$ a $\alpha \Vdash \psi[e]$,*

- $\alpha \Vdash (\varphi \vee \psi)[e]$, *právě když* $\alpha \Vdash \varphi[e]$ *nebo* $\alpha \Vdash \psi[e]$,
- $\alpha \Vdash (\varphi \to \psi)[e]$, *právě když pro každý stav* $\beta \geq \alpha$, *pro který platí* $\beta \Vdash \varphi[e]$, *platí i* $\beta \Vdash \psi[e]$,
- $\alpha \Vdash (\neg\varphi)[e]$, *právě když pro každý stav* $\beta \geq \alpha$ *platí* $\beta \nVdash \varphi[e]$,
- $\alpha \Vdash (\exists x\varphi)[e]$, *právě když existuje prvek* a *nosné množiny struktury* $l(\alpha)$ *takový, že* $\alpha \Vdash \varphi[e(x/a)]$,
- $\alpha \Vdash (\forall x\varphi)[e]$, *právě když pro každý stav* $\beta \geq \alpha$ *a pro každý prvek* b *nosné množiny struktury* $l(\beta)$ *platí* $\beta \Vdash \varphi[e(x/b)]$.

Podmínku $\alpha \Vdash \varphi[e]$ *čteme „formule* φ *je splněna ohodnocením* e *ve vrcholu* α*“.*

Je zřejmé, že posledních šest podmínek odpovídá podmínkám T4–T9 z definice 3.1.9 (v jiném pořadí). Podmínka pro univerzální kvantifikátor se podobá podmínce pro implikaci a negaci v tom, že chceme-li určit, zda $\alpha \Vdash (\forall x\varphi)[e]$, potřebujeme vědět, kterými ohodnoceními je formule φ splněna ve vrcholech dosažitelných z vrcholu α. Naproti tomu chceme-li určit, zda $\alpha \Vdash (\exists x\varphi)[e]$, stačí vědět, kterými ohodnoceními je formule φ splněna v samotném vrcholu α.

V dalším budeme někdy ztotožňovat vrchol α kripkovské struktury $\langle W, \leq, l\rangle$ se strukturou $l(\alpha)$, tj. budeme si myslet, že prvky množiny W jsou struktury v klasickém smyslu a že l je identická funkce, a budeme psát například $\mathbf{D} \Vdash \varphi[e]$ místo $\mathbf{D} = l(\alpha)$ a $\alpha \Vdash \varphi[e]$. Takovéto zjednodušení je ovšem zcela korektní pouze tehdy, je-li funkce l prostá, což obecně být nemusí.

Podívejme se ještě jednou na strukturu z obrázku 5.1.5. K libovolnému objektu d libovolného ze tří stavů této struktury existuje v tomtéž stavu objekt d' takový, že $R[d, d']$. Tedy formule $\exists y R(x, y)$ je splněna všemi prvky všech tří stavů. To znamená, že $\alpha_i \Vdash \forall x \exists y R(x, y)$ pro $i \in \{1, 2, 3\}$. Platí $\alpha_1 \nVdash \forall x R(x, y)[b]$, není totiž pravda, že ve všech stavech viditelných z α_1 vede do b šipka ze všech objektů. Ani a ovšem v α_1 nesplňuje formuli $\forall x R(x, y)$. Tedy $\alpha_1 \nVdash \exists y \forall x R(x, y)$. Platí ale $\alpha_2 \Vdash \exists y \forall x R(x, y)$ i $\alpha_3 \Vdash \exists y \forall x R(x, y)$. To znamená, že formule $\neg\exists y \forall x R(x, y)$ není splněna v žádném ze tří stavů, a naopak formule $\neg\neg\exists y \forall x R(x, y)$, kterou lze číst „nemůže neexistovat y takové, že ...“, je ve všech splněna.

Lemma 5.1.19 *Nechť* $\langle W, \leq, l\rangle$ *je kripkovská struktura, nechť* α *a* β *jsou její vrcholy takové, že* $\alpha \leq \beta$, *a nechť* φ *je formule a* e *ohodnocení proměnných ve struktuře* $l(\alpha)$. *Když* $\alpha \Vdash \varphi[e]$, *pak* $\beta \Vdash \varphi[e]$.

Důkaz Indukcí podle složitosti formule φ. QED

Řekneme, že struktura $\langle W, \leq, l\rangle$ je *(intuicionistický kripkovský) protipříklad* na sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$, jestliže existuje vrchol $\alpha \in W$ a ohodnocení proměnných e ve struktuře $l(\alpha)$ tak, že $\alpha \Vdash \varphi[e]$ pro všechny formule $\varphi \in \Gamma$ a $\alpha \nVdash \varphi[e]$ pro všechny formule $\varphi \in \Delta$. Sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je *intuicionisticky logicky platný*, jestliže nemá žádný kripkovský protipříklad. Formule φ je *intuicionisticky logicky platná*, jestliže sekvent $\langle\, \Rightarrow \varphi \,\rangle$ je intuicionisticky logicky platný.

Dále řekneme, že formule φ je *intuicionistický důsledek* množiny formulí Δ, jestliže je v každém vrcholu každé kripkovské struktury splněna každým ohodnocením proměnných, které v něm splňuje všechny formule z množiny Δ. Formule φ je *intuicionistický důsledek formule* ψ, jestliže je intuicionistickým důsledkem množiny $\{\psi\}$. Formule φ a ψ jsou *intuicionisticky ekvivalentní*, jestliže každá z nich je intuicionistickým důsledkem druhé.

Příklad 5.1.20 Nechť P je unární predikátový symbol, nechť $\langle W, \leq, l\rangle$ je kripkovská struktura pro jazyk $\{P\}$ a nechť α je vrchol struktury $\langle W, \leq, l\rangle$, v němž je (některým čili každým ohodnocením proměnných) splněna sentence $\forall v(P(v) \vee \neg P(v))$. Je-li a je libovolný prvek nosné množiny struktury $l(\alpha)$, pak z příslušných řádků definice 5.1.17 plyne $\alpha \Vdash (P(x) \vee \neg P(x))[a]$ i $\alpha \Vdash (\exists v P(v) \vee \neg P(x))[a]$. Tudíž první dva z následujících tří sekventů jsou intuicionisticky logicky platné:

$$\langle\, \forall v(P(v) \vee \neg P(v)) \;\Rightarrow\; P(x), \neg P(x) \,\rangle,$$
$$\langle\, \forall v(P(v) \vee \neg P(v)) \;\Rightarrow\; \exists v P(v), \neg P(x) \,\rangle,$$
$$\langle\, \forall v(P(v) \vee \neg P(v)) \;\Rightarrow\; \exists v P(v), \forall v \neg P(v) \,\rangle.$$

Zvolme $W = \{\mathbf{A}_1, \mathbf{A}_2\}$, kde $\mathbf{A}_1 \leq \mathbf{A}_2$, $A_1 = \{a\}$, $A_2 = \{a, b\}$ a pro realizaci symbolu P platí $P_1^{\mathbf{A}} = \emptyset$ a $P_2^{\mathbf{A}} = \{b\}$. Tím jsme získali intuicionistickou strukturu, která je protipříkladem na třetí sekvent: objekt a splňuje v $\mathbf{A}_1$ i v $\mathbf{A}_2$ formuli $\neg P(x)$, objekt b splňuje v $\mathbf{A}_2$ (tj. všude, v $\mathbf{A}_1$ se totiž nevyskytuje) formuli $P(x)$, tedy $\mathbf{A}_1 \Vdash \forall v(P(v) \vee \neg P(v))$; na druhé straně ale $\mathbf{A}_1 \nVdash \forall v \neg P(v)$ (protože $\mathbf{A}_2 \nVdash (\neg P(x))[b]$) a $\mathbf{A}_1 \nVdash \exists v P(v)$.

Gentzenovský kalkulus GJ pro intuicionistickou *predikátovou* logiku má táž výroková a strukturální pravidla, která jsme definovali v předchozím pododdílu, a dále čtyři kvantifikátorová pravidla:

$\exists$-r: $\quad \langle\, \Gamma \Rightarrow \Delta, \varphi_x(t) \,\rangle \;/\; \langle\, \Gamma \Rightarrow \Delta, \exists x \varphi \,\rangle,$

$\forall$-l: $\quad \langle\, \Gamma, \varphi_x(t) \Rightarrow \Delta \,\rangle \;/\; \langle\, \Gamma, \forall x \varphi \Rightarrow \Delta \,\rangle,$

$\exists$-l: $\quad \langle\, \Gamma, \varphi_x(y) \Rightarrow \Delta \,\rangle \;/\; \langle\, \Gamma, \exists x \varphi \Rightarrow \Delta \,\rangle,$

$\forall$-rI: $\quad \langle\, \Gamma \Rightarrow \varphi_x(y) \,\rangle \;/\; \langle\, \Gamma \Rightarrow \forall x \varphi \,\rangle.$

kde, jako v klasické predikátové logice, t je term a y je proměnná substituovatelná za x do formule φ, a u pravidel generalizace, tj. u pravidel $\exists$-l a $\forall$-rI, se proměnná y nevyskytuje ve výsledném sekventu. První tři pravidla jsou úplně stejná jako v klasické predikátové logice. Pravidlo $\forall$-rI můžeme nazývat *kritickým*; stejně jako pravidla $\rightarrow$-rI a $\neg$-rI je použitelné jen tak, že po jeho použití je sukcedent jednoprvkový. Z příkladu 5.1.20 je zřejmé, že klasické pravidlo $\forall$-r s libovolnou množinou postranních formulí v sukcedentu není korektní vůči sémantice intuicionistické predikátové logiky.

Věta 5.1.21 (o korektnosti kalkulu GJ) *Každý sekvent dokazatelný v predikátovém kalkulu GJ je intuicionisticky logicky platný. Kalkulus GJ je tedy korektní vůči kripkovské sémantice intuicionistické predikátové logiky.*

Důkaz Korektnost strukturálních a výrokových pravidel platí ze stejných důvodů jako ve výrokové logice. Dokažme korektnost pravidla ∀-rI; ověření korektnosti ostatních pravidel ponecháváme na čtenáři. Nechť $\langle\, \Gamma \;\Rightarrow\; \varphi_x(y) \,\rangle$ je intuicionisticky logicky platný sekvent, $\langle W, \leq, l\rangle$ je kripkovská struktura, α její vrchol a e ohodnocení proměnných ve struktuře $l(\alpha)$ takové, že $\alpha \Vdash \Gamma[e]$. Máme ověřit, že $\alpha \Vdash (\forall x\varphi)[e]$. Podle podmínky pro univerzální kvantifikátor v definici 5.1.18 máme zdůvodnit, že $\beta \Vdash \varphi[e(x/b)]$ pro libovolný vrchol β dosažitelný z vrcholu α a pro libovolný prvek b struktury $l(\beta)$. Nechť tedy vrchol $\beta \geq \alpha$ a prvek b nosné množiny struktury $l(\beta)$ jsou dány. Lemma 5.1.19 dává $\beta \Vdash \Gamma[e]$. Dále můžeme uvažovat stejně jako v důkazu věty 3.3.1: protože proměnná y se nevyskytuje volně ve formulích z množiny Γ, platí $\beta \Vdash \Gamma[e]$, protože sekvent $\langle\, \Gamma \;\Rightarrow\; \varphi_x(y) \,\rangle$ je intuicionisticky logicky platný, máme $\beta \Vdash (\varphi_x(y))[e(y/b)]$, a protože proměnná y nemá volné výskyty ve formuli $\forall x\varphi$, jsou podmínky $\beta \Vdash \varphi_x(y)[e(y/b)]$ a $\beta \Vdash \varphi[e(x/b)]$ spolu ekvivalentní. QED

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\langle\, P(z) \;\Rightarrow\; P(z), P(y) \,\rangle}{\langle\, \neg P(z), P(z) \;\Rightarrow\; P(y) \,\rangle} \quad \langle\, P(y), P(z) \;\Rightarrow\; P(y) \,\rangle}{\langle\, \neg P(z) \vee P(y), P(z) \;\Rightarrow\; P(y) \,\rangle}}{\langle\, \forall y(\neg P(z) \vee P(y)), P(z) \;\Rightarrow\; P(y) \,\rangle}}{\langle\, \forall y(\neg P(z) \vee P(y)), P(z) \;\Rightarrow\; \forall y P(y) \,\rangle}}{\langle\, \forall y(\neg P(z) \vee P(y)), P(z) \;\Rightarrow\; \exists x \neg P(x) \vee \forall y P(y) \,\rangle}}{\langle\, \forall y(\neg P(z) \vee P(y)), \neg P(z) \vee P(z) \;\Rightarrow\; \exists x \neg P(x) \vee \forall y P(y) \,\rangle}}{\langle\, \forall y(\neg P(z) \vee P(y)) \;\Rightarrow\; \exists x \neg P(x) \vee \forall y P(y) \,\rangle}}{\langle\, \exists x \forall y(\neg P(x) \vee P(y)) \;\Rightarrow\; \exists x \neg P(x) \vee \forall y P(y) \,\rangle}$$

Obrázek 5.1.6: Příklad důkazu v intuicionistickém predikátovém kalkulu

Na obrázku 5.1.6 je příklad (bezřezového) důkazu v kalkulu GJ. Předpokládáme, že čtenář dovede doplnit formule, které jsme kvůli úspoře místa naznačili tečkami. Tento důkaz je obtížnější polovinou důkazu, že formuli $\exists x \neg P(x) \vee \forall y P(y)$ lze v intuicionistické logice převést na *prenexní normální tvar*. To je ne zcela samozřejmý výsledek, neboť věta o převeditelnosti libovolné formule na prenexní normální tvar v intuicionistické logice obecně neplatí.

Větou o úplnosti a větou o kompaktnosti pro intuicionistickou logiku se nezabývejme. Spokojme se s prohlášením *ex cathedra*, že obě věty platí. Důkaz lze nalézt například v [14], v [22] nebo v [91]. Některá cvičení dávají návod na sestrojení alternativního důkazu věty o úplnosti pro výrokové kalkuly, ze kterého plyne věta o kompaktnosti alespoň pro výrokovou logiku a který by šlo zobecnit i na predi-

kátovou logiku. Také věta o eliminovatelnosti řezů platí i pro predikátovou verzi kalkulu GJ, důkaz lze získat například modifikací našeho důkazu z oddílu 3.3.

Hilbertovský kalkulus HJ pro intuicionistickou predikátovou logiku lze utvořit tak, že k výrokovému kalkulu HJ uvedenému v předchozím pododdílu přidáme schémata B1 a B2 a pravidla Gen-A a Gen-E. To znamená, že axiomy a pravidla klasického hilbertovského kalkulu týkající se kvantifikátorů vyhovují bez jakékoliv modifikace i pro intuicionistickou logiku. Důkaz ekvivalence a vzájemné polynomiální simulovatelnosti kalkulů HJ a GJ ponecháváme za cvičení.

Uvažujme nyní jazyk s jediným unárním predikátovým symbolem P a všechny sentence, které lze v tomto jazyce napsat bez užití binárních logických spojek. To nám dá podrobnější představu o chování kvantifikátorů v intuicionistické logice a o vzájemné interakci obou kvantifikátorů a negace. V klasické logice jsou ve hře jen čtyři sentence: $\forall x P(x)$, $\exists x P(x)$ a jejich negace. Vezměme první z nich, $\forall x P(x)$, a zkoumejme, jaké implikace v intuicionistické logice platí mezi ní a sentencemi $\neg\exists x\neg P(x)$, $\forall x\neg\neg P(x)$, $\neg\neg\forall x P(x)$ a $\neg\neg\forall x\neg\neg P(x)$, které jsou s ní klasicky ekvivalentní. Žádné jiné sentence nemusíme uvažovat ani v intuicionistické logice: každá další sentence neobsahující binární logické spojky a klasicky ekvivalentní se sentencí $\forall x P(x)$ už obsahuje jalové kvantifikátory nebo trojnou negaci.

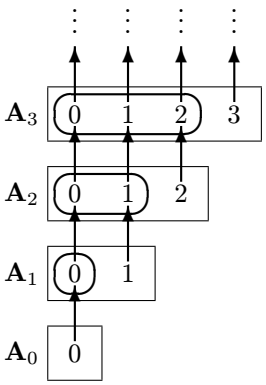
Snadno lze dokázat, že každé dvě formule tvaru $\neg\exists x\varphi$ a $\forall x\neg\varphi$ jsou spolu intuicionisticky ekvivalentní. Z toho plyne, že sentence $\forall x\neg\neg P(x)$ a $\neg\exists x\neg P(x)$ jsou spolu ekvivalentní, a také $\neg\neg\forall x\neg\neg P(x)$ je ekvivalentní s $\neg\neg\neg\exists x\neg P(x)$, tedy s $\neg\exists x\neg P(x)$. Vezmeme-li v úvahu ještě implikaci $\neg\neg\forall x P(x) \to \forall x\neg\neg P(x)$, jejíž důkaz ponecháváme na čtenáři, můžeme našich pět sentencí sestavit do posloupnosti

$$\forall x P(x), \quad \big| \quad \neg\neg\forall x P(x), \quad \big\| \quad \forall x\neg\neg P(x), \qquad \neg\exists x\neg P(x), \qquad \neg\neg\forall x\neg\neg P(x),$$

ve které každá následující sentence vyplývá z předchozí a poslední tři jsou spolu ekvivalentní. Svislými čarami jsou odděleny neekvivalentní sentence. Protipříklad na implikaci $\neg\neg\forall x P(x) \to \forall x P(x)$ lze sestrojit snadno, stačí vzít kripkovskou strukturu se dvěma stavy a jediným objektem, který nejprve nemá a potom má vlastnost P. Protipříklad na implikaci $\forall x\neg\neg P(x) \to \neg\neg\forall x P(x)$ je na obrázku 5.1.7. Je to kripkovská struktura, která má nekonečně mnoho stavů $\alpha_0 \le \alpha_1 \le \alpha_2 \le \ldots$, jimž funkce l přiřazuje struktury $\mathbf{A}_0$, $\mathbf{A}_1$, $\mathbf{A}_2$ atd. Každá struktura $\mathbf{A}_n$ obsahuje jeden „nový“ objekt n a n „starých“ objektů $0, \ldots, n-1$. Realizace symbolu P je naznačena ovály. Staré objekty mají vlastnost P, nový ji nemá. Od okamžiku $n+1$ ji ale mít bude, a to už pořád. Tedy v α_n nový objekt n splňuje formuli $\neg\neg P(x)$. Objekty $0, \ldots, n-1$ ji ovšem splňují také, a platí to pro každé n. Tedy $\alpha_0 \Vdash \forall x\neg\neg P(x)$. Na druhé straně jsou z každého stavu α_n viditelné objekty, které nesplňují formuli $P(x)$. Tedy $\alpha_n \nVdash \forall x P(x)$, a proto $\alpha_0 \Vdash \neg\forall x P(x)$.

Právě popsaný příklad ukazuje důležité rozdíly mezi výrokovou a predikátovou variantou intuicionistické logiky. Pro sentence $\varphi = \neg\neg\forall x P(x)$ a $\psi = \forall x\neg\neg P(x)$ jsme chtěli sestrojit strukturu a její vrchol α tak, aby platilo $\alpha \Vdash \psi$ a $\alpha \nVdash \varphi$. Sestrojili jsme strukturu a její vrchol α dokonce takové, že $\alpha \Vdash \psi$ a $\alpha \Vdash \neg\varphi$. Toto je něco, co by se ve výrokové logice stát nemohlo, a je to zároveň důvod, proč

jsme sentence φ a ψ v našem seznamu pěti sentencí oddělili dvojitou čarou. Když $\psi \to \varphi$ je *výroková* formule a a vrchol nějakého modelu takový, že $a \Vdash \psi$ a $a \Vdash \neg\varphi$, pak $a \nVdash \psi \to \neg\neg\varphi$, a podle věty 5.1.15 formule $\psi \to \varphi$ není klasickou tautologií. V predikátové logice ale existují sentence ψ a φ takové, že $\psi \to \varphi$ je klasicky logicky platnou formulí, a přitom $\psi \to \neg\neg\varphi$ není intuicionisticky logicky platnou formulí. Z toho plyne, že *analogie věty 5.1.15 v intuicionistické predikátové logice neplatí.*



Obrázek 5.1.7: Protipříklad na schéma DNS

O kripkovské struktuře řekneme, že je *konečná*, má-li jen konečně mnoho stavů (které ovšem mohou být nekonečné). O schématu

DNS: $\quad \forall x \neg\neg P(x) \to \neg\neg \forall x P(x),$

jehož označení pochází z anglického *double negation shift*, přesunutí dvojné negace před univerzální kvantifikátor, lze ověřit, že platí v každé konečné kripkovské struktuře. To znamená, že existují formule, které mají protipříklad, ale nemají konečný protipříklad, a tedy že *FMP, vlastnost konečných modelů, pro intuicionistickou predikátovou logiku neplatí.*

I v predikátové logice ale platí, že kdo zná intuicionistickou logiku, zná vlastně i klasickou, neboť klasická predikátová logika je interpretovatelná v intuicionistické. Jednou z možností, jak zvolit příslušný překlad, je tato:

$$\varphi^* = \varphi, \qquad \text{je-li } \varphi \text{ atomická},$$
$$(\varphi \bowtie \psi)^* = \varphi^* \bowtie \psi^*, \qquad \text{je-li } \bowtie \text{ kterákoliv ze spojek } \&, \vee, \to,$$
$$(\neg\varphi)^* = \neg\varphi^*, \qquad (\exists x\varphi)^* = \exists x\varphi^*, \qquad (\forall x\varphi)^* = \forall x\neg\neg\varphi^*.$$

Formule φ^* tedy vznikne z φ připsáním dvojné negace za každý univerzální kvantifikátor. Označme ještě $\Sigma^* = \{\, \varphi^* \,;\, \varphi \in \Sigma \,\}$ a $\neg\Sigma = \{\, \neg\varphi \,;\, \varphi \in \Sigma \,\}$, kde Σ je libovolná množina formulí.

Věta 5.1.22 *Libovolný sekvent* $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ *je klasicky logicky platný, právě když sekvent* $\langle\, \Gamma^*, \neg\Delta^* \;\Rightarrow\, \rangle$ *je intuicionisticky logicky platný. Tedy libovolná predikátová*

formule φ je klasicky logicky platná, právě když formule $\neg\neg\varphi^*$ je intuicionisticky logicky platná.

Důkaz Je jasné, že druhá část věty plyne z první, neboť φ je klasicky logicky platná, právě když sekvent $\langle\, \Rightarrow\, \varphi\,\rangle$ je klasicky logicky platný, a $\neg\neg\varphi^*$ je intuicionisticky logicky platná, právě když sekvent $\langle\, \neg\varphi^*\, \Rightarrow\,\rangle$ je intuicionisticky logicky platný. Také je jasné, že je-li sekvent $\langle\, \Gamma^*, \neg\Delta^*\, \Rightarrow\,\rangle$ intuicionisticky logicky platný, pak sekvent $\langle\, \Gamma^*\, \Rightarrow\, \neg\neg\Delta^*\,\rangle$ je klasicky logicky platný, a také sekvent $\langle\, \Gamma\, \Rightarrow\, \Delta\,\rangle$ je klasicky logicky platný; každá formule $\neg\neg\psi^*$ v $\neg\neg\Delta^*$ je totiž klasicky ekvivalentní s formulí ψ.

Zbývá dokázat jen implikaci $\Rightarrow$ v první části věty. Věta o úplnosti pro klasický kalkulus GK říká, že každý logicky platný sekvent je v kalkulu GK dokazatelný. Můžeme tedy postupovat indukcí podle počtu kroků v důkazu sekventu. Proberme na ukázku případ, kdy poslední krok v důkazu daného sekventu je &-r. Všechny ostatní případy jsou podobné nebo jednodušší. Mějme tedy důkaz tvaru

$$\dfrac{\begin{array}{cc}\mathcal{P}_1 & \mathcal{P}_2\\ \langle\, \Pi\, \Rightarrow\, \Lambda, \varphi\,\rangle & \langle\, \Pi\, \Rightarrow\, \Lambda, \psi\,\rangle\end{array}}{\langle\, \Pi\, \Rightarrow\, \Lambda, \varphi\,\&\,\psi\,\rangle}$$

v kalkulu GK. Ten lze přepracovat na důkaz v kalkulu GJ:

$$\dfrac{\dfrac{\dfrac{\begin{array}{cc}\mathcal{P}_0 & \mathcal{P}'_1\\ \langle\, \neg(\varphi^*\,\&\,\psi^*), \psi^*\, \Rightarrow\, \neg\varphi^*\,\rangle & \langle\, \Pi^*, \neg\Lambda^*, \neg\varphi^*\, \Rightarrow\,\rangle\end{array}}{\langle\, \Pi^*, \neg\Lambda^*, \neg(\varphi^*\,\&\,\psi^*), \psi^*\, \Rightarrow\,\rangle}}{\langle\, \Pi^*, \neg\Lambda^*, \neg(\varphi^*\,\&\,\psi^*)\, \Rightarrow\, \neg\psi^*\,\rangle} \qquad \begin{array}{c}\mathcal{P}'_2\\ \langle\, \Pi^*, \neg\Lambda^*, \neg\psi^*\, \Rightarrow\,\rangle\end{array}}{\langle\, \Pi^*, \neg\Lambda^*, \neg(\varphi^*\,\&\,\psi^*)\, \Rightarrow\,\rangle.}$$

Důkazy $\mathcal{P}'_1$ a $\mathcal{P}'_2$ sekventů $\langle\, \Pi^*, \neg\Lambda^*, \neg\varphi^*\, \Rightarrow\,\rangle$ a $\langle\, \Pi^*, \neg\Lambda^*, \neg\psi^*\, \Rightarrow\,\rangle$ existují podle indukčního předpokladu, důkaz $\mathcal{P}_0$ sekventu $\langle\, \neg(\varphi^*\,\&\,\psi^*), \varphi^*\, \Rightarrow\, \neg\psi^*\,\rangle$ lze snadno sestrojit. QED

Cvičení

1. Dokažte lemma 5.1.3.
2. Nechť a je libovolný vrchol libovolného kripkovského modelu. Dokažte, že $a \Vdash \neg\neg A$, právě když $\forall b \geq a \exists c \geq b (c \Vdash A)$.
3. Nechť A je libovolná výroková formule a $\langle W, \leq, \Vdash\rangle$ je libovolný kripkovský model. Dokažte, že ke každému vrcholu $a \in W$ existuje vrchol $b \in W$ takový, že $a \leq b$, a přitom $b \Vdash A$ nebo $b \Vdash \neg A$. Vyvoďte z toho, že každá formule tvaru $\neg\neg(A \vee \neg A)$ je intuicionistickou tautologií.

4. Dokažte, že množina Int-Taut je uzavřená na pravidlo substituce.

5. Rozhodněte, které z následujících formulí (schémat) jsou intuicionistické tautologie:

   $(A \to B) \to (\neg B \to \neg A)$,
   $(\neg B \to \neg A) \to (A \to B)$,
   $(\neg\neg A \to B) \to (\neg B \to \neg A)$,
   $(A \to B) \vee (B \to A)$,
   $\neg(A \to B) \to \neg B$,
   $\neg(A \to B) \to A$,
   $\neg(A \to B) \to \neg\neg A$,
   $(A \to B) \to ((\neg A \to B) \to B)$,
   $(A \to B) \to (\neg\neg A \to \neg\neg B)$,
   $\neg A \vee \neg\neg A$,
   $A \vee \neg A \to (\neg\neg A \to A)$,
   $\neg\neg A \vee (\neg\neg A \to A)$,
   $(A \to \neg\neg B) \to (\neg\neg A \to \neg\neg B)$,
   $(A \to \neg\neg B) \to \neg\neg(A \to B)$,
   $\neg\neg(A \to B) \to (A \to \neg\neg B)$,
   $A \,\&\, (B \vee C) \to (A \,\&\, B) \vee (A \,\&\, C)$,
   $A \vee (B \,\&\, C) \to (A \vee B) \,\&\, (A \vee C)$,
   $A \to (B \vee C) \to (A \to B) \vee (A \to C)$,
   $\neg\neg(A \,\&\, B) \equiv (\neg\neg A \,\&\, \neg\neg B)$,
   $\neg\neg(\neg\neg A \to A)$.

6. Nechť $\langle W, \leq, \Vdash\rangle$ je kripkovský model pro intuicionistickou výrokovou logiku. Řekneme, že formule A v modelu $\langle W, \leq, \Vdash\rangle$ *definuje* množinu $X \subseteq W$, jestliže $X = \{\, x \in W \,;\, x \Vdash A \,\}$. Řekneme, že množina $X \subseteq W$ je *definovatelná* v modelu $\langle W, \leq, \Vdash\rangle$, jestliže existuje formule, která ji v něm definuje. Například v modelu z obr. 5.1.1 definuje formule $p\&q$ množinu $\{d\}$. Dokažte indukcí podle složitosti formule A, že neobsahuje-li formule A spojku &, pak A v modelu z obr. 5.1.1 nedefinuje množinu $\{d\}$. Vyvoďte z toho, že formule $p \,\&\, q$ není v intuicionistické logice ekvivalentní s žádnou formulí neobsahující spojku &. To znamená, že konjunkce není v intuicionistické logice vyjádřitelná pomocí ostatních logických spojek. Podobnou úvahu (a model) lze navrhnout i pro ostatní logické spojky, viz [9].

7. Je-li $A \vee B$ intuicionistická tautologie, pak alespoň jedna z formulí A a B je také intuicionistická tautologie. Dokažte pomocí amalgamace kripkovských modelů.

8. Řekneme, že A je *negativní formule*, jestliže A je výroková formule sestavená pomocí konjunkce, implikace a negace z negovaných atomů. Dokažte, že není-li negativní formule intuicionistickou tautologií, pak má jednoprvkový kripkovský protipříklad, a není tedy ani klasickou tautologií.

   Návod. Dokažte indukcí podle složitosti formule A, že je-li $\langle W, \leq, \Vdash\rangle$ kripkovský model a platí-li $a \not\Vdash A$ pro negativní formuli A a nějaký vrchol $a \in W$, pak existuje vrchol $b \geq a$ takový, že $b \not\Vdash A$ a v podstromu generovaném vrcholem b žádný z atomů vyskytujících se ve formuli A nemění pravdivostní hodnotu.

9. Nechť A je negativní formule. Rozhodněte, zda formule $\neg\neg A \to A$ a $A \vee \neg A$ musí být intuicionistické tautologie.

10. Nechť $p_0, p_1, p_2, \ldots, q_0, q_1, q_2, \ldots$ jsou navzájem různé výrokové atomy a nechť posloupnosti A_n a B_n výrokových formulí jsou definovány takto:

$$A_0 = \bot, \qquad A_{n+1} = p_n \vee (p_n \to A_n),$$
$$B_0 = \bot, \qquad B_{n+1} = (B_n \to q_n) \to (p_n \to q_n) \vee (\neg p_n \to q_n).$$

Má každá formule A_n a B_n kripkovský protipříklad? Jaká je jeho minimální hloubka a počet vrcholů?

11. Zdůvodněte, že výrokový kalkulus GJ je korektní vůči kripkovské sémantice.

12. Dokažte v kalkulu GJ všechny formule z cvičení 5, které jsou intuicionistickými tautologiemi.

13. (a) Dokažte, že každý sekvent tvaru $\langle\, \neg(A \,\&\, B), \neg(\neg A \vee \neg B) \;\Rightarrow\; \rangle$ je v gentzenovském intuicionistickém kalkulu GJ dokazatelný.

(b) Dokažte, že každý sekvent tvaru

$$\langle\, \neg(p_1 \,\&\, .. \,\&\, p_n), \neg(\neg p_1 \vee .. \vee \neg p_n) \;\Rightarrow\; \rangle$$

je v kalkulu GJ dokazatelný. Předpokládejte, že závorky se kumulují doprava, tj. například $p_1 \,\&\, (p_2 \,\&\, (.. \,\&\, p_n)\,..)$. Lze sestrojit buď bezřezový důkaz hloubky $\mathcal{O}(n^2)$, nebo zobecněním bodu (a) sestrojit důkaz hloubky $\mathcal{O}(n)$ s řezy na formule $\neg(p_2 \,\&\, .. \,\&\, p_n)$, $\neg(p_3 \,\&\, .. \,\&\, p_n)$ atd.

14. Řekneme, že D je *harropovská formule*, jestliže disjunkce se v D vyskytuje pouze v rozsahu některé negace nebo v „levém rozsahu“ některé implikace. Dokažte, že když $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je intuicionisticky tautologický sekvent, množina Γ obsahuje pouze harropovské formule a $\Delta \neq \emptyset$, pak existuje formule $A \in \Delta$ taková, že $\langle\, \Gamma \;\Rightarrow\; A \,\rangle$ je intuicionisticky tautologický sekvent.

Návod. Postupujte indukcí podle počtu kroků v *bezřezovém* důkazu sekventu $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ v kalkulu GJ.

15. Dokažte, že každý sekvent dokazatelný v kalkulu GJ má důkaz (s řezy), ve kterém není použito pravidlo $\to$-w.

16. Dokažte, že je-li sekvent $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ dokazatelný v kalkulu GJ, pak sekvent $\langle\, \Gamma \;\Rightarrow\; \bigvee \Delta \,\rangle$ má důkaz (s řezy), ve kterém se v žádném sukcedentu nevyskytuje víc než jedna formule, tj. má důkaz v kalkulu GJ^1.

17. Dokažte, že jak užitím schématu $\neg\neg A \to A$, tak užitím schématu $A \vee \neg A$ lze v kalkulu HJ dokázat axiom A3 klasické výrokové logiky.

18. Dokažte implikaci $\Rightarrow$ v tvrzení 5.1.15 indukcí dle délky důkazu v kalkulu HJ.

19. Navrhněte modifikace kalkulů GJ a HJ pro případ, kdy nikoliv $\neg$, ale $\bot$ je základním symbolem, a $\neg A$ se definuje jako $A \to \bot$.

20. Množina Γ výrokových formulí je *D-úplná*, jestliže

- Γ je bezesporná, tj. neexistuje formule A taková, že z Γ lze (v kalkulu HJ) dokázat A i $\neg A$,
- Γ je deduktivně uzavřená, tj. kdykoliv $\Gamma \vdash A$, pak $A \in \Gamma$,
- kdykoliv $A \vee B \in \Gamma$, pak $A \in \Gamma$ nebo $B \in \Gamma$.

Dokažte, že když $\Delta \nvdash A$, pak existuje D-úplná množina $\Gamma \supseteq \Delta$ taková, že $\Gamma \nvdash A$.

Návod. Vezměte posloupnost $B_0, B_1, B_2, \ldots$ všech výrokových formulí a definujte posloupnost $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ množin rekurzí: $\Gamma_0 = \Delta$, $\Gamma_{n+1} = \Gamma_n \cup \{B_n\}$, jestliže $\Gamma_n \cup \{B_n\} \nvdash A$, jinak $\Gamma_{n+1} = \Gamma_n$. Zdůvodněte, že $\Gamma = \bigcup_n \Gamma_n$ vyhovuje.

21. Vypracujte alternativní důkaz věty o úplnosti kalkulu HJ vůči kripkovské sémantice založený na předchozím cvičení. Vezměte model $\langle W, \leq, \Vdash \rangle$, kde W je množina všech D-úplných množin, $\leq$ je inkluze a $\Vdash$ je pro atomy definována podmínkou $\Gamma \Vdash p \Leftrightarrow p \in \Gamma$. Model $\langle W, \leq, \Vdash \rangle$ je „univerzální protipříklad“: každá formule nedokazatelná v kalkulu HJ je nesplněna v některém vrcholu tohoto (jednoho) modelu.

22. Zdůvodněte, že z předchozích cvičení plyne i věta o kompaktnosti pro intuicionistickou výrokovou logiku.

23. (topologická sémantika intuicionistické logiky) Nechť S je topologický prostor. Funkce v z množiny všech výrokových formulí do množiny všech otevřených množin prostoru S je topologická evaluace v S, jestliže splňuje rovnosti

$$v(A \,\&\, B) = v(A) \cap v(B), \qquad v(A \vee B) = v(A) \cup v(B), \qquad v(\bot) = \emptyset,$$
$$v(A \to B) = \mathrm{Int}(\overline{v(A)} \cup v(B)),$$

kde $\mathrm{Int}(X)$ je vnitřek množiny X (tj. sjednocení všech otevřených podmnožin množiny X). Definujme dočasně, že A je *topologická tautologie*, jestliže platí $v(A) = S$ pro každý prostor S a pro každou topologickou evaluaci v v S. Dokažte, že každá intuicionistická tautologie je topologickou tautologií.

Návod. Postupujte indukcí podle počtu kroků v důkazu v kalkulu HJ. Dokažte pomocné tvrzení, že je-li X libovolná a Z uzavřená množina prostoru S, pak $\mathrm{Int}(Z \cup X) \subseteq Z \cup \mathrm{Int}(X)$ a $\mathrm{Int}(Z \cup X) = \mathrm{Int}(Z \cup \mathrm{Int}(X))$.

24. Dokažte, že každá topologická tautologie je intuicionistickou tautologií.

Návod. Definujte, že podmnožina nějakého kripkovského modelu je otevřená, jestliže s každým prvkem x obsahuje i všechny y dosažitelné z x.

25. Definujme dočasně, že sekvent je *skoro uzavřený*, jestliže splňuje první čtyři z pěti podmínek v definici 5.1.8. Nechť $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$ je sekvent nedokazatelný v kalkulu GJ. Vezměte za W množinu všech skoro uzavřených nedokazatelných sekventů sestavených z podformulí formulí vyskytujících se v $\langle\, \Gamma \;\Rightarrow\; \Delta \,\rangle$. Definujte relaci dosažitelnosti na množině W podmínkou

$$\langle\, \Pi_1 \;\Rightarrow\; \Lambda_1 \,\rangle \leq \langle\, \Pi_2 \;\Rightarrow\; \Lambda_2 \,\rangle \Leftrightarrow \Pi_1 \subseteq \Pi_2.$$

Dokončete důkaz úplnosti kalkulu GJ vůči kripkovské sémantice. Zdůvodněte, že i pro kalkulus vzniklý z GJ odstraněním pravidla $\to$-w platí věta o úplnosti a věta o eliminovatelnosti řezů.

26. Dokažte, že v logice vzniklé přidáním schématu $(A \to B) \vee (B \to A)$ k intuicionistické logice nelze dokázat $A \vee \neg A$, lze ale dokázat formule $\neg A \vee \neg\neg A$ i $(\neg\neg A \to A) \to (A \vee \neg A)$.

    Návod. Uvažte, že daná logika je korektní vůči třídě všech lineárně uspořádaných rámců.

27. Dokažte, že když X je libovolná bezesporná množina výrokových formulí uzavřená na pravidlo substituce a platí Int-Taut $\subseteq X$, pak $X \subseteq$ Taut. Množina Taut je tedy jedinou maximální bezespornou množinou obsahující množinu Int-Taut. Jak rozumíte termínu *bezesporná*?

    Návod. Není-li A tautologie, pak z A lze substitucí získat formuli A' takovou, že $\neg A'$ je tautologie.

28. Rozhodněte, zda množina všech intuicionistických tautologií, které jsou negativními formulemi, resp. které jsou harropovskými formulemi, je *PSPACE*-kompletní.

29. Nechť P je unární predikátový symbol. Určete, jaké implikace platí v intuicionistické predikátové logice mezi formulemi

    (a) $\exists x P(x)$, $\neg\neg\exists x P(x)$, $\exists x \neg\neg P(x)$, $\neg\forall x \neg P(x)$, $\neg\neg\exists x \neg\neg P(x)$,

    (b) $\neg\forall x P(x)$, $\exists x \neg P(x)$, $\neg\forall x \neg\neg P(x)$, $\neg\neg\exists x \neg P(x)$,

    (c) $\neg\exists x P(x)$, $\forall x \neg P(x)$, $\neg\exists x \neg\neg P(x)$, $\neg\neg\forall x \neg P(x)$.

    Sestrojte příslušné důkazy v kalkulu GJ a kripkovské protipříklady. Ve všech případech, kdy zjistíte, že implikace není intuicionisticky logicky platná, určete také, zda je možné, aby současně platily premisa a negace závěru.

30. Určete, které z následujících formulí jsou intuicionisticky logicky platné. Sestrojte příslušné důkazy a protipříklady. Předpokládejte, že formule χ neobsahuje volné výskyty proměnné x.

    $\neg\exists x\varphi \equiv \forall x\neg\varphi$, $\qquad$ $\forall x(\varphi \,\&\, \psi) \equiv \forall x\varphi \,\&\, \forall x\psi$,

    $\exists x\neg\varphi \to \neg\forall x\varphi$, $\qquad$ $\forall x(\chi \vee \varphi) \equiv \chi \vee \forall x\varphi$,

    $\exists x(\chi \vee \varphi) \equiv \chi \vee \exists x\varphi$, $\qquad$ $\forall x(\chi \to \varphi) \equiv \chi \to \forall x\varphi$,

    $\exists x(\neg\varphi \to \forall v\neg\varphi(v))$, $\qquad$ $\forall x(\varphi \to \chi) \equiv \exists x\varphi \to \chi$,

    $\neg\neg\exists x(\varphi \to \forall v\varphi(v))$, $\qquad$ $\forall x(\varphi \vee \neg\varphi) \,\&\, \forall x\neg\neg\varphi \to \neg\neg\forall x\varphi$,

    $\neg\neg\forall x\varphi \to \forall x\neg\neg\varphi$, $\qquad$ $\forall x(\varphi \vee \neg\varphi) \to (\neg\neg\exists x\varphi \to \exists x\varphi)$.

31. Dokažte, že schéma DNS platí ve všech konečných kripkovských strukturách.

32. Navrhněte definici harropovské formule i pro predikátovou logiku, předpokládejte platnost věty o eliminovatelnosti řezů a dokažte predikátovou verzi cvičení 14: když množina Γ obsahuje pouze harropovské formule, $\Delta \neq \emptyset$ a sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ je dokazatelný v kalkulu GJ, pak existuje formule $\varphi \in \Delta$ taková, že i sekvent $\langle\, \Gamma \Rightarrow \varphi \,\rangle$ je dokazatelný v kalkulu GJ.

33. Dokažte, že analogické tvrzení, jako bylo v předchozím cvičení dokázáno pro disjunkci, platí i pro existenční kvantifikátor: když φ je formule v L, když Γ je množina harropovských formulí v L a když sekvent $\langle\, \Gamma \Rightarrow \exists x \varphi \,\rangle$ je dokazatelný v kalkulu GJ, pak existuje term t v jazyce L takový, že i sekvent $\langle\, \Gamma \Rightarrow \varphi_x(t) \,\rangle$ je dokazatelný.

34. Navrhněte definici negativní formule i pro predikátovou logiku a dokažte, že formule $\neg\neg\varphi \to \varphi$ je v kalkulu GJ dokazatelná pro každou negativní formuli φ.

35. Nechť funkce g je definovaná rovnostmi

$$\varphi^{\mathrm{g}} = \neg\neg\varphi, \qquad \text{je-li } \varphi \text{ atomická},$$
$$(\varphi \,\&\, \psi)^{\mathrm{g}} = \varphi^{\mathrm{g}} \,\&\, \psi^{\mathrm{g}}, \qquad (\varphi \to \psi)^{\mathrm{g}} = \varphi^{\mathrm{g}} \to \psi^{\mathrm{g}}, \qquad (\neg\varphi)^{\mathrm{g}} = \neg\varphi^{\mathrm{g}},$$
$$(\varphi \vee \psi)^{\mathrm{g}} = \neg(\neg\varphi^{\mathrm{g}} \,\&\, \neg\psi^{\mathrm{g}}), \qquad (\exists x\varphi)^{\mathrm{g}} = \neg\forall x\neg\varphi^{\mathrm{g}}, \qquad (\forall x\varphi)^{\mathrm{g}} = \forall x\varphi^{\mathrm{g}}.$$

Dokažte, že libovolná predikátová formule φ je klasicky logicky platná, právě když formule φ^{g} je intuicionisticky logicky platná. Funkce $\varphi \mapsto \varphi^{\mathrm{g}}$ je tedy také interpretací klasické predikátové logiky v intuicionistické.

Návod. Nejprve dokažte predikátovou analogii věty 5.1.22. Pak uvažte, že každá formule φ^{g} je negativní formulí a užijte předchozí cvičení.

5.2 Gödelova fuzzy logika (napsal Petr Hájek)

V tomto oddílu se seznámíme s jednou z významných vícehodnotových logik, nazývanou Gödelova logika. To potřebuje vysvětlení. Jak bylo řečeno v úvodu k této kapitole, klasická logika je dvouhodnotová, má dvě pravdivostní hodnoty. To lze zobecnit tak, že pravdivostní hodnoty 1 (pravda) a 0 (nepravda) považujeme za extremální a mezi nimi připouštíme mezilehlé hodnoty částečné pravdivosti. (Hned na začátku čtenáře důrazně varujeme, aby se nepokoušel myslet na pravděpodobnost, jde o něco zcela jiného.) První, kdo se takovými logikami zabýval, byl polský logik Jan Łukasiewicz ([56] jsou jeho sebrané spisy). Později zavedl jiné systémy vícehodnotové logiky E. Post [65]. V souvislosti s intuicionistickou logikou studoval vícehodnotové logiky A. Heyting [36] a také Kurt Gödel. Jeho kratičká práce [26] se stala základem logiky, kterou zde probereme. Z dalších významných autorů, kteří se vícehodnotovými logikami zabývali, jmenujme alespoň tyto: Moisil, Rose, Rosser, Chang, Belluce, Scott. V roce 1965 vyšla Zadehova práce [100], která se stala základem teorie fuzzy množin a fuzzy logiky. „Fuzzy“ znamená „roztřepený“, „neostrý“; za fuzzy považujeme vágní pojmy jako „malý“, „velký“, „vysoký“ apod.,

které nemají ostré hranice (to souvisí s některými známými logickými paradoxy, tím se však nezabýváme).

Fuzzy logiku tedy můžeme chápat jako logiku *komparativní pravdy*: výroky mohou být *více či méně pravdivé*. To je rozumná myšlenka. Potíž byla v tom, že po řadu let (desetiletí) se fuzzy logikou zabývali nelogikové (inženýři, odborníci na řízení) a dělali to, co uměli. Matematikové a logikové nad tím ohrnovali nos a jen výjimečně se fuzzy logikou zabývali. Čestnou výjimkou jsou např. monografie S. Gottwalda [27], [28]. Zadeh sám správně rozlišuje fuzzy logiku v širokém smyslu (cokoli, co se týká fuzzy pojmů a množin) a v úzkém smyslu (vícehodnotové logické kalkuly vhodné pro formulaci usuzování za vágnosti). V současné době je fuzzy logika v úzkém smyslu předmětem intenzívního matematického studia a ukazuje se, že kalkuly fuzzy logiky mají pozoruhodné (a krásné) logické vlastnosti. Gödelova logika je jedním z několika takových kalkulů. Gödel sám pochopitelně na žádnou fuzzy logiku nemyslel (ta přišla o 33 let později); použil vícehodnotovou logiku jako prostředek studia logiky intuicionistické. A protože jsme s intuicionistickou logikou seznámeni, bude se nám Gödelova logika dobře studovat a vyložíme mimo jiné i původní Gödelův výsledek z r. 1932. Probereme jak výrokovou, tak predikátovou Gödelovu logiku a na závěr se stručně zmíníme o některých jiných fuzzy logikách. Čtenáři, který se zajímá o tuto problematiku hlouběji, doporučujeme monografii [34].

5.2.1 Gödelova výroková fuzzy logika

Gödelovu výrokovou fuzzy logiku budeme značit písmenem G. *Formule* jsou budovány z výrokových atomů pomocí logických spojek $\&$, $\vee$, $\rightarrow$, $\neg$ (stejně jako v klasické a v intuicionistické logice). Předpokládáme, že výrokových atomů je konečně nebo spočetně mnoho. *Standardní množina pravdivostních hodnot* logiky G je reálný jednotkový interval $[\![0,1]\!]$; *pravdivostní ohodnocení* je zobrazení v přiřazující každému atomu p hodnotu $v(p) \in [\![0,1]\!]$. *Pravdivostní funkce logických spojek* jsou definovány následovně.

Pravdivostní funkce konjunkce je funkce $\min(x,y)$, (minimum); pravdivostní funkce disjunkce je $\max(x,y)$. Pravdivostní funkce implikace je funkce $(x \Rightarrow y)$ definovaná takto:

$$x \Rightarrow y = \begin{cases} 1 & \text{jestliže } x \leq y \\ y & \text{jinak.} \end{cases}$$

Pravdivostní funkce negace je funkce $x \mapsto -x$ definovaná předpisem $-x = (x \Rightarrow 0)$; platí tedy $-0 = 1$ a $-x = 0$ pro $x > 0$ (hned si všimněme, že $-(-x)$ se obecně nerovná x).

Množinu $[\![0,1]\!]$ s operacemi max a min, právě definovanou funkcí $\Rightarrow$ a vytčenými prvky 0 a 1 značíme $[\![0,1]\!]_{\mathrm{G}}$ a nazýváme *standardní G-algebrou* (obecné G-algebry definujeme později).

Pomocí pravdivostních funkcí se každé ohodnocení výrokových atomů jednoznačně rozšíří na ohodnocení v všech formulí takové, že pro každé dvě formule

A a B platí

$$\begin{aligned} v(A \,\&\, B) &= \min(v(A), v(B)), \\ v(A \vee B) &= \max(v(A), v(B)), \\ v(A \to B) &= (v(A) \Rightarrow v(B)), \\ v(\neg A) &= -v(A). \end{aligned}$$

Formule A je *tautologie* (přesněji: $[\![0,1]\!]_{\mathrm{G}}$*-tautologie*), jestliže $v(A) = 1$ pro každé ohodnocení v. Nyní uvidíme souvislost logiky G s intuicionistickou logikou.

Věta 5.2.1 *(a) Všechny axiomy hilbertovského kalkulu HJ pro intuicionistickou logiku jsou* $[\![0,1]\!]_{\mathrm{G}}$*-tautologie.*
(b) Dále každá formule tvaru $(A \to B) \vee (B \to A)$ *je* $[\![0,1]\!]_{\mathrm{G}}$*-tautologie.*
(c) $[\![0,1]\!]_{\mathrm{G}}$*-tautologie jsou uzavřeny na modus ponens: když* A *a* $A \to B$ *jsou* $[\![0,1]\!]_{\mathrm{G}}$*-tautologie, pak i* B *je* $[\![0,1]\!]_{\mathrm{G}}$*-tautologie.*
(d) Avšak formule $A \vee \neg A$ *obecně není* $[\![0,1]\!]_{\mathrm{G}}$*-tautologie.*

Důkazu předřadíme lemma, které je užitečné na více místech:

Lemma 5.2.2 *Pro každé* $x, y, z \in [\![0,1]\!]$ *platí* $z \le (x \Rightarrow y)$*, právě když* $\min(x, z) \le y$*. (Tomu se říká, že operace* $\Rightarrow$ *je* reziduum *operace maxima.)*

Důkaz Je-li $x \le y$, pak $(x \Rightarrow y) = 1$ a podmínky $z \le 1$ a $\min(x, z) \le y$ platí pro každé z. Je-li $x > y$, pak $(x \Rightarrow y) = y$, a zřejmě v tomto případě máme $z \le y$, právě když $\min(x, z) \le y$. QED

Důkaz věty 5.2.1 (a) Pro většinu axiomů je ověření tautologičnosti velmi lehké. Ověříme axiom A2. Následující řádky jsou ekvivalentní:

$$\begin{aligned} 1 &\le (a \Rightarrow (b \Rightarrow c)) \Rightarrow ((a \Rightarrow b) \Rightarrow (a \Rightarrow c)) \\ a \Rightarrow (b \Rightarrow c) &\le (a \Rightarrow b) \Rightarrow (a \Rightarrow c) \\ \min(a \Rightarrow b, a \Rightarrow (b \Rightarrow c)) &\le a \Rightarrow c \\ \min(a, a \Rightarrow b, a \Rightarrow (b \Rightarrow c)) &\le c. \end{aligned}$$

Všimněme si, že $\min(a, a \Rightarrow b) \le \min(a, b)$; tedy $\min(a, a \Rightarrow b, a \Rightarrow (b \Rightarrow c)) \le \min(a, b, a \Rightarrow (b \Rightarrow c)) \le \min(a, b, b \Rightarrow c) \le \min(a, b, c) \le c$. Tím je dokázán poslední ze čtyř navzájem ekvivalentních řádků, a tedy i první.

(b) Zřejmě $\max(x \Rightarrow y, y \Rightarrow x) = 1$, neboť $x \le y$ nebo $y \le x$.

(c) Je-li $v(A) = 1$ a $v(B) < 1$, je $v(A \to B) = v(B) < 1$; tedy je-li $v(A) = 1$ a $v(A \to B) = 1$, pak $v(B) = 1$.

(d) Pro $v(p) = \frac{1}{2}$ je $v(p \vee \neg p) = \max(\frac{1}{2}, 0) = \frac{1}{2}$. QED

Můžeme tedy definovat *hilbertovský kalkulus* pro logiku G: axiomy jsou axiomy kalkulu HJ a dále všechny instance schématu $(A \to B) \vee (B \to A)$ (nazývaného *axiom prelinearity*), odvozovací pravidlo je modus ponens. Protože jiným než hilbertovským kalkulem se v případě logiky G nezabýváme, značíme právě definovaný kalkulus opět písmenem G. Kalkulus G je korektní vůči $[\![0,1]\!]_{\mathrm{G}}$-tautologiím: každá formule dokazatelná v G je $[\![0,1]\!]_{\mathrm{G}}$-tautologie.

Vidíme, že logika G je silnější než intuicionistická a slabší než klasická (takovým logikám se říká *intermediární*). O logice G jsme se už nepřímo zmínili ve cvičení 26 oddílu 5.1.

Teorií rozumíme (jako obvykle) libovolnou množinu formulí — vlastních axiomů této teorie. Pojem důkazu je definován obvyklým způsobem: *důkaz* v teorii T (nad logikou G) je posloupnost formulí $A_1, \ldots, A_n$, z nichž každá je buď axiom logiky G, nebo vlastní axiom teorie T (tj. prvek množiny T), nebo je odvozena z některých předchozích formulí pomocí odvozovacího pravidla. $T \vdash A$ (přesněji $T \vdash_{\mathrm{G}} A$) značí, že formule A je dokazatelná v teorii T (nad logikou G).

Pro logiku G platí *věta o dedukci* v obvyklém znění: $T \cup \{A\} \vdash_{\mathrm{G}} B$, právě když $T \vdash_{\mathrm{G}} A \to B$ (k tomu stačí axiomy A1 a A2).

Ukážeme teď, že (na rozdíl od intuicionistické logiky) disjunkce je v logice G vyjádřitelná pomocí ostatních spojek:

Lemma 5.2.3 *Formule* $A \vee B$ *a* $((A \to B) \to B) \& ((B \to A) \to A)$ *jsou nad logikou G ekvivalentní pro každou volbu formulí* A *a* B.

Důkaz Označme C formuli $((A \to B) \to B) \,\&\, ((B \to A) \to A)$. Snadno lze ověřit, že jak z předpokladu A, tak z předpokladu B lze v logice G dokázat jak formuli $(A \to B) \to B$, tak formuli $(B \to A) \to A$. Z toho a užitím axiomů A4–A7 se dokáže $\vdash_{\mathrm{G}} A \vee B \to C$, a to stejně, jako kdybychom pracovali v klasické nebo v intuicionistické logice. Obráceně platí

$$\vdash_{\mathrm{G}} (A \to B) \to (((A \to B) \to B) \to B),$$
$$\vdash_{\mathrm{G}} (A \to B) \to (C \to A \vee B).$$

Zcela analogicky se dokáže

$$\vdash_{\mathrm{G}} (B \to A) \to (C \to A \vee B).$$

Tedy

$$\vdash_{\mathrm{G}} (A \to B) \vee (B \to A) \to (C \to A \vee B).$$

Díky tomu, že formule $(A \to B) \vee (B \to A)$ je axiom, máme $\vdash_{\mathrm{G}} C \to A \vee B$. QED

Nic takového, co jsme právě udělali pro disjunkci, nelze udělat pro konjunkci ani pro implikaci. Metody, kterými je v [9] dokázáno, že konjunkci ani implikaci v intuicionistické logice nelze vyjádřit pomocí ostatních logických spojek, lze totiž přizpůsobit i pro logiku G, viz [89].

Zobecníme nyní pojem struktury pravdivostních hodnot. *G-algebrou* budeme rozumět libovolnou lineárně uspořádanou množinu $\mathbf{L} = (L, \leq)$ s nejmenším prvkem $0_{\mathbf{L}}$, největším prvkem $1_{\mathbf{L}}$ a operacemi minima $\min(x, y)$, maxima $\max(x, y)$ a rezidua $x \Rightarrow y$ definovaného takto: pro $x \leq y$ je $x \Rightarrow y = 1$, pro $x > y$ je $x \Rightarrow y = y$.[2]

L-ohodnocení výrokových atomů je zobrazení v přiřazující každému výrokovému atomu p hodnotu $v(p) \in L$. To se rozšíří na ohodnocení $v(A)$ libovolné formule A užitím operací algebry **L** jako pravdivostních funkcí (pochopitelně definujeme $-x = (x \Rightarrow 0_{\mathbf{L}})$). Formule A je **L**-*tautologie*, jestliže $v(A) = 1_{\mathbf{L}}$ pro každé **L**-ohodnocení v. Snadno lze ověřit *korektnost* kalkulu G vůči takto zobecněné sémantice: je-li formule A dokazatelná v kalkulu G, pak A je **L**-tautologií pro každou G-algebru **L**.

Nadto: **L**-*modelem* teorie T rozumíme **L**-ohodnocení v takové, že pro každou formuli $A \in T$ platí $v(A) = 1_{\mathbf{L}}$. *Silná korektnost* říká, že je-li formule A dokazatelná v T (nad logikou G), pak $v(A) = 1_{\mathbf{L}}$ pro každý **L**-model teorie T.

Pochopitelně nás zajímá, zda to platí také obráceně. Kladnou odpověď dá věta o úplnosti, ke které směřujeme.

Nejprve si uvědomme některé základní vlastnosti G-algeber. Připomeňme, že *izomorfismus* dvou lineárně uspořádaných množin $(L_1, \leq_1)$ a $(L_2, \leq_2)$ je prosté zobrazení f množiny L_1 na L_2 zachovávající uspořádání, tj. splňující podmínku, že pro každé $a, b \in L_1$ je $a \leq_1 b$, právě když $f(a) \leq_2 f(b)$.

Lemma 5.2.4 *(a) Každý izomorfismus f lineárně uspořádaných množin $(L_1, \leq_1)$ a $(L_2, \leq_2)$ majících nejmenší a největší prvek 0_i, 1_i $(i = 1, 2)$ zobrazuje 0_1 na 0_2, zobrazuje 1_1 na 1_2 a zachovává operace maxima, minima a rezidua, tj. je izomorfismem G-algeber daných uspořádanými množinami $(L_1, \leq_1)$ a $(L_2, \leq_2)$.*
(b) Každé dvě konečné G-algebry stejné mohutnosti jsou izomorfní.
(c) Každou konečnou nebo spočetnou G-algebru lze izomorfně vnořit do G-algebry racionálních čísel z intervalu $[\![0, 1]\!]$.

Důkaz Jde vesměs o zřejmé věci, pro (a) ukažme například, že $f(1_1) = 1_2$ a $f(x \Rightarrow_1 y) = f(x) \Rightarrow_2 f(y)$. Skutečně, je-li 0_1 nejmenší v L_1, tj. $0_1 \leq x$ pro každé $x \in L_1$, pak $f(0_1) \leq f(x)$ pro každé $x \in L_1$, a tedy (jelikož f je zobrazení na L_2) $f(0_1) \leq y$ pro libovolné $y \in L_2$, tedy $f(0_1)$ je nejmenší v L_2, $f(0_1) = 0_2$. Podobně pro reziduum: ať $x, y \in L_1$. Pak *buďto* $x \leq_1 y$, a pak $x \Rightarrow_1 y = 1_1$, $f(x \Rightarrow_1 y) = 1_2$, $f(x) \leq_2 f(y)$, tedy $f(x) \Rightarrow_2 f(y) = 1_2$; *nebo* $x >_1 y$, a pak $x \Rightarrow_1 y = y$, $f(x) >_2 f(y)$, tedy $f(x) \Rightarrow_2 f(y) = f(y)$. V obou případech $f(x \Rightarrow_1 y) = f(x) \Rightarrow_2 f(y)$.

Tvrzení (b) a (c) plynou z toho, že obdobná tvrzení platí pro lineárně uspořádané množiny a z (a) víme, že izomorfismus vůči uspořádání je zároveň izomorfismem ve smyslu G-algeber. Vskutku: každé dvě lineárně uspořádané množiny téže konečné mohutnosti jsou izomorfní a každou nejvýše spočetnou lineárně uspořádanou

[2] Vlastně bychom měli mluvit o *lineárně uspořádaných G-algebrách;* obvyklý pojem G-algebry je obecnější. My však s jinými než lineárně uspořádanými G-algebrami nebudeme pracovat, a proto použijeme naši terminologii (srov. [34]).

množinu s nejmenším a největším prvkem lze izomorfně zobrazit na nějakou podmnožinu uspořádaného racionálního intervalu $[\![0,1]\!]$ tak, že obrazem nejmenšího prvku je 0 a obrazem největšího prvku je 1. QED

Věta 5.2.5 *Pro libovolnou formuli A platí: A je $[\![0,1]\!]_{\mathrm{G}}$-tautologie, právě když A je $\mathbf{L}$-tautologie pro každou G-algebru $\mathbf{L}$.*

Důkaz Když A je $\mathbf{L}$-tautologií pro každou G-algebru $\mathbf{L}$, pak i pro $\mathbf{L} = [\![0,1]\!]_{\mathrm{G}}$. Obráceně, jestliže $\mathbf{L}$ je G-algebra a v je $\mathbf{L}$-ohodnocení takové, že $v(A) < 1_{\mathbf{L}}$, pak vezměme množinu X obsahující $0_{\mathbf{L}}$ a $1_{\mathbf{L}}$ a hodnoty všech výrokových atomů formule A v ohodnocení v. Množina X je konečná a lze ji izomorfně vnořit do $[\![0,1]\!]$ se zachováním nejmenšího a největšího prvku. Buď f takový izomorfismus; víme, že f zachovává i operace G-algebry (tj. operace max, min a $\Rightarrow$). Nechť v' je $[\![0,1]\!]_{\mathrm{G}}$-ohodnocení splňující $v'(p) = f(v(p))$ pro každý výrokový atom p vyskytující se v A; pak pro každou podformuli B formule A máme $v'(B) = f(v(B))$ a speciálně $v'(A) = f(v(A)) < 1$ (protože $v(A) < 1_{\mathbf{L}}$). QED

Dokázali jsme vlastně více, než jsme tvrdili: Jestliže A není $[\![0,1]\!]_{\mathrm{G}}$-tautologie, pak umíme zkonstruovat *konečnou* G-algebru $\mathbf{L}$ takovou, že A není $\mathbf{L}$-tautologie. Body nosné množiny L struktury $\mathbf{L}$ jsou čísla 0 a 1, a dále hodnoty $v(p_i)$, kde $p_1, .., p_n$ jsou atomy formule A. Množina L má tedy nejvíce $n+2$ prvků; má-li méně, můžeme další libovolně přidat. Máme tedy následující důsledek:

Důsledek 5.2.6 *Buď A formule obsahující n výrokových atomů. A je $[\![0,1]\!]_{\mathrm{G}}$-tautologie, právě když je $\mathbf{L}_{n+2}$-tautologie, kde $\mathbf{L}_{n+2}$ je G-algebra mající přesně $n+2$ prvků (struktura $\mathbf{L}_{n+2}$ je určena jednoznačně až na izomorfismus).*

Definice 5.2.7 *Teorie T je* úplná (nad logikou G)*, jestliže pro každou dvojici formulí A a B platí $T \vdash A \to B$ nebo $T \vdash B \to A$ (nebo obojí).*

Lemma 5.2.8 *Buď T teorie a C formule nedokazatelná v T. Pak existuje úplná teorie $T' \supseteq T$ taková, že C je nedokazatelná v T'.*

Důkaz Protože je nejvýše spočetně mnoho výrokových atomů, lze uspořádané dvojice všech formulí seřadit do spočetné posloupnosti

$$[A_0, B_0], \quad [A_1, B_1], \quad [A_2, B_2], \quad \ldots$$

Položme $T_0 = T$ a předpokládejme, že již máme teorii $T_n \supseteq T_0$ takovou, že pro všechna $i < n$ platí $T_n \vdash A_i \to B_i$ nebo $T_n \vdash B_i \to A_i$, a přitom $T_n \nvdash C$. Tvrdíme, že pak buďto $T_n \cup \{A_n \to B_n\} \nvdash C$, nebo $T_n \cup \{B_n \to A_n\} \nvdash C$; v prvním případě bude $T_{n+1} = T_n \cup \{A_n \to B_n\}$, v druhém $T_{n+1} = T_n \cup \{B_n \to A_n\}$. Dokazujeme sporem: ať C je dokazatelná jak v $T_n \cup \{A_n \to B_n\}$, tak v $T_n \cup \{B_n \to A_n\}$. Dle věty o dedukci je $T_n \vdash (A_n \to B_n) \to C$ a $T_n \vdash (B_n \to A_n) \to C$, tedy

$$T_n \vdash [(A_n \to B_n) \vee (B_n \to A_n)] \to C,$$

a tedy $T_n \vdash C$, což je ve sporu s předpokladem (postřehli jste, že výraz v hranatých závorkách je axiom logiky G). Stačí tedy vzít za T' sjednocení všech teorií T_n; zřejmě $T' \supseteq T$, teorie T' je úplná a $T' \nvdash C$ (neboť každý důkaz v T' je důkazem v některé T_n). QED

Definice 5.2.9 *Nechť T je úplná teorie. Pro každou formuli A nechť $[A]_T$ je množina $\{ B ; T \vdash A \equiv B \}$ (třída všech formulí ekvivalentních s A v T). Množinu všech tříd $\{ [A]_T ; A \text{ formule} \}$ označme L_T. Definujme, že $[A]_T \leq [B]_T$, jestliže $T \vdash A \to B$.*

Poznamenejme, že relace $\leq$ je dobře definována: platí-li $[A]_T = [A']_T$, pak $T \vdash A \to B$, právě když $T \vdash A' \to B$; a podobně $T \vdash B \to A$, právě když $T \vdash B \to A'$.

Lemma 5.2.10 *Nechť T je úplná teorie. Pak*
(a) Relace $\leq$ je lineární uspořádání množiny L_T, největší prvek je třída všech formulí dokazatelných v T a nejmenší prvek je třída všech formulí vyvratitelných v T (tj. takových formulí B, že $T \vdash \neg B$).
(b) Pro libovolné dvě formule A a B platí:

$$\min([A]_T, [B]_T) = [A \,\&\, B]_T,$$
$$\max([A]_T, [B]_T) = [A \vee B]_T,$$
$$[A]_T \Rightarrow [B]_T = [A \to B]_T,$$

kde max, min *a* $\Rightarrow$ *jsou operace definované pomocí uspořádání* $\leq$.

Důkaz (a) Připomeňme dokazatelnost následujících formulí v G:

$$A \to A,$$
$$(A \to B) \,\&\, (B \to C) \to (A \to C),$$
$$(A \to B) \,\&\, B \to A) \to (A \equiv B).$$

Z toho dostáváme

$$[A] \leq [A],$$
$$\text{jestliže } [A] \leq [B] \text{ a } [B] \leq [C], \text{ pak } [A] \leq [C],$$
$$\text{jestliže } [A] \leq [B] \text{ a } [B] \leq [A], \text{ pak } [A] = [B],$$

(vynecháváme index T). Protože teorie T je úplná, pro každou dvojici A a B formulí buď $T \vdash A \to B$, nebo $T \vdash B \to A$, platí tedy $[A] \leq [B]$ nebo $[B] \leq [A]$; relace $\leq$ je lineární uspořádání. Zbytek je zřejmý.

(b) Je-li $[A] \leq [B]$, tedy $T \vdash A \to B$, pak $T \vdash A \equiv (A \,\&\, B)$, takže $\min([A], [B]) = [A] = [A \,\&\, B]$. Podobně z $[A] \leq [B]$ plyne $T \vdash B \equiv (A \vee B)$.

Je-li $[A] \leq [B]$, pak $T \vdash A \to B$, tedy $[A \to B] = 1_{L_T} = [A] \Rightarrow [B]$. Nechť tedy $[A] > [B]$, tj. $T \nvdash A \to B$ a $T \vdash B \to A$. Chceme ověřit $T \vdash (A \to B) \equiv B$. Jedna implikace je zřejmá: $T \vdash B \to (A \to B)$. Vyšetřme dvojici formulí A a $A \to B$. Víme

$$T \vdash (A \,\&\, (A \to B)) \to B, \qquad (*)$$

a dále buď $T \vdash A \to (A \to B)$, nebo $T \vdash (A \to B) \to A$. První možnost by vzhledem k $(*)$ dávala $T \vdash A \to B$ (neboť v T by byly dokazatelné formule $A \to (A \,\&\, A)$, $(A \& A) \to (A \& (A \to B))$ a $(A \& (A \to B)) \to B$, což je ve sporu s předpokladem); tedy nastává druhá možnost $T \vdash (A \to B) \to A$ a z ní podobně plyne $T \vdash (A \to B) \to B$. Tedy v případě $[A] > [B]$ dostáváme $[A \to B] = [B] = [A] \Rightarrow [B]$. QED

G-algebru určenou uspořádanou množinou $(L_T, \leq)$ značíme $\mathbf{L}_T$ a nazýváme ji *G-algebrou teorie T*.

Věta 5.2.11 (o silné úplnosti kalkulu G) *Nechť T je teorie nad logikou G a nechť A je formule. Následující tři tvrzení jsou ekvivalentní:*

(i) $T \vdash_G A$,

(ii) $v(A) = 1$ *pro každý* $[\![0,1]\!]_{\mathrm{G}}$*-model v teorie T (A je pravdivá v každém modelu teorie T nad standardní G-algebrou),*

(iii) $v_{\mathbf{L}}(A) = 1$ *pro každou G-algebru* $\mathbf{L}$ *a každý* $\mathbf{L}$*-model v teorie T (A je pravdivá v každém modelu teorie T nad libovolnou G-algebrou).*

Důkaz Implikace (i) ⇒ (iii) je silná korektnost (viz předchozí výklad); implikace (iii) ⇒ (ii) je evidentní. Zbývá předpokládat (ii) a dokázat (i), neboli: předpokládáme $T \nvdash A$ a najdeme $[\![0,1]\!]_{\mathrm{G}}$-model v teorie T, v němž $v(A) < 1$.

Nechť S je úplné rozšíření teorie T, pro které platí $S \nvdash A$. Vyšetříme algebru $\mathbf{L}_S$. Protože předpokládáme spočetný jazyk, je množina L_S (tříd S-ekvivalentních formulí) spočetná. Definujme $\mathbf{L}_S$-ohodnocení v takto: pro každý výrokový atom p je $v(p) = [p]_S$. Z vlastností algebry $\mathbf{L}_S$ ihned plyne, že $v_{\mathbf{L}_S}(B) = [B]_S$ pro libovolnou formuli B; přitom pokud je B axiom teorie T, je $[B]_S = 1_{\mathbf{L}_S}$, ale $[A]_S < 1_{\mathbf{L}_S}$, neboť $S \nvdash A$. Tedy v je $\mathbf{L}_S$-ohodnocení, v němž A není pravdivá (nemá hodnotu $1_{\mathbf{L}_S}$). My však chceme $[\![0,1]\!]_{\mathrm{G}}$-model; proto použijeme lemma 5.2.4(c) a vnoříme $\mathbf{L}_S$ do $[\![0,1]\!]_{\mathrm{G}}$ pomocí vhodného izomorfismu f (dokonce lze uvést f takový, že zobrazuje $\mathbf{L}_S$ do racionálních čísel intervalu $[\![0,1]\!]$, ale to je teď nepodstatné). Definujme $[\![0,1]\!]_{\mathrm{G}}$-ohodnocení v' takto: $v'(p) = f(v(p))$. Pro všechny formule B platí $v'(B) = f(v_{\mathbf{L}_S}(B))$. Tedy v' je $[\![0,1]\!]_{\mathrm{G}}$-model teorie S. Tím spíše v' je $[\![0,1]\!]_{\mathrm{G}}$-model teorie T a platí $v'(A) < 1$. QED

Důsledek 5.2.12 (úplnost kalkulu G) *Pro libovolnou formuli A jsou následující čtyři tvrzení ekvivalentní:*

(i) A je dokazatelná v logice G,

(ii) A je $[\![0,1]\!]_{\mathrm{G}}$*-tautologie,*

(iii) A je $\mathbf{L}$*-tautologie pro každou G-algebru* $\mathbf{L}$*,*

(iv) A je $\mathbf{L}_{n+2}$*-tautologie, kde n je počet výrokových atomů ve formuli A (a* $\mathbf{L}_{n+2}$ *je $(n+2)$-prvková G-algebra).*

Úplnost logiky G (vůči tautologiím nad racionálním intervalem $[\![0,1]\!] \cap \mathbb{Q}$) dokázal M. Dummett, viz [18].

Nyní vyložíme výsledky o výpočtové složitosti Gödelovy fuzzy výrokové logiky. Nechť G-Taut značí množinu všech tautologií logiky G a G-Sat značí množinu všech formulí splnitelných v logice G (A je v G-Sat, jestliže existuje $[\![0,1]\!]_{\mathrm{G}}$-ohodnocení v takové, že $v(A) = 1$). Připomeňme, že pro analogické množiny Taut a Sat klasické (booleovské) logiky platí, že Sat je *NP*-kompletní a Taut je *coNP*-kompletní (viz kapitolu 2). Ukažme, že pro množiny G-Sat a G-Taut platí totéž. Pro jistotu ještě připomeňme, že G-Taut $\neq$ Taut: například formule $p \vee \neg p$ je v Taut a není v G-Taut.

Věta 5.2.13 *Platí* G-Sat = Sat. *Množina* G-Sat *je tedy* *NP*-*kompletní.*

Důkaz Zřejmě Sat $\subseteq$ G-Sat (je-li A splnitelná v klasické logice ohodnocením v s hodnotami 0 a 1, pak totéž ohodnocení v dává formuli A hodnotu 1 i ve smyslu algebry $[\![0,1]\!]_{\mathrm{G}}$). Obráceně nechť $A \in$ G-Sat a nechť v je $[\![0,1]\!]_{\mathrm{G}}$-ohodnocení takové, že $v(A) = 1$ ve smyslu $[\![0,1]\!]_{\mathrm{G}}$. Definujme ohodnocení v' takto: $v'(p) = 0$, jestliže $v(p) = 0$; $v'(p) = 1$, pokud $v(p) > 0$. Ověřte, že pro každou formuli B platí: $v'(B) = 0$, jestliže $v(B) = 0$; $v'(B) = 1$, jestliže $v(B) > 0$ (indukcí podle počtu logických spojek ve formuli B). Tedy $v'(A) = 1$ a $A \in$ Sat. QED

Věta 5.2.14 *Množina* G-Taut *je* *coNP*-*kompletní.*

Důkaz Máme ukázat, že množina G-Taut je v třídě *coNP* a že je v ní kompletní. K první věci stačí ukázat, že množina všech formulí, které nejsou G-tautologie, je v *NP*. Jde o to ukázat, že existuje nedeterministický algoritmus pracující v polynomiálním čase, který přijme formuli A, právě když pro nějaké ohodnocení v platí $v(A) < 1$. Činnost takového algoritmu popíšeme neformálně; čtenář může vypracovat detaily. Uvědomme si, že dle důsledku 5.2.6 stačí ohodnocovat čísly $0, \frac{1}{k+1}, \frac{2}{k+2}, \ldots, \frac{k}{k+1}, 1$, kde k je počet atomů formule A. Algoritmus tedy nedeterministicky uhodne takové ohodnocení a pak deterministicky spočítá příslušnou hodnotu dané formule. Kompletnost ukážeme tak, že udáme funkci f počitatelnou v logaritmickém prostoru a takovou, že pro libovolnou formuli A je $A \in$ Taut, právě když $f(A) \in$ G-Taut. Takovou funkcí je například funkce, která ve formuli A nahradí každý atom p jeho dvojitou negací $\neg\neg p$ (ověřte). QED

Nyní si ještě položme otázku, zda logika G umožňuje odvozovat *částečně* pravdivé důsledky z *částečně* pravdivých předpokladů. Ukážeme, že ano. Buď $r \in [\![0,1]\!]$; říkejme, že formule A je *r-pravdivá* při ohodnocení v, jestliže $v(A) \geq r$ (nyní pracujeme s $[\![0,1]\!]_{\mathrm{G}}$-ohodnoceními).

Lemma 5.2.15 (o korektnosti vůči r-pravdivosti) *Nechť $r \in [\![0,1]\!]$ a dále nechť T je teorie, A formule dokazatelná v teorii T a v pravdivostní ohodnocení. Jestliže každý axiom teorie T je r-pravdivý, pak i formule A je r-pravdivá při ohodnocení v.*

Důkaz Jediné, co je třeba ověřit, je skutečnost, že pravidlo modus ponens zachovává r-pravdivost.

Nechť $v(C) \geq r$ a $v(C \to D) \geq r$. Kdyby $v(D) < r$, bylo by $v(C \to D) = v(D) < r$, což není. Tedy $v(D) \geq r$. Vidíme tedy, že je-li $v(B) \geq r$ pro každý axiom $B \in T$, pak každý důkaz v T nad G sestává jen z formulí r-pravdivých při ohodnocení v. QED

Toto tvrzení lze dokonce obrátit, logika G je silně úplná vůči r-pravdivosti. Říkejme, že v je *r-model teorie T*, jestliže $v(B) \geq r$ pro každý axiom $B \in T$.

Věta 5.2.16 *Nechť T je teorie, A formule a $0 < r \leq 1$. Pak $T \vdash_G A$, právě když A je r-pravdivá v každém r-modelu v teorie T, tj. právě když $v(A) \geq r$ pro každé $[\![0,1]\!]_{\mathrm{G}}$-ohodnocení v, které každému prvku $B \in T$ přiřazuje hodnotu alespoň r.*

Důkaz V jednom směru jde o předcházející lemma. Obráceně nechť formule A je r-pravdivá v každém r-modelu teorie T. Je-li $r = 1$, jde o úplnost dokázanou výše. Je-li $0 < r < 1$, pak si všimněme, že pro každé $0 < s < 1$ platí, že A je s-pravdivá v každém s-modelu teorie T. Pro dané s stačí vzít libovolné prosté rostoucí zobrazení f intervalu $[\![0,1]\!]$ na sebe takové, že $f(r) = s$. Pro daný s-model v teorie T buď $v'(p) = f^{-1}(v(p))$ pro každý výrokový atom p. Všimněme si, že $v(B) = f(v'(B))$ pro každou formuli B; jelikož v' je r-model teorie T, je $v'(A) \geq r$, a tedy $v(A) = f(v'(A)) \geq s$. QED

Výklad Gödelovy výrokové fuzzy logiky uzavřeme důkazem Gödelova výsledku z r. 1932, kvůli němuž se Gödel vícehodnotovou logikou zabýval. Pro tento účel definujme:

Definice 5.2.17 Konečná sémantika *výrokové logiky je libovolná struktura tvaru*

$$\mathbf{H} = \langle H, *, \oplus, \Rightarrow, -, 1_{\mathbf{H}} \rangle,$$

kde H je konečná (neprázdná) množina, $*$, $\oplus$ a $\Rightarrow$ jsou binární operace na H (chápané jako pravdivostní funkce konjunkce, disjunkce a implikace), $-$ je unární operace na H (pravdivostní funkce negace) a $1_{\mathbf{H}}$ je vytčený prvek struktury $\mathbf{H}$ (pravda). Struktura $\mathbf{H}$ je n-hodnotová sémantika*, jestliže její nosná množina H má n prvků.*

Každá G-algebra $\mathbf{L}_{n+2}$ je příkladem $(n+2)$-hodnotové sémantiky. Také dvouhodnotová sémantika klasické výrokové logiky je příkladem sémantiky vyhovující definici 5.2.17. Protože každá sémantika $\mathbf{H}$ vyhovující definici 5.2.17 je konečná, lze pravdivostní funkce zadávat tabulkami.

Ke konečné sémantice $\mathbf{H}$ se obvyklým způsobem definuje $\mathbf{H}$-*ohodnocení* v výrokových atomů a jeho rozšíření přiřazující každé formuli A její hodnotu $v(A)$. Formule A je $\mathbf{H}$-*tautologie*, když $v(A) = 1_{\mathbf{H}}$ pro každé $\mathbf{H}$-ohodnocení v. Naše (Gödelova) otázka je, zda existuje konečná sémantika $\mathbf{H}$ ekvivalentní se sémantikou

intuicionistické logiky, tj. taková konečná sémantika **H**, že množina všech **H**-tautologií je rovna množině INT-TAUT všech intuicionistických tautologií. Odpověď dává věta 5.2.21, kterou dokázal K. Gödel.

Definice 5.2.18 *Mějme výrokové atomy $p_0, p_1, \ldots, p_n$. Symbolem DP_n (kde „DP“ značí Dirichletův princip) označíme formuli, která je disjunkcí všech formulí $p_i \equiv p_j$ pro $0 \leq i < j \leq n$, tj. formuli $\bigvee_{0 \leq i < j \leq n} (p_i \equiv p_j)$.*

Lemma 5.2.19 *Nechť **H** je n-hodnotová sémantika taková, že každá intuicionistická tautologie je **H**-tautologií. Pak DP_k je **H**-tautologie pro každé $k \geq n$.*

Důkaz Protože **H** má n pravdivostních hodnot, je každé **H**-ohodnocení $(k+1)$ výrokových atomů $p_0, \ldots, p_n$ neprosté, tj. pro jisté $i_0 < j_0$ je $v(p_{i_0}) = v(p_{j_0})$. Pro toto v má tedy formule DP_k stejnou hodnotu jako formule, která z ní vznikne tak, že atom p_{j_0} nahradíme atomem p_{i_0}. Tímto nahrazením ale vznikne intuicionistická tautologie (neboť každá disjunkce, která obsahuje formuli $p_{i_0} \equiv p_{i_0}$ jako jeden člen, jistě je intuicionistickou tautologií). Protože pro všechny intuicionistické tautologie A platí $v(A) = 1_{\mathbf{H}}$, máme $v(\mathrm{DP}_k) = 1_{\mathbf{H}}$. QED

Lemma 5.2.20 *Žádná z formulí DP_k pro $k \geq 1$ není intuicionistickou tautologií.*

Důkaz Vezměme $n \geq k$; pak můžeme ohodnotit atomy $p_0, p_1, \ldots, p_k$ vesměs různými hodnotami $0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{k}{n}$. Pro toto ohodnocení v a pro $i < j$ v $\mathbf{L}_{n+1}$ (tj. v $(n+1)$-prvkové G-algebře) platí $v(p_i \equiv p_j) = \frac{i}{n}$, tedy $v(\mathrm{DP}_k) = \frac{k-1}{n} < 1$. Tedy formule DP_k není $\mathbf{L}_{n+1}$-tautologie a tudíž není dokazatelná v G; tím spíše není intuicionistickou tautologií. QED

Věta 5.2.21 *Neexistuje žádná konečná sémantika **H** taková, že množina všech **H**-tautologií je rovna množině všech intuicionistických tautologií.*

5.2.2 Gödelova predikátová fuzzy logika

Formule Gödelovy predikátové logiky jsou tytéž jako formule klasické (a intuicionistické) predikátové logiky. Nebudeme pro jednoduchost pracovat s funkčními symboly kromě konstant ani s predikátem rovnosti. *Atomické formule* mají tvar $P(t_1, \ldots, t_n)$, kde P je predikátový symbol četnosti n a t_i jsou proměnné nebo konstanty. Složené formule se budují pomocí logických spojek $\rightarrow$, $\&$, $\vee$ a $\neg$ a kvantifikátorů $\forall$ a $\exists$. Pojem struktury (viz 3.1.7) zobecníme tak, že budeme predikátové symboly realizovat fuzzy relacemi.

Definice 5.2.22 *Nechť D je neprázdná množina a nechť **H** je G-algebra. Pak n-ární **H**-fuzzy relace na množině D je libovolné zobrazení r přiřazující každé n-tici $[a_1, \ldots, a_n]$ prvků množiny D prvek $r(a_1, \ldots, a_n) \in H$ (stupeň příslušnosti n-tice k relaci). Je-li **H** standardní G-algebra $[\![0,1]\!]_{\mathrm{G}}$, mluvíme prostě o* fuzzy relaci. **H**-struktura **D** *pro jazyk L s nosnou množinou D je dána funkcí r přiřazující*

každému predikátovému symbolu P četnosti n nějakou n-ární $\mathbf{H}$*-fuzzy relaci* $P^{\mathbf{D}}$ *na* D *a každé konstantě* c *nějaký prvek* $c^{\mathbf{D}} \in \mathbf{H}$. Tarského definice *(viz 3.1.9) se přirozeně zobecní následovně.*

(a) Hodnota $t^{\mathbf{D}} = [e]$ *termu* t *při ohodnocení proměnných* e *ve struktuře* $\mathbf{D}$ *je určena rovnostmi*

T1: $x^{\mathbf{D}}[e] = e(x)$, *je-li* x *proměnná,*

T2: $c^{\mathbf{D}}[e] = c^{\mathbf{D}}$, *je-li* x *konstanta.*

(b) Pravdivostní hodnota $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}$ *formule* φ *v* $\mathbf{H}$*-struktuře* $\mathbf{D}$ *při ohodnocení* e *je určena takto:*

T3: $\|P(t_1, .., t_n)\|^{\mathbf{H}}_{\mathbf{D}}[e] = P^{\mathbf{D}}(t_1^{\mathbf{D}}[e], .., t_n^{\mathbf{D}}[e])$,

tj. stupeň pravdivosti atomické formule $P(t_1, .., t_n)$ *je stupeň, v němž* n*-tice hodnot termů* $t_1, .., t_n$ *je v relaci* $r(P)$*,*

T4: $\|\varphi \to \psi\|^{\mathbf{H}}_{\mathbf{D}}[e] = \|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e] \Rightarrow \|\psi\|^{\mathbf{H}}_{\mathbf{D}}[e]$,

T5: $\|\neg\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e] = -\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e]$,

T6: $\|\varphi \,\&\, \psi\|^{\mathbf{H}}_{\mathbf{D}}[e] = \min(\, \|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e],\, \|\psi\|^{\mathbf{H}}_{\mathbf{D}}[e]\,)$,

T7: $\|\varphi \vee \psi\|^{\mathbf{H}}_{\mathbf{D}}[e] = \max(\, \|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e],\, \|\psi\|^{\mathbf{H}}_{\mathbf{D}}[e]\,)$,

T8: $\|\exists x\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e] = \sup_{a\in D}\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e(x/a)]$,

T9: $\|\forall x\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e] = \inf_{a\in D}\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e(x/a)]$,

kde $\Rightarrow$, $-$, min *a* max *jsou operace algebry* $\mathbf{H}$ *a hodnoty na levé straně rovnosti v podmínkách T8 a T9 se považují za nedefinované, pokud supremum resp. infimum neexistuje.*

Příklad 5.2.23 Nechť V je unární predikát „vysoký“, S binární predikát „sympatický“. Nechť $D = \{1, 2, 3, 4\}$, nechť $r(V)$ a $r(S)$ jsou dány těmito tabulkami:

1	2	3	4
0.2	0.4	0.9	1

	1	2	3	4
1	1	0.7	0.3	0
2	0.4	0.9	0.4	0.4
3	0.3	0.6	1	0.8
4	0.5	0.5	1	1

Platí-li například $e(x) = 3$ a $e(y) = 4$, pak $\|S(x, y)\|_{\mathbf{D}}[e] = 0.8$, $\|S(y, x)\|_{\mathbf{D}}[e] = 1$ a $\|V(x) \,\&\, V(y)\|_{\mathbf{D}}[e] = 0.9$. Označíme-li φ formuli $V(x) \,\&\, V(y) \to S(x, y)$, platí dále $\|\forall y\varphi\|_{\mathbf{D}}[e] = \inf_{a\in D}\|\varphi\|_{\mathbf{D}}[e(y/a)] = \inf\{\min(0.9, 0.2) \Rightarrow 0.3, \min(0.9, 0.4) \Rightarrow 0.6, \min(0.9, 0.9) \Rightarrow 1, \min(0.9, 1) \Rightarrow 0.8\} = \inf\{1, 1, 1, 0.8\} = 0.8$. Číslo 0.8 je pravdivostní hodnota tvrzení, které lze číst objekt 3 je sympatický každému objektu y, který je také vysoký.

Pokud je struktura $\mathbf{D}$ konečná nebo G-algebra $\mathbf{H}$ je *úplně uspořádaná* (tj. každá množina $X \subseteq H$ má infimum a supremum, což splňuje například algebra $[\![0, 1]\!]_{\mathrm{G}}$), pak pravdivostní hodnota $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e]$ je definována pro každou dvojici φ a e.

Definice 5.2.24 *(a)* **H**-*struktura* **D** *pro jazyk* L *je* bezpečná, *jestliže* $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e]$ *je definováno pro každou dvojici* φ *a* e. *(Tedy každá* $[\![0,1]\!]_{\mathrm{G}}$*-struktura je bezpečná; ale existují i bezpečné* **H**-*struktury pro G-algebry* **H**, *které nejsou úplně uspořádány.)*

(b) Pravdivostní hodnota $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}$ formule φ *v* **H**-*struktuře* **D** *je definována jako*

$$\|\varphi\|^{\mathbf{H}}_{\mathbf{D}} = \inf_{e} \|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e],$$

pokud toto infimum existuje.

(c) Formule φ platí (je pravdivá) *v* **H**-*struktuře* **D**, *jestliže* $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}} = 1_{\mathbf{H}}$ *(kde* $1_{\mathbf{H}}$ *je největší prvek G-algebry* **H**). *Formule* φ *je* logicky **H**-platná, *je-li pravdivá v každé bezpečné* **H**-*struktuře. Konečně řekneme, že* φ *je* logicky platná, *je-li logicky* **H**-*platná pro každou G-algebru* **H**.

Dále budeme uvažovat o tom, jak lze hilbertovský kalkulus pro výrokovou logiku G rozšířit na kalkulus pro predikátovou logiku G∀.

Definice 5.2.25 Axiomy kalkulu G∀ (logiky G∀) *jsou*

- *axiomy Gödelova výrokového kalkulu G, tj. axiomy intuicionistického výrokového kalkulu HJ s přidaným axiomem prelinearity* $(\varphi \to \psi) \vee (\psi \to \varphi)$,
- *axiomy B1 a B2 klasického (i intuicionistického) predikátového kalkulu (viz oddíl 3.2),*
- *pro každé* φ *a* ψ *takové, že* x *není volně ve* ψ, *následující axiom BG:*

  BG: $\quad \forall x(\varphi \vee \psi) \to (\forall x\varphi \vee \psi)$.

Odvozovací pravidla *kalkulu G∀ jsou pravidla generalizace Gen-A a Gen-E (viz opět oddíl 3.2).*

Pro ověření korektnosti axiomů si nejprve uvědomme, že v Gödelově predikátové logice platí následující varianta lemmatu 3.1.14:

Lemma 5.2.26 *(a) Pro každé ohodnocení* e, *termy* s *a* t *a proměnnou* x *platí* $(s_x(t))^{\mathbf{D}}[e] = s^{\mathbf{D}}[e(x/t^{\mathbf{D}}[e])]$ *(připomeňme, že termy v kalkulu G∀ jsou jen proměnné a konstanty).*
(b) Je-li φ *formule (daného jazyka) a* t *term substituovatelný za* x *ve* φ, *pak*

$$\|\varphi_x(t)\|^{\mathbf{H}}_{\mathbf{D}}[e] = \|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e(x/t^{\mathbf{D}}[e])].$$

Důkaz je zcela analogický důkazu lemmatu 3.1.14; zejména máme pro formuli φ tvaru $\exists y\psi$ a proměnnou y různou od x (vynecháváme indexy **H** a **D**):

$$\begin{aligned}
\|\varphi_x(t)\|[e] = \|\exists y\psi_x(t)\|[e] &= \sup_{a\in D} \|\psi_x(t)\|[e(y/a)] \\
&= \sup_{a\in D} \|\psi\|[(e(y/a))(x/t^{\mathbf{D}}[e(y/a)])] \\
&= \sup_{a\in D} \|\psi\|[(e(x/t^{\mathbf{D}}[e]))(y/a)] \\
&= \|\exists y\psi\|[e(x/t^{\mathbf{D}}[e])].
\end{aligned}$$

QED

Lemma 5.2.27 (korektnost kalkulu G∀) *(a) Všechny axiomy kalkulu G∀ jsou logicky platné, tj. jsou logicky* **H***-platné pro každou G-algebru* **H**.
(b) Odvozovací pravidla zachovávají r-pravdivost: pro každé $r \in \mathbf{H}$ *a každou bezpečnou* **H***-strukturu* **D** *platí: jsou-li předpoklady odvozovacího pravidla r-pravdivé v* **D**, *je i závěr pravidla r-pravdivý v* **D**.

Důkaz Postupujeme analogicky jako v důkazu věty 3.2.3 a lemmatu 3.1.20. Z důkazu korektnosti logiky G je jasné, že pro každé ohodnocení e a pro každý výrokový axiom φ logiky G∀ platí $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e] = 1$.

Korektnost axiomů B1 a B2 plyne z předchozího lemmatu; za předpokladu substituovatelnosti máme

$$\|\forall x\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e] = \inf_a \|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e(x/a)] \leq \|\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e(x/t^{\mathbf{D}}[e])] = \|\varphi_x(t)\|^{\mathbf{H}}_{\mathbf{D}}[e],$$

tedy $\|\forall x\varphi \to \varphi_x(t)\|^{\mathbf{H}}_{\mathbf{D}} = 1_{\mathbf{H}}$. Úvaha pro axiom B2 je analogická.

Nyní k odvozovacím pravidlům. Nechť proměnná x nemá volné výskyty ve formuli ψ; ukážeme $\|\psi{\to}\varphi\|^{\mathbf{H}}_{\mathbf{D}} \leq \|\psi{\to}\forall x\varphi\|^{\mathbf{H}}_{\mathbf{D}}$. Protože $\|\psi{\to}\varphi\|^{\mathbf{H}}_{\mathbf{D}} = \inf_e \|\psi{\to}\varphi\|^{\mathbf{H}}_{\mathbf{D}}[e] = \|\forall x(\psi \to \varphi)\|^{\mathbf{H}}_{\mathbf{D}}$, stačí ukázat, že formule $\forall x(\psi \to \varphi) \to (\psi \to \forall x\varphi)$ je logicky platná. Nechť tedy e je libovolné ohodnocení. Pro $a \in D$ označme $v_a = \|\varphi\|[e(x/a)]$. Dále označme $u = \|\psi\|[e]$. Protože x nemá volné výskyty ve ψ, pro každé $a \in D$ platí $u = \|\psi\|[e](x/a)$. Máme dokázat

$$\inf_a(u \Rightarrow v_a) \leq (u \Rightarrow \inf_a v_a).$$

Ukážeme dokonce rovnost. Na jedné straně $\inf_a v_a \leq v_a$ pro každé a, tedy $u{\Rightarrow}\inf_a v_a$ je dolní závorou všech prvků $u{\Rightarrow}v_a$. Na druhé straně, je-li z nějaká jiná dolní závora, tj. $z \leq u{\Rightarrow}v_a$ pro všechna a, pak dle lemmatu 5.2.2 je $\min(z,u) \leq v_a$ pro všechna a, tj. $\min(z,u) \leq \inf_a v_a$, tedy $z \leq (u \Rightarrow \inf_a v_a)$. Tedy $u \Rightarrow \inf_a v_a$ je infimum všech hodnot $u{\Rightarrow}v_a$. To je korektnost pravidla Gen-A. Důkaz korektnosti pravidla Gen-E je analogický a ponecháváme jej čtenáři jako cvičení.

Zbývá ověřit logickou platnost axiomu BG. K tomu stačí (při označení jako výše) dokázat

$$\inf_a \max(u, v_a) \leq \max(u, \inf_a v_a).$$

Opět dokážeme rovnost. Platí $\max(u, \inf_a v_a) \leq \max(u, v_a)$ pro každé $a \in D$, tedy $\max(u, \inf_a v_a) \leq \inf_a \max(u, v_a)$. Nechť pro nějaké z platí $z \leq \max(u, v_a)$ pro všechna a; dokážeme $z \leq \max(u, \inf_a v_a)$. Máme dvě možnosti: *buďto* $u \leq \inf_a v_a$, tedy $\max(u, v_a) = v_a$ pro všechna a, takže $z \leq \inf_a v_a \leq \max(u, \inf_a v_a)$; *nebo* $\inf_a v_a < u$, tedy pro jisté a je $v_a < u$, pro toto a platí $\max(u, v_a) = u$, takže $z \leq u \leq \max(u, \inf_a v_a)$. Tedy $\max(u, \inf_a v_a)$ je infimum všech hodnot $\max(u, v_a)$. QED

Definice 5.2.28 Teorie (nad logikou G∀) *je libovolná množina* T *sentencí — axiomů teorie* T. *Důkaz v teorii* T *je posloupnost formulí* $\varphi_1, \ldots, \varphi_n$, *jejíž každý člen je buď axiom logiky G∀, nebo axiom teorie* T, *nebo je odvozen z některých předchozích formulí pomocí některého odvozovacího pravidla.*

Lemma 5.2.29 *Pro kalkulus G∀ platí věta o dedukci ve stejném znění jako pro klasický predikátový kalkulus HK (viz lemma 3.2.2).*

Důkaz je stejný jako důkaz lemmatu 3.2.2.

Definice 5.2.30 *Nechť* $\mathbf{H}$ *je G-algebra.* $\mathbf{H}$-modelem *teorie* T *rozumíme libovolnou bezpečnou* $\mathbf{H}$*-strukturu* $\mathbf{D}$ *pro jazyk teorie* T*, v níž jsou všechny axiomy teorie* T *pravdivé, tj. platí* $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}} = 1_{\mathbf{H}}$ *pro každý axiom* $\varphi \in T$*.* Modelem *teorie* T *rozumíme* $[\![0,1]\!]_{\mathrm{G}}$*-model, tj. libovolnou* $[\![0,1]\!]_{\mathrm{G}}$*-strukturu, v níž jsou všechny axiomy teorie* T *pravdivé. Pro* $r \in (\!(0,1]\!]$ *rozumíme* r-modelem *teorie* T *libovolnou* $[\![0,1]\!]_{\mathrm{G}}$*-strukturu, v níž mají všechny axiomy teorie* T *hodnotu alespoň* r*.*

Lemma 5.2.27 o korektnosti axiomů a odvozovacích pravidel má následující důsledek pro dokazatelnost v teoriích:

Důsledek 5.2.31 (silná korektnost) *Nechť* T *je teorie v logice G∀ a nechť* $\mathbf{D}$ *je* $\mathbf{H}$*-model teorie* T*. Pak každá formule dokazatelná v* T *je* $\mathbf{H}$*-pravdivá v* $\mathbf{D}$*. (Speciálně každá formule dokazatelná v logice G∀ je logicky pravdivá.)*

Zdůvodněme, že formule z lemmatu 3.2.1 nejsou dokazatelné v G∀, a to tak, že najdeme strukturu $\mathbf{D}$ (nad $[\![0,1]\!]_{\mathrm{G}}$), v níž tyto formule nejsou 1-pravdivé. Buď $D = \mathrm{N}$ (přirozená čísla); buď $0 < v < 1$ a buď u_n klesající posloupnost čísel z $[\![0,1]\!]$ taková, že $\inf_n u_n = v$. Buď $r(P)(n) = u_n$; vyšetřeme strukturu $\mathbf{D} = (D, r)$ a formuli $\exists z(P(z) \to \forall x P(x))$. Zřejmě její hodnota ve struktuře $\mathbf{D}$ je $\sup_n(u_n \Rightarrow v) = \sup_n v = v < 1$. Podobně lze postupovat v případě formule $\exists z(\exists x P(x) \to P(z))$ (zde předpokládáme, že u_n rostou a $\sup_n u_n = v$).

Nyní přistoupíme k důkazu (silné) úplnosti logiky G∀. Z předchozího plyne, že nelze mechanicky převzít důkaz, který jsme užili pro klasický predikátový kalkulus HK.

Převezmeme z výrokového kalkulu G definice úplné a bezesporné teorie takto: teorie T je *bezesporná*, jestliže neexistuje formule φ taková, že $T \vdash \varphi$ a zároveň $T \vdash \neg\varphi$. Teorie T je *úplná*, jestliže je bezesporná a pro každou dvojici *uzavřených* formulí φ a ψ platí $T \vdash \varphi \to \psi$ nebo $T \vdash \psi \to \varphi$. Vztah následujícího pojmu *henkinovská teorie* k analogickému pojmu užitému v oddílu 3.2 je vysvětlen ve cvičeních.

Definice 5.2.32 *Teorie* T *je* henkinovská*, jestliže pro každou uzavřenou formuli tvaru* $\forall x\varphi$ *nedokazatelnou v* T *existuje v jazyce teorie* T *konstanta* c *taková, že sentence* $\varphi_x(c)$ *není dokazatelná v* T*.*

Lemma 5.2.33 *Nechť* T *je teorie a* α *formule taková, že* $T \nvdash \alpha$*. Pak existuje bezesporné úplné henkinovské rozšíření* S *teorie* T *takové, že* $S \nvdash \alpha$*.*

Důkaz Rozšiřme nejprve jazyk teorie T o henkinovské konstanty $c_{\forall x\varphi}$ všech řádů (jako v oddílu 3.2, ale henkinovské konstanty pro sentence začínající existenčním kvantifikátorem nyní neuvažujeme). Máme nalézt teorii S s tímto rozšířeným jazykem, pro kterou platí $S \nvdash \alpha$ a která má navíc tyto vlastnosti:

- pro každý pár sentencí φ, ψ je alespoň jedna z formulí $\varphi \to \psi$ a $\psi \to \varphi$ dokazatelná (podmínka prvního druhu),
- pro každou sentenci $\forall x \rho$ platí $S \vdash \forall x \rho$, právě když $S \vdash \rho_x(c_{\forall x \rho})$ (podmínka druhého druhu).

Předpokládejme, že jazyk teorie T (a tedy i jazyk teorie S) je spočetný (konstrukci lze s užitím axiomu výběru zobecnit na libovolné jazyky). Máme tedy zaručit spočetně mnoho podmínek indexovaných dvojicemi sentencí $[\varphi, \psi]$ a sentencemi $\forall x \rho$. Seřadíme je do posloupnosti podmínek tak, že má-li podmínka pro $\forall x \rho$ číslo n, pak se henkinovská konstanta $c_{\forall x \rho}$ nevyskytuje ve formulích odpovídajících předchozím podmínkám (s čísly $0, \ldots, n-1$). Konstruujeme rekurzí posloupnost $\{ T_i \,;\, i \in \mathrm{N} \}$ teorií a posloupnost $\{ \alpha_i \,;\, i \in \mathrm{N} \}$ sentencí. Položme $T_0 = T$ a $\alpha_0 = \alpha$. Předpokládejme, že je již sestrojena teorie T_n a sentence α_n splňující $T_n \supseteq T_0$, $T_n \vdash \alpha \to \alpha_n$ a $T_n \nvdash \alpha_n$. Přitom T_n neobsahuje henkinovské konstanty dané podmínkami druhého druhu s číslem k takovým, že $k \geq n$. Sestrojme teorii T_{n+1} a sentenci α_{n+1} rozebráním následujících případů.

Případ 1, n-tá podmínka se týká dvojice $[\varphi, \psi]$. V tomto případě postupujeme jako v důkazu lemmatu 5.2.8, teorii T_{n+1} definujeme jako tu z teorií $T_n \cup \{\varphi \to \psi\}$ a $T_n \cup \{\psi \to \varphi\}$, ve které nelze dokázat sentenci α_n. Dále definujeme $\alpha_{n+1} = \alpha_n$.

Případ 2(a), n-tá podmínka se týká sentence $\forall x \rho$ a navíc $T_n \nvdash \alpha_n \vee \rho_x(c_{\forall x \rho})$. Pak zřejmě $T_n \nvdash \forall x \rho$. Definujeme T_{n+1} jako T_n a dále definujeme $\alpha_{n+1} = \alpha_n \vee \rho_x(c_{\forall x \rho})$. Platí $T_{n+1} \nvdash \alpha_{n+1}$ a ostatní požadavky (včetně podmínky druhého druhu pro sentenci $\forall x \rho$) jsou také splněny.

Případ 2(b), n-tá podmínka se týká sentence $\forall x \rho$ a navíc $T_n \vdash \alpha_n \vee \rho_x(c_{\forall x \rho})$. Vezměme důkaz sentence $\alpha_n \vee \rho_x(c_{\forall x \rho})$ a nahraďme v něm všechny výskyty konstanty c nějakou proměnnou y, která se v důkazu nevyskytla. Tím dostaneme důkaz formule $\alpha_n \vee \rho_x(y)$ v teorii T_n. Generalizace (ve tvaru Gen z cvičení 5 oddílu 3.2) dává $T_n \vdash \forall y(\alpha_n \vee \rho_x(y))$. Užití axiomu B1, faktu, že $(\rho_x(y))_y(x)$ je ρ, a opětovná generalizace dávají $T_n \vdash \forall x(\alpha_n \vee \rho)$. Díky axiomu BG máme $T_n \vdash \alpha_n \vee \forall x \rho$. Z toho plyne $T_n \cup \{\forall x \rho \to \alpha_n\} \vdash \alpha_n$. Tedy $T_n \cup \{\alpha_n \to \forall x \rho\} \nvdash \alpha_n$, neboť jinak by platilo $T_n \vdash \alpha_n$, což by byl spor s předpoklady o T_n a α_n. Definujme tedy teorii T_{n+1} jako $T_n \cup \{\alpha_n \to \forall x \rho\}$ a položme $\alpha_{n+1} = \alpha_n$. Platí $T_{n+1} \nvdash \alpha_{n+1}$ a ostatní požadavky na T_{n+1} a α_{n+1} jsou také splněny. Dále platí $T_{n+1} \vdash \forall x \rho$, tedy je splněna i podmínka druhého druhu pro sentenci $\forall x \rho$.

Nyní položme $S = \bigcup_{n \in \mathrm{N}} T_n$. Zřejmě S je úplná a $S \nvdash \alpha$ (neboť pro všechna n platí $S \nvdash \alpha_n$). Ověřme, že S je henkinovská. Nechť $S \nvdash \forall x \rho$ a nechť podmínka pro $\forall x \rho$ má číslo n. Pak při ošetření této podmínky musel nastat případ 2(a), jinak by platilo $T_{n+1} \vdash \forall x \rho$ a také $S \vdash \forall x \rho$. Tedy $\alpha_{n+1} = \alpha_n \vee \rho_x(c_{\forall x \rho})$, a protože $S \nvdash \alpha_{n+1}$, máme $S \nvdash \rho_x(c_{\forall x \rho})$. QED

Lemma 5.2.34 *Nechť φ, ψ a χ jsou formule, nechť x není volně v χ. Pak následující formule jsou dokazatelné v kalkulu G∀ (dokonce v predikátovém intuicionistickém kalkulu HJ):*

(a) $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$, *(c)* $\forall x(\varphi \to \chi) \equiv (\exists x\varphi \to \chi)$.
(b) $\forall x(\chi \to \varphi) \equiv (\chi \to \forall x\varphi)$,

Důkaz tohoto lemmatu je naznačen ve cvičeních.

Definice 5.2.35 *Nechť T je úplná bezesporná teorie. Pak G-algebra $\mathbf{H}_T$ teorie T je definována takto: pro libovolnou sentenci φ nechť $[\varphi]_T$ označuje množinu všech sentencí T-ekvivalentních s φ, nosná množina H_T algebry $\mathbf{H}_T$ je množina $\{\, [\varphi]_T \,;\, \varphi$ sentence $\}$, dále $[\varphi]_T \leq_T [\psi]_T$, jestliže $T \vdash \varphi \to \psi$, a konečně operace* min, max *a $\Rightarrow$ jsou dány uspořádáním $\leq_T$.*

Ověření korektnosti této definice je stejné jako ve výrokové logice; všimněme si jen, že pracujeme s třídami T-ekvivalentních *sentencí*. Protože algebra $\mathbf{H}_T$ je z teorie T definována stejně jako v lemmatu 5.2.10, i nyní platí tvrzení onoho lemmatu: logické spojky jsou „kongruentní“ vůči operacím algebry $\mathbf{H}_T$. Následující lemma tvrdí, že také kvantifikátory jsou kongruentní vůči supremům a infimům.

Lemma 5.2.36 *Je-li teorie T úplná, bezesporná a henkinovská, pak pro každou formuli φ s jedinou volnou proměnnou x platí*

$$[\forall x\varphi]_T = \inf\{\, [\varphi_x(c)]_T \,;\, c \text{ konstanta}\,\},$$
$$[\exists x\varphi]_T = \sup\{\, [\varphi_x(c)]_T \,;\, c \text{ konstanta}\,\}.$$

Důkaz Jelikož $\mathrm{G}\forall \vdash \varphi_x(c) \to \exists x\varphi$, je třída $[\exists x\varphi]$ (vynecháváme index T) horní závorou všech tříd tvaru $[\varphi_x(c)]$. Ukážeme, že je nejmenší horní závorou. Nechť γ je sentence taková, že $[\varphi_x(c)] \leq [\gamma]$ pro všechny konstanty c; tvrdíme $[\exists x\varphi] \leq [\gamma]$. Neplatí-li to, máme $T \nvdash \exists x\varphi \to \gamma$, lemma 5.2.34(c) dává $T \nvdash \forall x(\varphi \to \gamma)$, a protože T je henkinovská, pro příslušnou henkinovskou konstantu c platí $T \nvdash (\varphi \to \gamma)_x(c)$. To je spor s $T \vdash \varphi_x(c) \to \gamma$, neboť $(\varphi \to \gamma)_x(c)$ je táž formule jako $\varphi_x(c) \to \gamma$. Podobně se dokáže, že $[\forall x\varphi]$ je infimem všech hodnot tvaru $[\varphi_x(c)]$. QED

Věta 5.2.37 (o silné úplnosti kalkulu G$\forall$) *Nechť T je teorie nad logikou G$\forall$ (se spočetným jazykem), nechť φ je formule. Následující tvrzení jsou navzájem ekvivalentní:*

(i) $T \vdash \varphi$,

(ii) φ *je pravdivá v každém* **H***-modelu teorie T pro každou G-algebru* **H**,

(iii) φ *je pravdivá v každém $[\![0,1]\!]_{\mathrm{G}}$-modelu teorie T.*

Důkaz Připomeňme, že **H**-modelem teorie T rozumíme *bezpečnou* strukturu **D** pro jazyk teorie T takovou, že $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}} = 1_{\mathbf{H}}$ pro každý axiom $\varphi \in T$. Z (i) plyne (ii) (to je silná korektnost) a z (ii) evidentně plyne (iii). Zbývá dokázat, že z (iii) plyne (i).

Nechť tedy $T \nvdash \varphi$, máme najít model **D** teorie T takový, že $\|\varphi\|_{\mathbf{D}} < 1$. Naším cílem je nalézt model nad algebrou $[\![0,1]\!]_{\mathrm{G}}$; nejprve najdeme model nad jistou spočetnou

G-algebrou $\mathbf{H}$. Podle lemmatu 5.2.33 můžeme předpokládat, že teorie T je bezesporná, úplná a henkinovská. Nechť $\mathbf{H}_T$ je G-algebra teorie T; pišme $\mathbf{H}$ místo $\mathbf{H}_T$. Napodobíme důkaz lemmatu 3.2.9. Nechť D je množina všech konstant teorie T; když P je n-ární predikát, definujeme

$$P^{\mathbf{D}}(c_1, .., c_n) = [P(c_1, .., c_n)]_T,$$

tj. pravdivostní hodnota $\|P(c_1, .., c_n)\|_{\mathbf{D}}$ je třída určená formulí $P(c_1, .., c_n)$, což je prvek G-algebry $\mathbf{H}$. Dále položme $c^{\mathbf{D}} = c$ pro každou konstantu c. Podobně jako v lemmatu 3.2.9 nyní ukažme, že pro libovolnou sentenci ψ je

$$\|\psi\|^{\mathbf{H}}_{\mathbf{D}} = [\psi]_T$$

(detaily jsou ve cvičeních). Tedy naše struktura $\mathbf{D}$ je $\mathbf{H}$-model teorie T, protože pochopitelně pro každý axiom teorie T je $[\alpha]_T = 1_{\mathbf{H}}$. Přitom pro naši formuli φ nedokazatelnou v T je $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}} = [\varphi]_T \neq 1_{\mathbf{H}}$, tj. φ neplatí v $\mathbf{D}$.

Zbývá ukázat, jak z $\mathbf{D}$ sestrojit $[\![0,1]\!]_{\mathrm{G}}$-model, tj. model nad standardní G-algebrou. K tomu opět stačí ukázat, že naše $\mathbf{H}$ lze izomorfně vnořit do intervalu $[\![0,1]\!]$ tak, že izomorfismus zachovává všechna suprema a infima existující v $\mathbf{H}$. Tento fakt, přesněji řečeno o trochu silnější fakt, formulujeme jako samostatné lemma. Pak dokončíme důkaz věty.

Lemma 5.2.38 *Pro každou spočetnou G-algebru $\mathbf{H}$ existuje prosté zobrazení f množiny H do racionálních čísel zachovávající uspořádání (tj. pro $u, v \in H$ je $u \leq_H v$, právě když $f(u) \leq f(v)$) a zachovávající suprema a infima existující v H (tj. je-li $X \subseteq H$ a $a = \sup_{\mathbf{H}} X$, pak $f(a) = \sup f(X)$, kde $f(X) = \{\, f(b) \,;\, b \in X \,\}$; podobně pro* inf*).*

Důkaz Připomeňme, že dle lemmatu 5.2.4 zobrazení jedné G-algebry do druhé přenášející (lineární) uspořádání přenáší též operace minima, maxima a rezidua $\Rightarrow$, a je tedy izomorfním vnořením první algebry do druhé. Ukážeme nejprve, že tvrzení lemmatu platí za dodatečného předpokladu, že uspořádání algebry $\mathbf{H}$ je husté (tj. pro každé $x < y$ existuje z tak, že $x <_{\mathbf{H}} z <_{\mathbf{H}} y$). Je známo, že každá spočetná hustě uspořádaná množina s největším a nejmenším prvkem je izomorfní s uspořádanou množinou racionálních čísel z $[\![0,1]\!]$, tj. s množinou $[\![0,1]\!] \cap \mathbb{Q}$ (viz cvičení). Nechť f je takové izomorfní vnoření algebry $\mathbf{H}$ do $[\![0,1]\!] \cap \mathbb{Q}$. Ukážeme, že f zachovává libovolná suprema i infima. Buď $X \subseteq H$ a $a = \inf_{\mathbf{H}} X$. Pak $f(a) \leq f(b)$ pro každé $b \in X$, tj. $f(a)$ je dolní závora množiny $f(X)$. Kdyby $z \in [\![0,1]\!]$ byla jiná dolní závora množiny $f(X)$ taková, že $f(a) < z$, pak by existovalo racionální číslo $u = f(c)$ takové, že $f(a) < u < z$; tedy c by byla dolní závora množiny X větší než a — to je spor. Tedy $f(a) = \inf f(X)$. Podobně se uvažuje v případě operace sup.

K dokončení důkazu lemmatu je třeba si uvědomit, že každou spočetnou lineárně uspořádanou množinu $\mathbf{H}_0$ lze vnořit do spočetné lineárně hustě uspořádané množiny $\mathbf{H}$ izomorfismem zachovávajícím suprema a infima existující v $\mathbf{H}_0$ (viz cvičení). QED

Dokončení důkazu věty o úplnosti Zbývá ukázat, že ke každému $\mathbf{H}$-modelu $\mathbf{D}$ teorie T takovému, že $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}} < 1$, existuje $[\![0,1]\!]_{\mathrm{G}}$-model $\mathbf{M}$ teorie T takový, že $\|\varphi\|_{\mathbf{M}} < 1$. Struktura $\mathbf{H}$ je spočetná G-algebra. Buď f její izomorfní vnoření do $[\![0,1]\!]_{\mathrm{G}}$ (s racionálními hodnotami) zachovávající suprema a infima existující v $\mathbf{H}$ a buď $P^{\mathbf{M}}(c_1,..,c_n) = f(P^{\mathbf{D}}(c_1,..,c_n))$, jinak jsou struktury $\mathbf{D}$ a $\mathbf{M}$ stejné. $\mathbf{M}$ je $[\![0,1]\!]_{\mathrm{G}}$-struktura a pro každou sentenci ψ platí $\|\psi\|^{\mathbf{H}}_{\mathbf{D}} = \|\psi\|_{\mathbf{M}}$, jakmile je levá strana definována. Tedy $\mathbf{M}$ je $[\![0,1]\!]_{\mathrm{G}}$-model teorie T a $\|\varphi\|_{\mathbf{M}} < 1$. QED

	$x * y$	$x \Rightarrow y$	$-x$
Łukasiewiczova t-norma	$\max(0, x+y-1)$	$1-x+y$	$1-x$
Gödelova t-norma	$\min(x,y)$	$\begin{cases} y & \text{pro } x>y \\ 1 & \text{jinak} \end{cases}$	$\begin{cases} 0 & \text{pro } x>0 \\ 1 & \text{jinak} \end{cases}$
produktová t-norma	$x \cdot y$	$\begin{cases} y/x & \text{pro } x>y \\ 1 & \text{jinak} \end{cases}$	$\begin{cases} 0 & \text{pro } x>0 \\ 1 & \text{jinak} \end{cases}$

Obrázek 5.2.1: Spojité t-normy

V úvodu k tomuto oddílu jsme se zmínili o tom, že Gödelova logika je jednou z významných fuzzy logik, nikoliv však jedinou. Obecný přístup, zpracovaný v monografii [34] (který také není jediný možný), vychází z pojmu spojité t-normy jako pravdivostní funkce konjunkce a jejího rezidua jako pravdivostní funkce implikace. Binární operace $*$ na intervalu $[\![0,1]\!]$ je *t-norma*, jestliže je komutativní, asociativní, neklesající v obou argumentech a platí $1 * x = 1$ pro každé x. Je-li t-norma spojitá, pak má operaci rezidua $\Rightarrow$ definovanou takto: $x \Rightarrow y = \max\{\, z \,;\, x * z \le y \,\}$. Pravdivostní funkcí negace je operace $-$ definovaná předpisem $-x = x \Rightarrow 0$. Pro každou spojitou t-normu platí $x \Rightarrow y = 1$ pro $x \le y$, a tedy $-0 = 1$. Tři nejdůležitější spojité t-normy jsou uvedeny ve druhém sloupci tabulky na obrázku 5.2.1. Ve třetím a čtvrtém sloupci tabulky jsou operace rezidua a negace příslušející k dané normě. Gödelova fuzzy logika (G a G$\forall$), se kterou jsme se v tomto oddílu dost podrobně seznámili, je tedy logikou Gödelovy t-normy. Je vybudována výroková i predikátová logika Ł a Ł$\forall$ Łukasiewiczovy t-normy i výroková a predikátová logika Π a $\Pi\forall$ produktové t-normy. Studuje se také logika *všech* spojitých t-norem (*basic logic* BL resp. BL$\forall$). Přehled predikátových fuzzy logik a jejich algebraických protějšků může čtenář najít v knize [57]; pro plný výklad odkazujeme k monografii [34]. Za zmínku stojí rovněž rozšíření Łukasiewiczovy logiky o pravdivostní konstanty: pro každé $r \in [\![0,1]\!]$ (případně $r \in [\![0,1]\!] \cap \mathbb{Q}$) je k dispozici formule $\bar{r}$ mající hodnotu r pro každé ohodnocení. Tuto logiku zavedl (bez vztahu k Łukasiewiczově logice) Jan Pavelka v disertační práci z r. 1979 a je známa jako Pavelkova logika. Navázal na něho Vilém Novák, který tuto logiku intenzívně studuje a rozvíjí (viz [60]).

Cvičení

1. Rozhodněte, které z následujících formulí (schémat) jsou $[\![0,1]\!]_{\mathrm{G}}$-tautologie:
   $(A \,\&\, B \to C) \to ((A \to C) \vee (B \to C))$, $\quad \neg A \vee \neg\neg A$,
   $(\neg\neg A \to A) \to A \vee \neg A$, $\quad \neg\neg A \to A$,
   $\neg(A \,\&\, B) \to \neg A \vee \neg B$, $\quad (A \to B) \to \neg A \vee B$,
   $\neg(\neg A \,\&\, \neg B) \to A \vee B$, $\quad (A \to \neg B) \to \neg A \vee B$.

2. Ověřte silnou korektnost kalkulu G: buď T teorie nad G a buď $\varphi_1, \dots, \varphi_n$ důkaz v T (nad G). Nechť $\mathbf{L}$ je G-algebra a nechť v je $\mathbf{L}$-ohodnocení, které je $\mathbf{L}$-modelem teorie T. Ukažte indukcí, že $v_{\mathbf{L}}(\varphi_i) = 1_{\mathbf{L}}$ pro každé $i = 1, \dots, n$.

3. Prověřte důkaz věty o dedukci pro kalkulus G.

4. Pro každou z formulí z cvičení 1, která je $[\![0,1]\!]_{\mathrm{G}}$-tautologií, zdůvodněte bez užití věty o úplnosti, že je dokazatelná v G.

5. Dokažte, že každé spočetné lineární uspořádání s největším a nejmenším prvkem lze izomorfně vnořit do uspořádané množiny $[\![0,1]\!] \cap \mathrm{Q}$ racionálních čísel z intervalu $[\![0,1]\!]$.

   Návod: Nechť $\mathbf{H} = \langle H, \leq_{\mathbf{H}} \rangle$ je uvažované uspořádání a $H = \{h_0, h_1, h_2, \dots\}$ je nějaké očíslování množiny H. Předpokládejte, že h_0 je nejmenší a h_1 největší prvek v $\mathbf{H}$. Dále postupujte metodou „cik-cak“ podobně jako v příkladu 3.4.12.

6. Vypracujte detaily důkazu tvrzení, že množina G-Taut je v *coNP*.

7. Ukažte, že formule $((p \to q) \to q) \to ((q \to p) \to p)$ není dokazatelná v kalkulu G, je ale dokazatelná v kalkulu HK.

8. Ukažte, že axiom BG není dokazatelný predikátovém kalkulu HJ, je ale dokazatelný v kalkulu HK.

9. Vypracujte detaily důkazu korektnosti pravidla Gen-E v kalkulu G$\forall$.

10. Ukažte, že pro klasickou logiku splývá definice úplné teorie podané zde (pro každé dvě sentence φ a ψ je $T \vdash \varphi \to \psi$ nebo $T \vdash \psi \to \varphi$) s definicí obvyklou pro klasickou logiku (pro každou sentenci φ je $T \vdash \varphi$ nebo $T \vdash \neg\varphi$).

11. Totéž platí pro pojem henkinovské teorie (henkinovského rozšíření dané teorie).

12. Postupně ukažte, že každá z následujících formulí je dokazatelná v kalkulu G$\forall$. (Které formule je třeba doplnit, aby vzniklá posloupnost byla důkazem?)
    $\forall x(\varphi \to \psi) \to (\varphi \to \psi)$, $\quad \forall x(\varphi \to \psi) \to (\forall x\varphi \to \psi)$,
    $\forall x\varphi \to \varphi$, $\quad \forall x(\varphi \to \psi) \,\&\, \forall x\varphi \to \psi$,
    $(\forall x\varphi \to \varphi) \to ((\varphi \to \psi) \to (\forall x\varphi \to \psi))$, $\quad \forall x(\varphi \to \psi) \,\&\, \forall x\varphi \to \forall x\psi$,
    $(\varphi \to \psi) \to (\forall x\varphi \to \psi)$, $\quad \forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$.

13. V důkazu úplnosti logiky G∀ vypracujte důkaz (indukcí), že $\|\varphi\|^{\mathbf{H}}_{\mathbf{D}} = [\varphi]_{\mathbf{T}}$ pro každou sentenci φ.

    Návod: indukční krok pro případ, kdy φ má tvar $\forall x\psi$, vypadá takto:
    $$\|\forall x\psi\|^{\mathbf{H}}_{\mathbf{D}} = \inf_v \|\psi\|^{\mathbf{H}}_{\mathbf{D}}[v] = \inf_c \|\psi_x(c)\|^{\mathbf{H}}_{\mathbf{D}} = \inf_c [\psi_x(c)]_T = [\forall x\psi]_T.$$

14. Dokažte, že každé spočetné lineární uspořádání **H** lze vnořit do hustého spočetného lineárního uspořádání vnořením zachovávajícím všechna suprema i infima existující v **H**. Návod: Pro $a \in H$ buď α^+ nejbližší větší prvek H, pokud takový existuje (horní soused), jinak buď $\alpha^+ = \alpha$. Pokud $\alpha^+ \neq \alpha$, přidejte mezi α a α^+ exemplář racionálních čísel větších než 0 a menších než 1 (pro různé α různé exempláře).

5.3 Logika dokazatelnosti

Hlavní myšlenku stojící v pozadí Gödelových vět o neúplnosti lze stručně vyjádřit takto: aritmetický jazyk umožňuje napsat sentenci, která říká o sobě já jsem nedokazatelná, a dokázat o ní, že opravdu je nedokazatelná. V roce 1952 položil L. Henkin otázku, která vypadá poněkud kuriózně: co kdybychom naopak napsali sentenci, která o sobě říká já jsem dokazatelná; byla by taková sentence dokazatelná? Henkinovu otázku vyřešil v roce 1955 (pozitivně) M. H. Löb v článku [55].

Fakt, že sentence φ tvrdí svou vlastní dokazatelnost například v Peanově aritmetice, se symbolicky zapíše

$$\mathsf{PA} \vdash \varphi \equiv \mathsf{Pr}_\pi(\overline{\varphi}), \qquad (*)$$

a my se ptáme, co můžeme říci o dokazatelnosti takto definované sentence. Není ale v použití slova „definované“ skryta nepřesnost? Věta o autoreferenci zaručuje existenci sentence φ, která splňuje podmínku $(*)$, ale netvrdí, že taková sentence je určena jednoznačně. Nejsme tedy možná oprávněni říci, že φ je *definována* vztahem $(*)$. O jedné sentenci, totiž o sentenci $0 = 0$, můžeme okamžitě říci, že splňuje podmínku $(*)$ a je dokazatelná. To ale samozřejmě není odpověď na Henkinovu otázku.

Tím jsme dospěli k přesnější formulaci Henkinovy otázky: platí o *každé* sentenci φ, která splňuje podmínku $(*)$, že je dokazatelná? Uvědomme si, že takovýmto zpřesněným způsobem je možno (a nutno) chápat i První Gödelovu větu: *každá* sentence, která tvrdí svou vlastní nedokazatelnost v PA, je v PA nedokazatelná.

Pozor, není to ale tak, že když nějaká sentence tvrdí něco o sobě, tak to také musí být pravda. Ponecháváme na čtenáři, aby si rozmyslel, že tvrdí-li sentence φ o sobě moje negace je dokazatelná, pak negace sentence φ určitě v PA dokazatelná není.

Věta 5.3.1 (Löbova) *Nechť T je teorie obsahující Peanovu aritmetiku a nechť $\tau(z)$ je Σ-formule, která definuje v $\mathbf{N}$ množinu T. Nechť φ je libovolná sentence, pro kterou platí $T \vdash \varphi \equiv \mathsf{Pr}_\tau(\overline{\varphi})$. Pak φ je dokazatelná v T.*

Důkaz Předpokládejme tedy, že sentence φ splňuje podmínku

1: $\quad T \vdash \varphi \equiv \mathsf{Pr}_\tau(\overline{\varphi})$.

Chceme dokázat dokazatelnost sentence φ v T. Domluvme se, že „T“ před znakem $\vdash$ psát nebudeme, všechny dokazatelnosti myslíme v teorii T. Vezměme pomocnou sentenci λ, o které platí

2: $\quad \vdash \lambda \equiv \mathsf{Pr}_\tau(\overline{\lambda}) \to \varphi$.

Taková sentence λ existuje díky větě o autoreferenci. Předpokládejme na chvíli, že λ je dokazatelná v T. Pak je v T dokazatelná jednak implikace $\mathsf{Pr}_\tau(\overline{\lambda}) \to \varphi$ (díky (2)), jednak její premisa $\mathsf{Pr}_\tau(\overline{\lambda})$ (díky podmínce D1). Tedy je dokazatelná i sentence φ. Tím jsme dokázali implikaci

3: $\quad$ Když $T \vdash \lambda$, pak $T \vdash \varphi$.

Vezměme nyní z ekvivalence (2) jen jednu implikaci a použijme na ni podmínku D1:

$$\vdash \mathsf{Pr}_\tau(\overline{\lambda \to (\mathsf{Pr}_\tau(\overline{\lambda}) \to \varphi)}).$$

Dvojí užití podmínky D2 dává

$$\vdash \mathsf{Pr}_\tau(\overline{\lambda}) \to \mathsf{Pr}_\tau(\overline{\mathsf{Pr}_\tau(\overline{\lambda}) \to \varphi}),$$

$$\vdash \mathsf{Pr}_\tau(\overline{\lambda}) \to (\mathsf{Pr}_\tau(\overline{\mathsf{Pr}_\tau(\overline{\lambda})}) \to \mathsf{Pr}_\tau(\overline{\varphi})).$$

Vezmeme-li nyní v úvahu implikaci $\mathsf{Pr}_\tau(\overline{\lambda}) \to \mathsf{Pr}_\tau(\overline{\mathsf{Pr}_\tau(\overline{\lambda})})$ (dokazatelnou díky podmínce D3), máme

4: $\quad \vdash \mathsf{Pr}_\tau(\overline{\lambda}) \to \mathsf{Pr}_\tau(\overline{\varphi})$.

Uvědomme si, že podmínka (4) je vlastně formalizací podmínky (3), a rovněž důkaz byl formalizací důkazu podmínky (3). A teď už rychle dostaneme dokazatelnost sentence φ:

5: $\quad \vdash \mathsf{Pr}_\tau(\overline{\lambda}) \to \varphi$; 4, 1

6: $\quad \vdash \lambda$; 5, 2

$\quad \vdash \varphi$; 3.

QED

Všimněme si, že z ekvivalence (2) se nakonec uplatnily obě implikace, ale z podmínky (1) jsme vystačili s jedinou implikací. To znamená, že postačující podmínkou pro dokazatelnost sentence φ je dokazatelnost implikace $\mathsf{Pr}_\tau(\overline{\varphi}) \to \varphi$.

Na důkazu Löbovy věty je pozoruhodné, že se v něm nevyskytují žádné proměnné ani kvantifikátory, přesněji řečeno všechny jsou skryty ve formuli Pr. Veškeré formule vyskytující se v důkazu jsou sestaveny jen z logických spojek, z formule Pr a ze sentencí (totiž λ a φ), jejichž vnitřní strukturu není nutno uvažovat. To je totéž, co lze říci i o důkazu Druhé Gödelovy věty. Navíc oba důkazy vystačily s podmínkami D1–D3. Jako by to byly důkazy v nějakém zvláštním logickém kalkulu *z axiomů* D1–D3.

Logické kalkuly, ve kterých se uvažují formule sestavené z dále nedělitelných formulí — atomů — pomocí logických spojek a jednoho dodatečného unárního operátoru, se studují a nazývají se *modální výrokové logiky*. Dodatečný operátor se nazývá *modalita* (nebo *modalita nutnosti*), zpravidla se značí $\Box$ a čte se „nutně“. Lze pochopitelně uvažovat i jiné nebo další modality. I v (nejobvyklejším) případě, kdy se uvažuje jen jediná modalita nutnosti, existuje více modálních logik, které se liší v tom, jaký význam se té modalitě dává. Liší se tedy sémantikou.

V tomto oddílu se zabýváme modální logikou, ve které se modalita nutnosti $\Box$ interpretuje formulí Pr, tj. nutnost se chápe jako formální dokazatelnost v nějaké axiomatické teorii. Tato modální logika se nazývá *logikou dokazatelnosti*. Logika dokazatelnosti nám umožní hlouběji pochopit metodu autoreference. Pokud tato logika bude úplná a rozhodnutelná, což bude, dá nám zároveň obecnou metodu pro řešení takových otázek, jako položil L. Henkin. Zdůrazněme, že naším cílem není logická analýza modalit v přirozené řeči. Zajímáme se o *aplikace* modální logiky v metamatematice.

Možnost modální analýzy sentencí definovaných autoreferencí se otevřela až formulováním podmínek D1–D3. Právě formulaci podmínek D1–D3 je asi nutno považovat za velký přínos Löbova článku [55]. Samotné tvrzení Löbovy věty lze získat i jednodušeji, viz cvičení. Před Löbem formuloval P. Bernays jiné podmínky — známé jako Hilbertovy-Bernaysovy podmínky pro dokazatelnost — které také umožňují dokázat Druhou Gödelovu větu, ale na rozdíl od Löbových podmínek na nich nelze založit modální logiku. O Hilbertových-Bernaysových podmínkách si lze přečíst ve Smoryńského knize [80]. Kniha [80] je celá věnována autoreferenci, náš text v tomto oddílu z ní do značné míry vychází a je jí pokryt s výjimkou pojednání o gentzenovském kalkulu pro logiku dokazatelnosti a o její algoritmické složitosti. Gentzenovský kalkulus pro logiku dokazatelnosti se studuje v článku [74]. Z novějších zdrojů doporučujeme také Boolosovu knihu [8]. Čtivý výklad o historii logiky dokazatelnosti je článek [7].

5.3.1 Modální formule, aritmetická sémantika

Modální (výrokové) formule jsou formule sestavené z konstanty $\bot$ a z výrokových atomů podle stejných pravidel jako v klasické výrokové logice s tím, že kromě negace se připouští ještě unární operátor $\Box$. Příklady modálních formulí jsou

$$\Box\neg\Box\bot, \quad (\Box p \to \Box\neg\bot) \quad \text{a} \quad \Box((p \vee q) \to (\Box p \vee \Box q)).$$

Domluvme se, že pro prioritu operací a pro vypouštění nadbytečných závorek platí obvyklá domluva s tím, že modalita $\Box$ má nejvyšší možnou prioritu (stejnou jako negace). Rovněž symbol $\bot$ má obvyklý význam: je to logická konstanta pro nepravdu (spor). Formuli $\Box A$ čteme „nutně A“, v našem kontextu případně též „je dokazatelné, že A“. Kromě $\bot$ a $\Box$ se často užívají duální symboly: $\top$ je zkratka pro $\neg\bot$ a $\Diamond A$ je zkratka pro $\neg\Box\neg A$. Formuli $\Diamond A$ čteme „možná A“; něco je možné, jestliže není nutný opak.

Logika dokazatelnosti (stejně jako klasická výroková logika) není příliš závislá na volbě seznamu logických spojek. Uvidíme ale, že logická konstanta $\bot$ je užitečná a neradi bychom ji postrádali.

Jak již bylo řečeno v úvodu, nutnost chceme chápat jako dokazatelnost. Teď se domluvme přesněji, že uvažujeme dokazatelnost v Peanově aritmetice vyjádřenou formulí Pr_π, kde π je přirozená definice axiomů Peanovy aritmetiky. S pomocí formule Pr_π tedy definujeme *aritmetickou sémantiku* modální logiky.

Definice 5.3.2 Aritmetický překlad *je libovolná funkce $*$ z množiny všech modálních formulí do množiny všech aritmetických sentencí, která splňuje podmínky:*

- $\bot^* = (0 = \mathrm{S}(0))$,
- *funkce $*$ komutuje se všemi logickými spojkami, tj.* $(A \to B)^* = A^* \to B^*$ *atd.*,
- $(\Box A)^* = \mathsf{Pr}_\pi(\overline{A^*})$.

Definice aritmetického překladu neříká nic o atomech, těm mohou být přiřazeny libovolné sentence. Existuje tedy více — nekonečně mnoho — aritmetických překladů. Jsou-li ale dány funkční hodnoty překladu na atomech, říkejme jim *ohodnocení atomů*, určuje definice překladu jednoznačně hodnoty na všech ostatních modálních formulích. Aritmetický překlad tedy hraje v aritmetické sémantice modální logiky stejnou úlohu jako pravdivostní ohodnocení v sémantice klasické výrokové logiky. A definice překladu hraje stejnou úlohu jako pravdivostní tabulky logických spojek: určuje, jak se ohodnocení formule spočítá z ohodnocení podformulí.

Je-li A modální formule a $*$ aritmetický překlad, dovolme si o hodnotě A^* funkce $*$ v bodě A mluvit jako o *překladu formule A*. Překlad jedné modální formule A je určen ohodnocením jen těch atomů, které se v A skutečně vyskytují. Neobsahuje-li formule A výrokové atomy, její překlad A^* je táž aritmetická sentence pro všechny překlady $*$.

Definice 5.3.3 *Řekneme, že modální formule A je* PA-platná*, jestliže* $\mathsf{PA} \vdash A^*$ *pro každý překlad $*$. Formule A je* **N**-platná*, jestliže* $\mathbf{N} \models A^*$ *pro každý překlad $*$. Množinu všech* PA*-platných resp.* **N***-platných formulí označme* PA-Taut *resp.* **N**-Taut.

Kromě „PA-platná“ a „**N**-platná“ by se také mohlo říkat PA*-tautologie* nebo **N***-tautologie*. Každá PA-tautologie je samozřejmě zároveň **N**-tautologií. Definice modální tautologie je podobná jako v klasické výrokové logice: A je tautologie, právě když pro každé ohodnocení atomů atd. Jeden rozdíl je v tom, že uvažujeme současně dvě definice modální tautologie. Druhý je v tom, že z definice není zřejmé, zda množina všech tautologií (v tom či onom smyslu) je obecně rekurzívní nebo alespoň rekurzívně spočetná. O některých formulích ale můžeme rovnou rozhodnout, zda vyhovují našim definicím.

Příklad 5.3.4 Je-li sentence $0 = \mathrm{S}(0)$ v PA dokazatelná, pak v PA je každá sentence dokazatelná. Uvnitř PA je tento fakt také znám: $\mathsf{PA} \vdash \mathsf{Pr}_\pi(\overline{0 = \mathrm{S}(0)}) \to \mathsf{Pr}_\pi(\overline{\varphi})$ pro

libovolnou sentenci φ. Tedy překlad modální formule $\Box\bot\to\Box p$ je vždy dokazatelný, takže formule $\Box\bot \to \Box p$ je PA-platná i $\mathbf{N}$-platná.

Příklad 5.3.5 Nechť A je modální formule $\Box p \to p$. Vezměme překlad $*$, který atom p ohodnocuje sentencí ν z První Gödelovy věty. Pak A^* je aritmetická sentence $\mathsf{Pr}_\pi(\overline{\nu}) \to \nu$. To je sentence, která není v PA dokazatelná: kdyby byla, pak by vzhledem k dokazatelnosti sentence $\neg\mathsf{Pr}_\pi(\overline{\nu}) \to \nu$ platilo $\mathsf{PA} \vdash \nu$, což není pravda. Našli jsme překlad $*$, pro který platí $\mathsf{PA} \nvdash A^*$. Tedy formule $\Box p \to p$ není PA-tautologií.

Příklad 5.3.6 Modální formule $\neg\Box\bot$ se bez ohledu na ohodnocení atomů přeloží na sentenci $\neg\mathsf{Pr}_\pi(\overline{0 = \mathrm{S}(0)})$, tj. na sentenci $\mathsf{Con}(\pi)$. O té víme, že ve struktuře $\mathbf{N}$ platí, ale v PA není dokazatelná. Formule $\neg\Box\bot$ je tedy $\mathbf{N}$-platná, ale není PA-platná.

Příklad 5.3.7 Formuli $A = \neg\Box\bot \to \neg\Box\neg\Box\bot$ lze číst „není-li dokazatelný spor, pak není dokazatelné, že není dokazatelný spor“. Tato formule vyjadřuje v modální logice Druhou Gödelovu větu. Jejím překladem je sentence $\mathsf{Con}(\pi)\to\neg\mathsf{Pr}_\pi(\overline{\mathsf{Con}(\pi)})$, o které z cvičení 4 oddílu 4.5 víme, že je v PA dokazatelná. Formule A je tedy PA-platná. Opačná implikace $\neg\Box\neg\Box\bot \to \neg\Box\bot$ je také PA-platná, což lze rychle zjistit dosazením formule $\neg\Box\bot$ za atom p do formule v příkladu 5.3.4.

Vidíme, že modální logika umožňuje formulovat *obecné fakty o dokazatelnosti v* PA, tj. fakty nezávislé na konkrétních tvrzeních. „Je-li dokazatelný spor, pak je dokazatelná každá formule“ je příklad obecného faktu. Tvrzení „Bezoutova věta je v PA dokazatelná“ nepovažujeme za obecný fakt.

Dvojí definice logické platnosti formule (PA-platná a $\mathbf{N}$-platná) nám umožňuje odlišit obecné fakty o dokazatelnosti, které jsou pravdivé, od obecných faktů o dokazatelnosti, o jejichž pravdivosti „ví“ Peanova aritmetika. Příklad 5.3.6 ukazuje, že to není totéž.

Mohli bychom si také klást obecnější otázku, totiž uvažovat dvě teorie T a S a ptát se, jaké obecné fakty o dokazatelnosti v teorii T ví teorie S. Aritmetická interpretace by tak byla zadána dvojicí $\langle S, \mathsf{Pr}_\tau\rangle$, kde formule Pr_τ definuje dokazatelnost v teorii T a určuje, jak se překládají modální formule, a S určuje, ve které teorii se ptáme na dokazatelnost jejich překladů. Takto obecnou situací se zabývat nebudeme, ale vypůjčíme si z ní terminologii. Místo „A je PA-platná“ nebo „$\mathbf{N}$-platná“ budeme také říkat, že *formule A platí v aritmetické interpretaci* $\langle\mathsf{PA}, \mathsf{Pr}_\pi\rangle$ resp. v interpretaci $\langle\mathbf{N}, \mathsf{Pr}_\pi\rangle$.

Čtenář by si ale neměl myslet, že modálních logik se vztahem k dokazatelnosti v axiomatických teoriích existuje velké množství, jiná pro každou aritmetickou interpretaci $\langle S, \mathsf{Pr}_\tau\rangle$. Je sice pravda, že například Zermelova-Fraenkelova teorie množin ví o Peanově aritmetice, že je bezesporná, což Peanova aritmetika o sobě neví. Uvažujeme-li ale, co se o dokazatelnosti v T dá dokázat uvnitř téže teorie T, v mnoha případech dostaneme tutéž modální logiku, totiž tu, kterou zde prezentujeme. Korektní a dostatečně silné teorie se neliší ve svých znalostech o *vlastní* dokazatelnosti.

5.3.2 Logické kalkuly

V tomto pododdílu se pokusíme axiomatizovat množinu všech PA-platných formulí a množinu všech **N**-platných formulí pomocí vhodných kalkulů. V následujících pododdílech dospějeme mimo jiné k důkazům úplnosti těchto kalkulů vůči aritmetické sémantice. Začněme definicí fregovského kalkulu pro jednu z modálních logik.

Definice 5.3.8 *Axiomy* modální logiky K4 *jsou*

L1: *všechny výrokové tautologie*,

a dále všechny modální formule tvaru

L2: $\Box(A \to B) \to (\Box A \to \Box B)$,

L3: $\Box A \to \Box\Box A$.

Logika K4 má odvozovací pravidla

MP: $A\,,\ A \to B \ /\ B$,

Nec: $A \ /\ \Box A$.

K4 je tradiční označení, viz např. [38]. Výrokovou tautologií myslíme modální formuli, která vznikne z nějaké klasické výrokové tautologie substitucí modálních formulí za její atomy. Vzpomeňme si, že podobně jsme v oddílu 3.2 (na str. 157) definovali predikátové formule, které jsou tautologiemi. Například $p \to (\Box q \to p)$ a $\bot \to p$ jsou modální formule, které jsou tautologiemi. Také $\neg A \to (A \to \bot)$ je výroková tautologie bez ohledu na volbu formule A.

Když $*$ je libovolný překlad a modální formule A je PA-platná, tj. platí $\mathsf{PA} \vdash A^*$, pak díky podmínce D1 platí i $\mathsf{PA} \vdash \mathsf{Pr}_\pi(\overline{A^*})$. To znamená, že množina všech PA-platných modálních formulí je uzavřena na pravidlo Nec. Je-li A modální formule, která je výrokovou tautologií, pak A^* je predikátová sentence, která je rovněž tautologií (v před chvílí zmíněném „predikátovém“ smyslu), a je tedy dokazatelná v PA. Také překlady axiomů L2 a L3 jsou v PA dokazatelné, to plyne bezprostředně z podmínek D2 a D3. Z toho je jasné, že logika K4 je *korektní* vůči interpretaci $\langle \mathsf{PA}, \mathsf{Pr}_\pi \rangle$.

Kdykoliv je dokázána nějaká modální formule A, můžeme díky pravidlu Nec usoudit, že platí i $\Box A$. To ale neznamená, že implikace $A \to \Box A$ musí být PA-platná. Vezměme sentenci ν z První Gödelovy věty. Kdyby platilo $\mathsf{PA} \vdash \nu \to \mathsf{Pr}_\pi(\overline{\nu})$, pak by vzhledem k dokazatelnosti sentence $\nu \to \neg\mathsf{Pr}_\pi(\overline{\nu})$ platilo i $\mathsf{PA} \vdash \neg\nu$. To ale není pravda. Vidíme, že sentence ν je *aritmetickým protipříkladem* na modální formuli $p \to \Box p$. Tento příklad zároveň ukazuje, že *věta o dedukci* pro logiku K4 neplatí a neplatí pro žádnou modální logiku, která je korektní vůči interpretaci $\langle \mathsf{PA}, \mathsf{Pr}_\pi \rangle$ a má mezi odvozovacími pravidly pravidlo Nec.

Pravidlo Nec se anglicky nazývá *rule of necessitation*, česky snad *pravidlo přidání nutnosti*. Hraje v modální logice podobnou úlohu, jako pravidlo generalizace v predikátové logice, a někdy se mu i tak říká. Ukažme si několik příkladů důkazů v našem kalkulu.

1: $\vdash \bot \to p$; L1

2: $\vdash \Box(\bot \to p)$; Nec

3: $\vdash \Box(\bot \to p) \to (\Box\bot \to \Box p)$; L2

4: $\vdash \Box\bot \to \Box p$; MP.

V druhém důkazu si už dovolíme malé přeskakování.

1: $\vdash A \to (B \to A \,\&\, B)$; L1

2: $\vdash \Box(A \to (B \to A \,\&\, B))$; Nec

3: $\vdash \Box A \to \Box(B \to A \,\&\, B)$; 2, L2

4: $\vdash \Box(B \to A \,\&\, B) \to (\Box B \to \Box(A \,\&\, B))$; L2

5: $\vdash \Box A \,\&\, \Box B \to \Box(A \,\&\, B)$; 3, 4.

Nejen s pojmem tautologie, ale i s pojmem tautologický důsledek můžeme zacházet analogicky, jako když jsme v oddílu 3.2 konstruovali důkazy v kalkulu HK. Formule (5) je tautologickým důsledkem formulí (3) a (4). Jinak řečeno, formuli (5) lze snadno odvodit z formulí (3) a (4) bez užití axiomů L2 a L3 a pravidla Nec, neboť formule $(3) \to ((4) \to (5))$ je výrokovou tautologií čili instancí schématu L1.

K formuli (5) ještě poznamenejme, že opačnou implikaci $\Box(A\&B)\to\Box A\&\Box B$ lze v logice K4 dokázat také, naopak nelze dokázat analogickou formuli pro disjunkci. O tom jsou některá cvičení.

Podívejme se ještě na jeden důkaz v logice K4. Začněme s implikací

1: $\vdash \Box(p \equiv \neg\Box p) \to (\Box p \to \Box\neg\Box p)$; L2.

Protože zápis $p\equiv\neg\Box p$ je zkratkou pro konjunkci $(p\to\neg\Box p)\,\&\,(\neg\Box p\to p)$, v odvození formule (1) jsme kromě axiomu L2 použili také schéma $\Box(A\&B)\to\Box A$. V odvození řádku (8) níže využijeme i opačnou implikaci ekvivalence $p \equiv \neg\Box p$. Označme D předpoklad $\Box(p \equiv \neg\Box p)$ implikace (1).

2: $\vdash \neg\Box p \to (\Box p \to \bot)$; L1

3: $\vdash \Box\neg\Box p \to (\Box\Box p \to \Box\bot)$; 2, Nec, dvakrát L2

4: $\vdash D \to (\Box p \to (\Box\Box p \to \Box\bot))$; 1, 3

5: $\vdash \Box p \to \Box\Box p$; L3

6: $\vdash D \to (\neg\Box\bot \to \neg\Box p)$; 4, 5.

Dosud napsaný důkaz je vlastně modální simulací důkazu První Gödelovy věty a formule (6) vyjadřuje *část* První Gödelovy věty: *když nějaká sentence tvrdí svou vlastní nedokazatelnost, pak, pokud ovšem není dokazatelný spor, není dokazatelná.* K plnému znění První Gödelovy věty chybí tvrzení, že *existuje* sentence, která tvrdí svou vlastní nedokazatelnost. Pochopitelně lze simulovat i důkaz Druhé Gödelovy věty:

7: $\vdash \Box D \to (\Box\neg\Box\bot \to \Box\neg\Box p)$; 6, Nec, dvakrát L2

8: $\vdash D \to (\Box\neg\Box p \to \Box p)$; L2

9: $\vdash D \to \Box D$; L3

10: $\vdash D \to (\Box\neg\Box\bot \to \Box p)$; 9, 7, 8

11: $\vdash D \to (\neg\Box\bot \to \neg\Box\neg\Box\bot)$; 6, 10.

Tím jsme skoro dokázali formuli $\neg\Box\bot \to \neg\Box\neg\Box\bot$, která nás zajímá a o které z příkladů k aritmetické sémantice víme, že je PA-platná. Bohužel předpokladu D se zbavit nelze, formule $\neg\Box\bot \to \neg\Box\neg\Box\bot$ není v logice K4 dokazatelná. Z toho je jasné, že chceme-li mít modální logiku úplnou vzhledem k aritmetické interpretaci, musíme k axiomům nebo pravidlům logiky K4 přidat ještě něco.

Jednou z možností je přidat odvozovací pravidlo, které umožňuje odvodit formuli A, pokud je dokázána implikace $D \to A$, kde jako v řádku (11), D je autoreferenční předpoklad o nějakém atomu p, který se nevyskytuje v A. O takovém pravidlu, pravidlu autoreference, se zmíníme v části o kripkovské sémantice.

Další možnosti, jak rozšířit logiku K4, jsou přidat k ní buď *Löbův axiom L4*, nebo *Löbovo pravidlo LR*:

L4: $\Box(\Box A \to A) \to \Box A$,

LR: $\Box A \to A \;/\; A$.

Rozmyslíme si, že obě možnosti jsou ekvivalentní. Všimněme si ještě, že jak Löbův axiom, tak Löbovo pravidlo je modálním vyjádřením Löbovy věty: je-li implikace $\mathsf{Pr}_\pi(\overline{\varphi}) \to \varphi$ dokazatelná, pak je dokazatelná i sentence φ. Löbův axiom je vlastně formalizací Löbova pravidla ve stejném smyslu, jako je axiom L3 formalizací pravidla Nec.

Lemma 5.3.9 *Množina všech formulí dokazatelných v rozšíření logiky K4 o Löbův axiom L4 je uzavřena na Löbovo pravidlo LR. V rozšíření logiky K4 o Löbovo pravidlo lze dokázat všechny instance Löbova axiomu. Rozšíření logiky K4 o Löbův axiom nebo o Löbovo pravidlo jsou tedy spolu ekvivalentní.*

Důkaz Je-li již dokázána implikace $\Box A \to A$, lze použitím pravidla Nec získat předpoklad Löbova axiomu, a tedy i formuli $\Box A$. Tato formule a opětovné užití implikace $\Box A \to A$ dává A.

Naopak, předpokládejme, že máme dokázat formuli $\Box(\Box A \to A) \to \Box A$. Označme ji B. Stačí v logice K4 dokázat formuli $\Box B \to B$ a pak užít pravidlo LR:

1:	$\Box B \to (\Box\Box(\Box A \to A) \to \Box\Box A)$	; L2
2:	$\Box(\Box A \to A) \to \Box\Box(\Box A \to A)$	; L3
3:	$\Box B \to (\Box(\Box A \to A) \to \Box\Box A)$	; 1, 2
4:	$\Box(\Box A \to A) \to (\Box\Box A \to \Box A)$	; L2
5:	$\Box B \to (\Box(\Box A \to A) \to \Box A)$	; 3, 4
6:	B	; 5, LR.

QED

Nyní už můžeme oficiálně definovat logiku dokazatelnosti a dokázat její aritmetickou korektnost. Ještě si uvědomme, že vzhledem k tomu, že uvažujeme současně dvě různé aritmetické interpretace, potřebujeme dvě modální logiky.

Definice 5.3.10 Modální logika GL, logika dokazatelnosti, *vznikne přidáním Löbova axiomu L4 k logice K4. Modální logika* GL^ω *má jediné odvozovací pravidlo modus ponens a jejími axiomy jsou všechny formule dokazatelné v logice GL a dále všechny formule tvaru* $\Box A \to A$.

Věta 5.3.11 (o korektnosti vůči aritmetické sémantice) *(a) Každá modální formule dokazatelná v (kalkulu z definice 5.3.10 pro logiku) GL je* PA*-platná.*
(b) Každá modální formule dokazatelná v logice GL^ω *je* $\mathbf{N}$*-platná.*

Důkaz Platnost axiomů L1–L3 a korektnost pravidel MP a Nec vůči interpretaci $\langle \mathsf{PA}, \mathsf{Pr}_\pi \rangle$ jsme již konstatovali. K důkazu korektnosti logiky GL zbývá ověřit PA-platnost Löbova axiomu L4. Vzhledem k lemmatu 5.3.9 stačí zdůvodnit, že množina všech PA-platných modálních formulí je uzavřena na pravidlo LR. To je ale přesně to, co věta 5.3.1 tvrdí pro formuli $\tau := \pi$ (tj. pro přirozenou definici axiomů Peanovy aritmetiky).

Předpokládejme nyní, že $\mathbf{N} \models \mathsf{Pr}_\pi(\overline{A^*})$ pro nějaký překlad nějaké modální formule A. Pak platí $\mathsf{PA} \vdash A^*$ (viz podmínku Def na str. 349), a protože PA je korektní teorie, musí platit i $\mathbf{N} \models A^*$. Tedy $\mathbf{N} \models \mathsf{Pr}_\pi(\overline{A^*}) \to A^*$. Tím je dokázána $\mathbf{N}$-platnost schématu $\Box A \to A$ a dokončen důkaz věty o korektnosti obou modálních logik vůči aritmetickým interpretacím. QED

Postup přijmout jako axiomy logiky GL^ω (mimo jiné) všechny formule dokazatelné v logice GL je oprávněn faktem, že množina všech formulí dokazatelných v logice GL je algoritmicky rozhodnutelná. To dokážeme v následujícím pododdílu.

V logice GL, a tedy ovšem i v GL^ω, lze snadno dokázat formuli $\neg\Box\bot \to \neg\Box\neg\Box\bot$, stačí volit $A := \bot$ v axiomu L4. V logice GL^ω lze navíc dokázat formuli $\neg\Box\bot$, a tedy i formuli $\neg\Box\neg\Box\bot$; stačí volit $A := \bot$ ve schématu $\Box A \to A$. Víme ale, že formule $\neg\Box\bot$ není PA-platná, a tedy není v logice GL dokazatelná. Z toho je zároveň vidět, že schéma $\Box A \to A$ není PA-platné, což už ostatně víme z jednoho z příkladů.

Pravidlo Nec není v logice GL^ω z dobrého důvodu přípustné. Jeho použitím na již dokázanou formuli $\neg\Box\bot$ bychom dostali $\Box\neg\Box\bot$, což je formule, která jednak není **N**-platná, jednak je ve sporu s již dokázanou formulí $\neg\Box\neg\Box\bot$. Modální logiky, které jsou definovány axiomatickými schématy, mezi nimiž je alespoň L1 a L2, a schematickými odvozovacími pravidly, mezi nimiž je alespoň MP a Nec, se nazývají *normální modální logiky*. Logika GL je, logika GL^ω není normální modální logika.

Schématu $\Box A \to A$ se říká *schéma reflexe*. Toto schéma lze v přirozené řeči považovat za korektní a v několika modálních logikách vystupuje jako axiom. Jeho **N**-platnost se odvolává na fakt, že struktura **N** je modelem Peanovy aritmetiky. To je argument, který není možno formalizovat uvnitř PA. Peanova aritmetika ví, že ve sporné teorii je dokazatelné cokoliv, ale neví o sobě, je-li bezesporná. Nemůže tedy s jistotou tvrdit, že jen pravdivé sentence jsou v ní dokazatelné. Ve skutečnosti to ovšem je pravda.

Až dokážeme úplnost logiky GL^ω vůči aritmetické sémantice, budeme zároveň vědět, že schéma reflexe je vlastně jediný obecný fakt o dokazatelnosti, který je platný ve skutečnosti, jehož platnost ale není známa uvnitř Peanovy aritmetiky.

$$\dfrac{\dfrac{\dfrac{\langle\, \Box p, p, \Box\Box p \;\Rightarrow\; \Box p \,\rangle}{\langle\, \Box p \;\Rightarrow\; \Box\Box p \,\rangle} \qquad \dfrac{\dfrac{\dfrac{\langle\, \Box p \;\Rightarrow\; \Box p, \bot \,\rangle}{\langle\, \Box p, \neg\Box p \;\Rightarrow\; \bot \,\rangle} \quad \langle\, p \;\Rightarrow\; p \,\rangle}{\langle\, \Box p, p \to \neg\Box p, p \;\Rightarrow\; \bot \,\rangle}}{\langle\, \Box\Box p, \Box(p \to \neg\Box p), \Box p \;\Rightarrow\; \Box\bot \,\rangle}}{\langle\, \Box p, \Box(p \to \neg\Box p) \;\Rightarrow\; \Box\bot \,\rangle}}{\langle\, \Box(p \to \neg\Box p) \;\Rightarrow\; \Box p, \neg\Box\bot \,\rangle}}{\langle\, \Box(p \to \neg\Box p), \neg\Box\bot \;\Rightarrow\; \neg\Box p \,\rangle}$$

Obrázek 5.3.1: Důkaz v gentzenovském kalkulu pro logiku GL

Gentzenovský kalkulus pro logiku GL vznikne přidáním jediného (!) modálního pravidla ke gentzenovskému výrokovému systému z kapitoly 1:

$$\Box\text{-r:} \qquad \langle\, \Gamma, \Box\Gamma, \Box A \;\Rightarrow\; A \,\rangle \;/\; \langle\, \Box\Gamma \;\Rightarrow\; \Box A \,\rangle,$$

kde $\Box\Gamma$ značí množinu $\{\, \Box B \,;\, B \in \Gamma \,\}$. Všimněme si, že pravidlo $\Box$-r je použitelné jen tak, že před jeho použitím i po něm je sukcedent jednoprvkový. V tom se pravidlo $\Box$-r podobá kritickým pravidlům intuicionistického gentzenovského kalkulu. Dále si všimněme, že následující jednodušší (odvozená) modální pravidla lze snadno simulovat pomocí pravidla $\Box$-r a několikanásobného užití pravidla W:

$$\dfrac{\langle\, \Box\Gamma \;\Rightarrow\; A \,\rangle}{\langle\, \Box\Gamma \;\Rightarrow\; \Box A \,\rangle} \qquad\qquad \dfrac{\langle\, \Gamma \;\Rightarrow\; A \,\rangle}{\langle\, \Box\Gamma \;\Rightarrow\; \Box A \,\rangle.}$$

Pamatujme si tedy, že pravidlo $\Box$-r umožňuje odstranit z antecedentu sekventu libovolnou formuli B, pokud je pravda, že v antecedentu je i formule $\Box B$ nebo že ji tam přidáme, a pokud současně v sukcedentu je jediná formule A, kterou musíme

nahradit formulí $\Box A$. Přitom byla-li v antecedentu formule $\Box A$, je povoleno ji odstranit bez náhrady. Je vidět, že pravidlo $\Box$-r i jeho odvozené varianty zachovávají podformule.

Na obrázku 5.3.1 jsme na ukázku převedli do gentzenovského kalkulu již dříve uvedený fregovský důkaz modální verze První Gödelovy věty. V tomto důkazu je pravidlo $\Box$-r užito dvakrát. Jednou má formule A tvar $\Box p$, podruhé je užito odvozené pravidlo $\langle\, \Gamma \Rightarrow A \,\rangle \;/\; \langle\, \Box\Gamma \Rightarrow \Box A \,\rangle$ a formule A má tvar $\bot$. V důkazu je také jednou užito pravidlo řezu na formuli $\Box\Box p$. Protože v tomto oddílu mezi základní logické symboly počítáme i symbol $\bot$, předpokládáme, že v našem kalkulu máme také pravidlo příslušné k tomuto symbolu, totiž pravidlo

$$\bot\text{-l:} \qquad / \;\langle\, \Gamma, \bot \Rightarrow \Delta \,\rangle,$$

které jsme dosud explicitně neformulovali, ale vlastně o něm byla řeč ve cvičeních oddílu 1.4. V důkazu z obrázku 5.3.1 se toto pravidlo neuplatnilo. Žádné pravé pravidlo pro symbol $\bot$ neexistuje, stejně jako neexistuje žádné levé pravidlo pro modalitu. Nepokoušíme se sestrojit gentzenovský kalkulus pro logiku GL^ω, bez toho se v dalším obejdeme.

Věta 5.3.12 *Je-li formule A dokazatelná ve fregovském kalkulu pro logiku GL, pak sekvent $\langle \Rightarrow A \rangle$ je dokazatelný v gentzenovském kalkulu. Naopak, je-li sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ dokazatelný v gentzenovském kalkulu pro logiku GL, pak formule $\bigwedge \Gamma \to \bigvee \Delta$ je dokazatelná ve fregovském kalkulu.*

Důkaz V následujících třech řádcích je sekvent vpravo vždy odvoditelný jediným krokem dle pravidla $\Box$-r ze sekventu vlevo:

$$\langle\, \Box(A \to B), \Box A, A \to B, A, \Box B \Rightarrow B \,\rangle \;/\; \langle\, \Box(A \to B), \Box A \Rightarrow \Box B \,\rangle,$$
$$\langle\, \Box A, A, \Box\Box A \Rightarrow \Box A \,\rangle \;/\; \langle\, \Box A \Rightarrow \Box\Box A \,\rangle,$$
$$\langle\, \Box(\Box A \to A), \Box A \to A, \Box A \Rightarrow A \,\rangle \;/\; \langle\, \Box(\Box A \to A) \Rightarrow \Box A \,\rangle.$$

Ve všech případech lze sekvent vlevo velmi rychle dokázat, a to bez dalšího užití modálního pravidla. V druhém případě máme dokonce iniciální sekvent. Ze sekventu vpravo lze jedním nebo dvěma kroky dokázat axiom L2 resp. L3 resp. L4. Simulaci pravidel MP a Nec přenecháváme čtenáři.

Simulace pravidla $\Box$-r ve fregovském kalkulu je také jednoduchá. Předpokládejme, že sekvent $\langle\, \Box\Gamma \Rightarrow \Box A \,\rangle$ byl jedním krokem odvozen ze sekventu $\langle\, \Gamma, \Box\Gamma, \Box A \Rightarrow A \,\rangle$ a že již máme fregovský důkaz formule $\bigwedge \Gamma \,\&\, \bigwedge \Box\Gamma \,\&\, \Box A \to A$. Tento důkaz můžeme přepracovat (doplnit) na důkaz formule $\bigwedge \Box\Gamma \to \Box A$:

1:	$\bigwedge \Gamma \,\&\, \bigwedge \Box\Gamma \,\&\, \Box A \to A$	
2:	$\bigwedge \Gamma \,\&\, \bigwedge \Box\Gamma \to (\Box A \to A)$	
3:	$\Box(\bigwedge \Gamma \,\&\, \bigwedge \Box\Gamma) \to \Box(\Box A \to A)$	; Nec, L2
4:	$\Box(\bigwedge \Gamma \,\&\, \bigwedge \Box\Gamma) \to \Box A$	; L4

5: $\bigwedge \Box\Gamma \,\&\, \bigwedge \Box\Box\Gamma \to \Box A$

6: $\bigwedge \Box\Gamma \to \Box A$; L3.

V odvození řádku 5 jsme využili již známý fakt, že modalita nutnosti komutuje s konjunkcí (viz náš druhý příklad důkazu v kalkulu pro logiku GL). V posledním řádku jsme z premisy implikace odstranili formule $\Box\Box B$, kde $B \in \Gamma$. Každá z nich je totiž zbytečná, neboť vyplývá z formule $\Box B$, která se v premise implikace vyskytuje také. QED

5.3.3 Kripkovská sémantika

V této části ukážeme, že logika dokazatelnosti má kromě aritmetické sémantiky také uspokojivou kripkovskou sémantiku v mnohém podobnou sémantice intuicionistické logiky.

Definici dobrého uspořádání lze snadno rozšířit i na uspořádání, které není lineární, nebo dokonce na libovolnou relaci. Tak dostaneme pojem fundované relace. Relace $R \subseteq A^2$ je *fundovaná* na množině A, jestliže pro každou neprázdnou podmnožinu $Y \subseteq A$ existuje prvek $a \in Y$ takový, že

$$\forall x \in A(x\ R\ a \Rightarrow x \notin Y).$$

Jinými slovy, každá neprázdná podmnožina Y množiny A má R-minimální prvek. Každá fundovaná relace je automaticky antireflexivní: kdyby pro nějaké x platilo $x\ R\ x$, množina $\{x\}$ by neměla R-minimální prvek. Naopak, každá tranzitivní a antireflexivní relace na *konečné* množině je fundovaná.

Definice 5.3.13 *Řekneme, že dvojice $\langle W, R\rangle$ je* kripkovský rámec (pro logiku dokazatelnosti)*, jestliže $W \neq \emptyset$ a $R \subseteq W^2$ je tranzitivní relace taková, že relace R^{-1} je fundovaná.*

Požadujeme tedy, aby každá neprázdná podmnožina množiny W měla maximální prvek vzhledem k relaci R. Domluvme se, že stejně jako v oddílu o intuicionistické logice mluvíme o prvcích rámce jako o *vrcholech*, případný nejmenší vrchol je *kořen*, maximální vrcholy jsou *listy*. Relace R je *relace dosažitelnosti*.

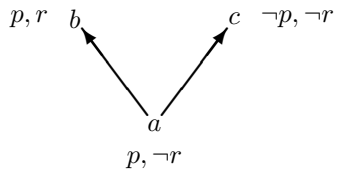
Definice 5.3.14 *Řekneme, že trojice $\langle W, R, \Vdash\rangle$ je* kripkovský model (pro logiku dokazatelnosti)*, jestliže $\langle W, R\rangle$ je kripkovský rámec a relace $\Vdash$ (pravdivostní relace) splňuje podmínky:*

- *$x \Vdash A \to B$, právě když $x \nVdash A$ nebo $x \Vdash B$, a podobně pro všechny ostatní logické spojky (pro $\bot$ to znamená $x \nVdash \bot$),*
- *$x \Vdash \Box A$, právě když $\forall y \in W(x\ R\ y \Rightarrow y \Vdash A)$.*

Zápis $x \Vdash A$ čteme stejně jako v intuicionistické logice „formule A je splněna ve vrcholu x“ nebo „x splňuje (formuli) A“. Modalita nutnosti se chová podobně jako implikace a negace v intuicionistické logice: pravdivostní hodnota formule $\Box A$

ve vrcholu x závisí na pravdivostní hodnotě formule A ve vrcholech dosažitelných z x (ve světech možných z hlediska x). Naproti tomu implikace a negace se chovají „klasicky“: pravdivostní hodnota formule $\neg A$ nebo $A \to B$ ve vrcholu x závisí jen na pravdivostních hodnotách formulí A a B v témže vrcholu x. Negace formule A je v x splněna, právě když A v x splněna není. Definice neříká nic o ohodnocení výrokových atomů. Pravdivostní hodnota atomu p ve vrcholu x může být zvolena libovolně a bez ohledu na ohodnocení atomu p v ostatních vrcholech. V kripkovské sémantice logiky dokazatelnosti tedy na rozdíl od intuicionistické logiky nemáme žádnou podmínku perzistence.

Příklad 5.3.15 Vzhledem k tomu, že negace se vyčísluje klasicky, můžeme kripkovský model graficky znázornit tak, že ke každému vrcholu připíšeme například p nebo $\neg p$ podle toho, zda atom p v onom vrcholu je nebo není splněn, viz obrázek 5.3.2. Z vrcholu b není dosažitelný žádný vrchol (ani b, relace dosažitelnosti je antireflexivní), takže $b \Vdash \Box A$ pro libovolnou formuli A. Totéž lze říci i o vrcholu c. Z a jsou dosažitelné vrcholy b a c, a v obou je splněna formule $p \to r$, tedy $a \Vdash \Box(p \to r)$. Platí také $a \Vdash \Box\Box\bot$, protože formule $\Box\bot$ je splněna ve všech (obou) vrcholech dosažitelných z a. Připomeňme, že $\Diamond A$ je zkratka pro formuli $\neg\Box\neg A$. V našem modelu platí například $b \nVdash \Diamond p$ a $a \Vdash \Diamond p$.



Obrázek 5.3.2: Kripkovský model pro logiku dokazatelnosti

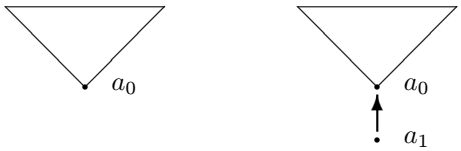
Řekneme, že *formule A platí v modelu* $\langle W, R, \Vdash\rangle$, jestliže A je splněna v každém vrcholu x z W. *Sekvent* $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ *platí v modelu* $\langle W, R, \Vdash\rangle$, jestliže v každém vrcholu $x \in W$, ve kterém jsou splněny všechny formule z Γ, je splněna také některá formule z Δ. Řekneme, že formule A nebo sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ *platí v kripkovském rámci* $\langle W, R\rangle$, jestliže formule A resp. sekvent $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ platí v každém modelu $\langle W, R, \Vdash\rangle$, tj. jestliže A či $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ platí při každé volbě pravdivostní relace $\Vdash$ na $\langle W, R\rangle$.

Příklad 5.3.16 Formule $r \to p$, $\Box(r \to p)$ a $\Box(p \to r)$ platí, formule $p \to r$ neplatí v modelu z obrázku 5.3.2.

Příklad 5.3.17 V jakémkoliv modelu $\langle W, R, \Vdash\rangle$ je formule $\Box\bot$ splněna ve vrcholu x právě tehdy, když z x není dosažitelný žádný (jiný) vrchol, tj. když x je maximálním prvkem (listem) v rámci $\langle W, R\rangle$. Formule $\neg\Box\bot$ neplatí v žádném rámci, protože z fundovanosti plyne, že nějaké maximální prvky existovat musí. Relace R může být i prázdná. V tom případě v rámci $\langle W, R\rangle$ platí formule $\Box\bot$.

Definice 5.3.18 *Nechť $\langle W, R, \Vdash\rangle$ je kripkovský model pro logiku dokazatelnosti. Řekneme, že vrchol $x \in W$ je* Δ-korektní*, kde Δ je množina modálních formulí, jestliže x splňuje formuli $\Box D \to D$, kdykoliv $\Box D$ je podformule některé formule v množině Δ. Vrchol $x \in W$ je* A-korektní*, kde A je modální formule, jestliže x je $\{A\}$-korektní.*

Příklad 5.3.19 V modelu z obrázku 5.3.2 vrchol b je $(\Box p)$-korektní. Vrchol b ale není $(\Box\neg p)$-korektní, protože platí $b \Vdash \Box\neg p$ a $b \not\Vdash \neg p$. Vrchol a není $(\Box(p\to r))$-korektní, je $(\Box(r \to p))$-korektní nebo třeba $(\Box(r \to p) \,\&\, \neg\Box\bot)$-korektní. Vrchol a je také $(\Diamond p)$- i $(\Diamond\neg r)$-korektní, není $(\Diamond(p \,\&\, \neg r))$-korektní.



Obrázek 5.3.3: Přidání nového kořenu ke kripkovskému modelu

Bohužel, termín „korektní“ je v této kapitole trochu přetížen. Korektní pravidla, axiomy a kalkuly, a teď ještě korektní vrcholy kripkovských modelů.

Nyní směřujeme k důkazu korektnosti logik GL a GL^ω vůči kripkovské sémantice. Důkaz pro logiku GL^ω je o dost komplikovanější a budeme v něm potřebovat lemma, které se týká situace jako na obrázku 5.3.3. Nalevo je kripkovský rámec s kořenem a_0, rámec vpravo je z něj utvořen přidáním nového kořenu a_1. Dosavadní kořen a_0 je v novém rámci dosažitelný jen z vrcholu a_1.

Lemma 5.3.20 *Nechť A je modální formule, $\langle W, R, \Vdash\rangle$ je kripkovský model s kořenem a_0 a a_0 je A-korektní vrchol modelu $\langle W, R, \Vdash\rangle$. Nechť rámec $\langle W', R'\rangle$ je utvořen z rámce $\langle W, R\rangle$ přidáním nového kořenu a_1 jako na obrázku 5.3.3. Nechť pravdivostní relace $\Vdash'$ rozšiřuje relaci $\Vdash$ tak, že každý výrokový atom má v a_1 tutéž pravdivostní hodnotu, jako měl (a má stále) v a_0. Pak A má v a_0 i v a_1 tutéž pravdivostní hodnotu a nový kořen a_1 je A-korektní.*

Důkaz Dokážeme indukcí podle složitosti podformule B formule A, že B má v a_0 a v a_1 tutéž pravdivostní hodnotu, a pokud B začíná modalitou, neporušuje A-korektnost vrcholu a_1. Pro atomy je to pravda, tak byly hodnoty atomů v a_1 zvoleny. Je-li B sestavena pomocí některé logické spojky z formulí, které mají v a_0 i v a_1 stejnou pravdivostní hodnotu, pak i B má v a_0 i v a_1 stejnou pravdivostní hodnotu. Nechť B začíná modalitou, $B = \Box D$. Když $a_0 \Vdash \neg\Box D$, podle definice pravdivostní relace to znamená, že pro nějaký vrchol x dosažitelný z a_0 platí $x \not\Vdash D$. Vrchol x je dosažitelný i z a_1, tedy $a_1 \Vdash \neg\Box D$. Když $a_0 \Vdash \Box D$, pak $a_0 \Vdash D$ (vzhledem ke korektnosti vrcholu a_0), $a_1 \Vdash \Box D$ (protože D je splněna ve všech vrcholech dosažitelných z a_1) a $a_1 \Vdash D$ (protože, podle indukčního předpokladu, D má

stejnou hodnotu v a_0 i v a_1). V obou případech má formule $\Box D$ stejnou pravdivostní hodnotu v a_0 i v a_1 a neporušuje A-korektnost vrcholu a_1. QED

Věta 5.3.21 (korektnost vůči kripkovské sémantice) *(a) Když $GL \vdash A$, pak formule A platí v každém kripkovském modelu.*
(b) Když $GL^\omega \vdash A$, pak je formule A splněna v každém A-korektním vrcholu libovolného kripkovského modelu.

Důkaz Uvažujme Löbův axiom L4. Nechť A je modální formule a nechť x je vrchol nějakého kripkovského modelu $\langle W, R, \Vdash\rangle$. Předpokládejme, že $x \not\Vdash \Box A$. Chceme dokázat $x \not\Vdash \Box(\Box A \to A)$. Uvažujme množinu Y všech vrcholů dosažitelných z x, ve kterých formule A není splněna: $Y = \{\, y \in W \,;\, x\, R\, y \;\&\; y \not\Vdash A \,\}$. Z $x \not\Vdash \Box A$ plyne, že $Y \neq \emptyset$. Díky fundovanosti relace R existuje nějaký R-maximální prvek množiny Y. Označme y_0 některý takový maximální vrchol. Uvažujme libovolný vrchol z dosažitelné z vrcholu y_0. Díky tranzitivitě relace R platí $x\, R\, z$, tj. vrchol z je dosažitelný z x. Kdyby platilo $z \not\Vdash A$, měli bychom $z \in Y$, tedy spor s tím, že vrchol y_0 je maximální v množině Y. Tedy $z \Vdash A$. Toto platí pro každý vrchol z dosažitelný z vrcholu y_0 (netvrdíme ovšem, že takové vrcholy z existují). Tedy $y_0 \Vdash \Box A$. Vrchol y_0 je dosažitelný z vrcholu x a splňuje formuli $\Box A \,\&\, \neg A$. Tedy není pravda, že implikace $\Box A \to A$ je splněna ve všech vrcholech dosažitelných z x, a tedy opravdu $x \not\Vdash \Box(\Box A \to A)$.

Dokázali jsme, že (každý) Löbův axiom je splněn v každém vrcholu x libovolného kripkovského modelu. Löbův axiom tedy platí v každém kripkovském modelu. Ověření platnosti ostatních axiomů logiky GL přenecháváme čtenáři. Důkaz bodu (a) lze uzavřít konstatováním, že množina všech modálních formulí splněných v daném vrcholu x daného modelu $\langle W, R, \Vdash\rangle$ je uzavřena na pravidlo MP a množina všech modálních formulí platných v daném modelu $\langle W, R, \Vdash\rangle$ je navíc uzavřena na pravidlo Nec.

Nechť nyní $A_1, \ldots, A_k (= A)$ je důkaz formule A v logice GL^ω. Nechť $\langle W, R, \Vdash\rangle$ je libovolný kripkovský model a a_0 jeho A-korektní vrchol. Chceme ověřit $a_0 \Vdash A$. Jako obvykle můžeme předpokládat, že a_0 je kořen rámce $\langle W, R\rangle$. Potíž je v tom, že nemůžeme rovnou dokázat indukcí podle j, že $a_0 \Vdash A_j$. Nevíme totiž, zda v a_0 jsou splněny všechny axiomy $\Box D \to D$ použité v důkazu. Z korektnosti vrcholu a_0 plyne pouze, že to platí, je-li $\Box D$ podformulí formule A. Potřebovali bychom vědět, že a_0 je nejen A-korektní, ale dokonce $\{A_1, \ldots, A_k\}$-korektní.

Vezměme v úvahu všechny formule $\Box D$ vyskytující se v důkazu $A_1, \ldots, A_k$. Zvolme číslo n větší, než je jejich počet. Použijme n-krát lemma 5.3.20 o přidání nového kořenu. To znamená, že k modelu přidáme n nových vrcholů $a_1, \ldots, a_n$, vrchol a_i prohlásíme za dosažitelný z vrcholů a_j pro $j > i$, a jen z nich, a každému atomu přidělíme v nových vrcholech $a_1, \ldots, a_n$ tutéž pravdivostní hodnotu, jakou měl v a_0.

Vezměme libovolnou formuli $\Box D$ vyskytující se v důkazu $A_1, \ldots, A_k$. Pokud $\Box D$ je zároveň podformulí formule A, víme o ní z lemmatu, že cestou proti směru šipek od a_0 k a_n nemění pravdivostní hodnotu. Pokud $\Box D$ není podformulí formule A,

cestou od a_0 k a_n pravdivostní hodnotu změnit může, ale z definice pravdivostní relace vyplývá, že jen z $\Box D$ na $\neg\Box D$, a tedy nejvýše jednou. Protože n je větší než počet všech takových formulí $\Box D$, existuje i takové, že od a_i k a_{i+1} se nestane nic: žádná formule $\Box D$ vyskytující se v důkazu $A_1, \ldots, A_k$ nezmění pravdivostní hodnotu. Snadno se ověří, že v tom případě vrchol a_i je $\{A_1, \ldots, A_k\}$-korektní. Indukcí podle j dostaneme, že a_i splňuje každou formuli A_j, tedy $a_i \Vdash A$. Lemma říká, že formule A má v a_i a v a_0 stejnou pravdivostní hodnotu, tedy $a_0 \Vdash A$. QED

Úplnost obou systémů vůči kripkovské sémantice lze dokazovat různým způsobem. Ve Smoryńského knize [80] je důkaz, jehož vedlejším produktem je důkaz úplnosti i pro logiku K4 a případně i jiné modální systémy. V Solovayově článku [86] je kratší důkaz jen pro logiku dokazatelnosti. My se přidržíme postupu paralelního s předchozím oddílem. To nám umožní využít některé zkušenosti, které jsme udělali s intuicionistickou logikou. Na rozdíl od před chvílí uvedeného důkazu korektnosti logik GL a GL^ω, ve kterém jsme pracovali s fregovskými kalkuly, nyní dáváme přednost (vzhledem k větě 5.3.12 ekvivalentnímu) gentzenovskému kalkulu pro logiku GL. Úplnost logiky GL^ω (tj. úplnost jejího fregovského kalkulu) pak bude snadným důsledkem úplnosti logiky GL.

Věta 5.3.22 (úplnost logiky GL) *Je-li libovolný sekvent délky n dokazatelný v logice dokazatelnosti, pak má také bezřezový důkaz hloubky $\mathcal{O}(n^3)$. Není-li dokazatelný, pak má kripkovský protipříklad hloubky nejvýše n, v němž má každý vrchol nejvýše n následníků. Gentzenovský kalkulus pro logiku GL je tedy úplný vůči kripkovské sémantice intuicionistické logiky a platí pro něj věta o eliminovatelnosti řezů. Intuicionistická výroková logika má vlastnost FMP. Platí* PA-Taut $\in$ *PSPACE, tj. úloha rozhodnout, zda daný sekvent je logicky platný, je rozhodnutelná v polynomiálním prostoru.*

Důkaz Důkaz ponecháváme na čtenáři, protože je velmi podobný příslušnému důkazu v intuicionistické logice a opírá se o dvě lemmata podobná lemmatům 5.1.7 a 5.1.10. Z prvního lemmatu uveďme pouze vzorek:

> *sekvent $\langle \Gamma, A{\to}B \Rightarrow \Delta \rangle$ platí ve všech kripkovských modelech, právě když oba sekventy $\langle \Gamma \Rightarrow \Delta, A \rangle$ a $\langle \Gamma, B \Rightarrow \Delta \rangle$ platí ve všech kripkovských modelech,*

z kterého by mělo být jasné, jak je třeba formulovat zbývajících sedm případů (logická spojka taková nebo onaká, a to v antecedentu nebo v sukcedentu). Rozdíl oproti lemmatu 5.1.1 je v tom, že zkoumanou formuli nikdy v sekventu neponecháváme, takže vícenásobným užitím tohoto lemmatu je otázka, zda daný sekvent platí ve všech kripkovských modelech, převedena na tutéž otázku týkající se nikoliv uzavřeného sekventu (ten pojem zde odpadá), nýbrž na otázku týkající se sekventu, v němž jsou jen atomy a formule začínající modalitou.

Druhé lemma říká, že je-li $\langle \Box\Gamma, \Pi \Rightarrow \Box\Delta, \Lambda \rangle$ sekvent takový, že množiny Π a Λ obsahují pouze atomy, pak sekvent $\langle \Box\Gamma, \Pi \Rightarrow \Box\Delta, \Lambda \rangle$ platí ve všech kripkovských

modelech, právě když $(\Box\Gamma \cup \Pi) \cap (\Box\Delta \cup \Lambda) \neq \emptyset$, nebo existuje formule $A \in \Delta$ taková, že sekvent $\langle\, \Gamma, \Box\Gamma, \Box A \;\Rightarrow\; A \,\rangle$ platí ve všech kripkovských modelech. Důkaz je úplně stejný jako v případě lemmatu 5.1.10. Poznamenejme, že právě z tohoto lemmatu lze vypozorovat formulaci pravidla $\Box$-r.

Na obou lemmatech lze stejně jako v intuicionistické logice založit algoritmus, který rozhodne o logické platnosti daného sekventu, a to se stejným odhadem na paměťový prostor. I zde platí, že algoritmus k danému sekventu vlastně buď sestrojí konečný kripkovský protipříklad, nebo nalezne jeho bezřezový důkaz v gentzenovském kalkulu. Více podrobností o důkazu je v článku [90]. QED

Věta 5.3.23 (úplnost logiky GL$^\omega$) *Modální formule A je dokazatelná ve fregovském kalkulu pro logiku GL$^\omega$, právě když je splněna ve všech A-korektních vrcholech libovolného kripkovského modelu. Úloha* **N**-TAUT *je také v* PSPACE.

Důkaz Nechť A je libovolná modální formule. Sestavme seznam $\Box D_1, \ldots, \Box D_n$ všech jejích podformulí začínajících modalitou. Libovolný vrchol libovolného kripkovského modelu je A-korektní, právě když splňuje konjunkci $\bigwedge_{i=1}^{n}(\Box D_i \to D_i)$. To znamená, že podmínky (ii) a (iii) v následujícím seznamu jsou ekvivalentní:

(i) $\mathrm{GL}^\omega \vdash A$,

(ii) A je splněna v každém A-korektním vrcholu libovolného kripkovského modelu,

(iii) $\bigwedge_{i=1}^{n}(\Box D_i \to D_i) \to A$ platí v každém kripkovském modelu,

(iv) $\mathrm{GL} \vdash \bigwedge_{i=1}^{n}(\Box D_i \to D_i) \to A$.

Implikace (i) $\Rightarrow$ (ii) je již dokázaná věta o korektnosti logiky GL$^\omega$. Podmínky (iii) a (iv) jsou ekvivalentní podle věty o úplnosti pro logiku GL. Platí také implikace (iv) $\Rightarrow$ (i): formuli A lze dokázat z formule v (d) a z předpokladů $\Box D_i \to D_i$ bez užití pravidla Nec, tedy ji lze dokázat v kalkulu pro logiku GL$^\omega$. Tím jsme ověřili, že všechny čtyři podmínky jsou ekvivalentní.

Implikace (ii) $\Rightarrow$ (i) je to, co se mělo dokázat — úplnost logiky GL$^\omega$. Formuli v (iv) lze sestrojit z A v logaritmickém prostoru. Tedy ekvivalence (i) $\Leftrightarrow$ (iv) je vlastně převodem úlohy **N**-TAUT na úlohu PA-TAUT, a úloha **N**-TAUT je tedy v třídě *PSPACE*. QED

Zbývající část tohoto oddílu lze číst selektivně, zejména již máme pohromadě vše, co potřebujeme k důkazu věty 5.3.30 o aritmetické úplnosti GL a GL$^\omega$. To je upozornění pro netrpělivého čtenáře.

V souvislosti se sémantikou, ať už aritmetickou nebo kripkovskou, jsme se nikde nezmínili o kompaktnosti. Možná, že tady je určitý prostor pro další výzkum. Nevíme, zda pro aritmetické interpretace $\langle \mathbf{N}, \mathsf{Pr}_\pi \rangle$ a $\langle \mathsf{PA}, \mathsf{Pr}_\pi \rangle$ věta o kompaktnosti platí, dokonce si nejsme jisti, jak by se měla formulovat. Je ale známo, že pro kripkovskou sémantiku věta o kompaktnosti neplatí, viz cvičení.

V tomto pododdílu o kripkovské sémantice se ještě chceme zmínit o některých důsledcích věty o úplnosti logik GL a GL$^\omega$ vůči kripkovské sémantice a také dokázat,

že obě úlohy jsou *PSPACE*-kompletní. V následujícím pododdílu se zmíníme o některých důsledcích věty o eliminovatelnosti řezů pro logiku GL.

Definujme formuli $\boxdot A$, kde A je libovolná modální formule, jako zkratku za formuli $A \,\&\, \Box A$. Formuli $\boxdot A$ čteme „silně nutně A“. Symbol $\boxdot$ je odvozená modalita, říkejme jí *operátor silné nutnosti*.

Je-li nějaká aritmetická sentence φ (například $\mathsf{Con}(\pi) \to \neg\mathsf{Pr}_\pi(\overline{\mathsf{Con}(\pi)})$) v PA dokazatelná s pomocí předpokladu, že nějaká jiná sentence (například ν) splňuje nějakou autoreferenční podmínku (v našem případě $\vdash \nu \equiv \neg\mathsf{Pr}_\pi(\overline{\nu})$), pak φ je dokazatelná i bez tohoto předpokladu. V modální logice tento fakt vystihuje *pravidlo autoreference*:

DiR: $\quad \boxdot(q \equiv B) \to A \;/\; A,$

kde atom q se nevyskytuje ve formuli A, a navíc všechny jeho výskyty ve formuli B jsou v rozsahu platnosti některé modality $\Box$. Zkratka DiR znamená *diagonalization rule*. Místo „atom q se vyskytuje jen v rozsahu platnosti některé modality“ říkejme také, že atom q se vyskytuje pouze v modálním kontextu. Z následující věty a ze cvičení plyne, že kalkulus vzniklý přidáním pravidla DiR k logice K4 je ekvivalentní s logikou GL.

Věta 5.3.24 (de Jonghova) *Když $\mathrm{GL} \vdash \boxdot(q \equiv B) \to A$ a atom q se ve formuli B vyskytuje jen v modálním kontextu a nevyskytuje se ve formuli A, pak $\mathrm{GL} \vdash A$. Logika GL je tedy uzavřena na pravidlo DiR.*

Důkaz Předpokládejme $\mathrm{GL} \nvdash A$. Podle věty o úplnosti má formule A nějaký kripkovský protipříklad $K = \langle W, R, \Vdash\!\!-\rangle$. Změníme-li kdekoliv v modelu K ohodnocení atomu q, nebude to mít vliv na pravdivostní hodnoty formule A, protože ta atom q neobsahuje. Tvrdíme, že atomu q lze ve vrcholech modelu K přidělit (nové) pravdivostní hodnoty tak, aby v K platila formule $\boxdot(q \equiv B)$. Tím dostaneme protipříklad na formuli $\boxdot(q \equiv B) \to A$. Ukažme si postup na modelu z obrázku 5.3.2. Předpokládejme, že B je formule $\Box q \to p$. Chceme tedy zvolit pravdivostní hodnoty atomu q tak, aby ekvivalence $q \equiv (\Box q \to p)$ byla splněna ve všech třech vrcholech. Víme $b \Vdash\!\!- p$, $c \Vdash\!\!- \Box q$ a $c \Vdash\!\!- \neg p$, takže $b \Vdash\!\!- \Box q \to p$ a $c \nVdash \Box q \to p$. Ekvivalenci $q \equiv (\Box q \to p)$ lze tedy zaručit volbou $b \Vdash\!\!- q$ a $c \nVdash q$. Teď můžeme vyčíslit pravdivostní hodnotu formule $\Box q \to p$ ve vrcholu a. Vychází $a \Vdash\!\!- \Box q \to p$, volíme tedy $a \Vdash\!\!- q$. Výsledkem je platnost formule $q \equiv (\Box q \to p)$, a tedy i formule $\boxdot(q \equiv (\Box q \to p))$ v modelu K.

Stejně můžeme postupovat i v případě jakéhokoliv jiného modelu K a jakékoliv jiné formule B. V každém kroku zvolíme vrchol a, v němž dosud nebyla stanovena hodnota atomu q, ale byla již stanovena ve všech vrcholech dosažitelných z a. V prvním kroku to samozřejmě znamená zvolit za a některý z listů. Vzhledem k tomu, že atom q se v B vyskytuje jen v modálním kontextu, jeho pravdivostní hodnoty ve vrcholech dosažitelných z vrcholu a dovolují určit pravdivostní hodnotu formule B v samotném vrcholu a. Atomu q pak přidělíme tutéž pravdivostní hodnotu, kterou jsme zjistili pro B. Tím bude zajištěno $a \Vdash\!\!- q \equiv B$. QED

Ukažme si ještě jednu jednoduchou aplikaci věty o úplnosti. Mějme kripkovský protipříklad K na formuli A. Jako obvykle můžeme předpokládat, že model K má kořen. Rozšíříme-li model K na nový model K' tak, jak je naznačeno na obrázku 5.3.3 a popsáno v lemmatu 5.3.20, dostaneme protipříklad na formuli $\Box A$. Tím je zdůvodněno, že má-li jakákoliv formule A protipříklad, pak i formule $\Box A$ má protipříklad. Vzhledem k větě o úplnosti pro logiku GL vůči kripkovské sémantice to znamená, že množina všech formulí dokazatelných v logice GL je uzavřena na pravidlo opačné k pravidlu Nec, totiž na pravidlo $\Box A \,/\, A$. Týž fakt lze dokázat i důkazově teoreticky: je-li $\langle \Rightarrow \Box A \rangle$ poslední sekvent bezřezového důkazu, pak předposlední sekvent musí být $\langle \Box A \Rightarrow A \rangle$, a užití řezu na tyto dva sekventy dává sekvent $\langle \Rightarrow A \rangle$. Další podobné příklady jsou uvedeny ve cvičeních 14–16.

Věta 5.3.25 *Obě úlohy* PA-Taut *a* **N**-Taut *jsou PSPACE-kompletní.*

Důkaz I tento důkaz je podobný příslušnému důkazu o intuicionistické logice, takže postup jen naznačíme a upozorníme na některé rozdíly. Také zde definujeme převod úlohy QBF, začínáme tedy s kvantifikovanou výrokovou formulí A tvaru $Q_m p_m \,..\, Q_1 p_1 B(\underline{p})$, kde každý ze symbolů $Q_1, \ldots, Q_m$ je jeden z kvantifikátorů $\forall$ nebo $\exists$ a formule B neobsahuje další výrokové kvantifikátory ani jiné atomy než $p_1, \ldots, p_m$. K formuli A sestrojíme modální formuli A^* podobným způsobem jako v intuicionistické logice:

$$\begin{aligned} A_0^* &= B(\underline{p}) \\ A_j^* &= \begin{cases} \Diamond(q_j \,\&\, (\boxdot p_j \vee \boxdot \neg p_j)) \,\&\, \Box(q_j \to A_{j-1}^*) & \text{pokud } Q_j = \exists \\ \Diamond(q_j \,\&\, \boxdot p_j) \,\&\, \Diamond(q_j \,\&\, \boxdot \neg p_j) \,\&\, \Box(q_j \to A_{j-1}^*) & \text{jinak} \end{cases} \\ A^* &= A_m^*. \end{aligned}$$

Stejným způsobem jako v intuicionistické logice se dokáže, že formule A platí, právě když formule A^* je splněna v některém vrcholu některého kripkovského modelu, tj. právě když formule $\neg A^*$ není dokazatelná v logice GL.

Navíc dokážeme, že když formule A^* je splněna v některém vrcholu kripkovského modelu, pak je splněna i v některém A^*-korektním vrcholu. To se udělá takto. Nechť A^* je splněna ve vrcholu a modelu $\langle W, R, \Vdash \rangle$. Předpokládejme, že model je konečný a vrchol a je jeho kořenem. Všechny atomy ve formuli A^* se vyskytují jen v modálním kontextu, a změníme-li jejich pravdivostní ohodnocení ve vrcholu a, nebude to mít vliv na pravdivostní hodnotu formule A^* ve vrcholu a. Změníme je tak, aby vrchol a byl A^*-korektní.

Vezměme v úvahu, že $\Diamond$ je zkratka za $\neg\Box\neg$ a také $\boxdot$ je zkratka, a napišme si seznam všech podformulí formule A^*, které začínají modalitou $\Box$:

$$\Box p_j, \quad \Box\neg p_j, \quad \Box\neg(q_j \,\&\, \boxdot p_j), \quad \Box\neg(q_j \,\&\, \boxdot\neg p_j), \quad \Box(q_j \to A_{j-1}^*),$$

kde $1 \leq j \leq m$. Může se stát, že ve vrcholu a je splněna některá z formulí $\Box p_j$ a $\Box\neg p_j$, ale ne obě najednou: formule A obsahuje modality pouze v případě,

kdy $m \neq 0$, a tehdy jsou z vrcholu a určitě dosažitelné nějaké jiné vrcholy. Správnou volbou pravdivostní hodnoty atomu p_j ve vrcholu a lze zajistit, že žádná z prvních dvou formulí neporušuje A^*-korektnost vrcholu a. Volbou $a \nVdash q_j$ lze zajistit, že ani žádná ze zbývajících tří formulí neporušuje A^*-korektnost.

Dokázali jsme, že když formule A neplatí, pak je formule $\neg A^*$ dokazatelná v logice GL (protože nemá žádný kripkovský protipříklad), a když A platí, pak formule $\neg A^*$ má dokonce A^*-korektní protipříklad. Funkce $A \mapsto \neg A^*$ tedy redukuje úlohu QBF (přesněji řečeno, její komplement $\overline{\mathrm{QBF}}$, ale víme, že je to jedno) zároveň na úlohu PA-Taut i na úlohu **N**-Taut. Obě úlohy jsou tedy *PSPACE*-kompletní. QED

Stejně jako v případě intuicionistické logiky je podstatným krokem v předchozím důkazu nalezení takové posloupnosti $\{ A_n ; n \in \mathrm{N} \}$ formulí, že délka formule A_n roste polynomiálně s n, každá formule A_n má kripkovský protipříklad, avšak délka minimálního kripkovského protipříkladu na formuli A_n roste exponenciálně s n. Ve cvičení 19 je ukázáno, že v případě logiky dokazatelnosti lze při konstrukci formulí A_n vystačit s jediným atomem. Tento výsledek lze způsobem analogickým jako v důkazu vět 5.1.16 a 5.3.25 doplnit na důkaz tvrzení, že úloha PA-Taut zůstane *PSPACE*-kompletní úlohou i v případě, omezíme-li se na jediný výrokový atom.

5.3.4 Některé aplikace v metamatematice

Aritmetické sentenci φ, která je řešením nějaké autoreferenční rovnice, tj. která splňuje podmínku tvaru $\mathsf{PA} \vdash \varphi \equiv \psi(\overline{\varphi})$, můžeme říkat *pevný bod* formule $\psi(x)$. Věta o autoreferenci zaručuje, že každá aritmetická formule *má* nějaký pevný bod. V úvodu k tomuto oddílu jsme se v souvislosti s Löbovou větou zmínili o otázce, zda aritmetická sentence je faktem, že splňuje nějakou autoreferenční podmínku, určena jednoznačně. To je otázka po *jednoznačnosti* pevných bodů: jsou každé dva pevné body nějaké formule $\psi(x)$ navzájem ekvivalentní? V tomto pododdílu mimo jiné uvidíme, že s pomocí modální logiky lze na tuto otázku určitým způsobem odpovědět. Zatím víme, že alespoň pro některé formule ψ je odpověď ano. Každé dva pevné body formule $\neg \mathsf{Pr}_\pi(x)$ jsou spolu ekvivalentní, protože jsou ekvivalentní se sentencí $\mathsf{Con}(\pi)$. Každý pevný bod formule $\mathsf{Pr}_\pi(x)$ je podle Löbovy věty dokazatelný, tedy ekvivalentní se sentencí $0=0$.

Mějme nějakou modální formuli A, výrokový atom p a jiný výrokový atom q, který se nevyskytuje ve formuli A. Současně s formulí A uvažujme formuli $A_p(q)$ vzniklou z formule A substitucí atomu q za všechny výskyty atomu p. Uvědomme si, že $(A_p(q))_q(p)$ je formule A a pišme $A(p)$ a $A(q)$ místo A a $A_p(q)$. Formule $A(p)$ a $A(q)$ mohou ovšem obsahovat i jiné atomy než p a q.

Věta 5.3.26 *(a) Jsou-li formule A a atomy p a q jako výše, pak v logice GL lze dokázat sekvent $\langle\, \Box(p \equiv q) \Rightarrow \Box(A(p) \equiv A(q)) \,\rangle$.*
(b) Pokud se navíc atom p vyskytuje ve formuli $A(p)$ pouze v modálním kontextu, pak je v logice GL dokazatelný i sekvent $\langle\, \Box(p \equiv q) \Rightarrow A(p) \equiv A(q) \,\rangle$.

Důkaz V (a) postupujme indukcí podle počtu logických symbolů ve formuli $A(p)$. Je-li jich nula, máme sekvent $\langle\, \Box(p \equiv q) \;\Rightarrow\; \Box(p \equiv q) \,\rangle$ nebo $\langle\, \Box(p \equiv q) \;\Rightarrow\; \Box(r \equiv r) \,\rangle$, který je v obou případech evidentně dokazatelný. Když $A(p)$ má tvar $B(p) \vee C(p)$, pak indukční předpoklad dává důkazy sekventů $\langle\, \Box(p \equiv q) \;\Rightarrow\; \Box(B(p) \equiv B(q)) \,\rangle$ a $\langle\, \Box(p \equiv q) \;\Rightarrow\; \Box(C(p) \equiv C(q)) \,\rangle$. V tom případě sestrojme samostatně důkaz sekventu $\langle\, \Box(B(p) \equiv B(q)), \Box(C(p) \equiv C(q)) \;\Rightarrow\; \Box(B(p) \vee C(p) \equiv B(q) \vee C(q)) \,\rangle$ a požadovaný sekvent $\langle\, \Box(p \equiv q) \;\Rightarrow\; \Box(B(p) \vee C(p) \equiv B(q) \vee C(p)) \,\rangle$ odvoďme dvěma řezy.

V (b) postupujme také indukcí, avšak podle počtu kroků, kterými je formule A utvořena pomocí logických spojek z formulí začínajících modalitou. Bázi indukce lze snadno odvodit z tvrzení (a), kroky týkající se logických spojek jsou podobné jako v důkazu tvrzení (a). Podrobnosti opět ponecháváme na čtenáři. QED

Věta 5.3.27 *Jsou-li formule A a atomy p a q jako výše a atom p se ve formuli $A(p)$ vyskytuje pouze v modálním kontextu, pak v logice GL lze dokázat sekvent $\langle\, \Box(p \equiv A(p)), \Box(q \equiv A(q)) \;\Rightarrow\; \Box(p \equiv q) \,\rangle$.*

Důkaz Sekvent

1: $\quad \langle\, p \equiv A(p), q \equiv A(q), A(p) \equiv A(q) \;\Rightarrow\; p \equiv q \,\rangle$

je tautologický a jako takový je dokazatelný (bez užití pravidla $\Box$-r). Dále postupujme takto:

2: $\quad \langle\, \Box(p \equiv q) \;\Rightarrow\; A(p) \equiv A(q) \,\rangle$; Věta 5.3.26(b)

3: $\quad \langle\, p \equiv A(p), q \equiv A(q), \Box(p \equiv q) \;\Rightarrow\; p \equiv q \,\rangle$; 1, 2, Cut

4: $\quad \langle\, \Box(p \equiv A(p)), \Box(q \equiv A(q)) \;\Rightarrow\; \Box(p \equiv q) \,\rangle$; 3, W, $\Box$-r.

QED

Větu 5.3.26 můžeme označit jako větu o substituci, věta 5.3.27 je věta o jednoznačnosti pevných bodů pro logiku dokazatelnosti. Jak už jsme poznamenali, je-li $\psi(x)$ formule $\neg\mathsf{Pr}_\pi(x)$ nebo formule $\mathsf{Pr}_\pi(x)$, pak řešení φ rovnice $\vdash \varphi \equiv \psi(\overline{\varphi})$ je určeno jednoznačně v tom smyslu, že každé dva pevné body jsou spolu dokazatelně ekvivalentní. Na základě věty 5.3.27 můžeme usoudit, že je to pravda i o mnoha dalších formulích $\psi(x)$. Ukažme si úvahu na formuli $\mathsf{Pr}_\pi(x) \to \chi$ z důkazu Löbovy věty. Věta 5.3.27 říká, že modální formule B:

$$(\Box(p \equiv \Box p \to r) \;\&\; \Box(q \equiv \Box q \to r) \to \Box(p \equiv q))$$

je dokazatelná v logice GL. Tedy musí být **N**-platná. Kdybychom ale měli dvě navzájem neekvivalentní sentence λ_1 a λ_2 splňující podmínky $\mathsf{PA} \vdash \lambda_1 \equiv \mathsf{Pr}_\pi(\overline{\lambda_1}) \to \chi$ a $\mathsf{PA} \vdash \lambda_2 \equiv \mathsf{Pr}_\pi(\overline{\lambda_2}) \to \chi$, měli bychom zároveň aritmetický protipříklad na formuli B: při ohodnocení atomů p, q a r sentencemi λ_1, λ_2 a χ by v **N** neplatil překlad formule B.

Věta 5.3.27 říká, že autoreferenční rovnice $\vdash \varphi \equiv \psi(\overline{\varphi})$ má jednoznačně určený pevný bod za podmínky, že sentence $\psi(\overline{\varphi})$ je tvaru A^*, kde $A(p)$ je modální formule a $*$ je aritmetický překlad, který atomu p přiřazuje hodnotu (aritmetickou sentenci) φ. Takovým autoreferenčním rovnicím můžeme říkat *gödelovské*. Užitím modální logiky jsme tedy ukázali, že všechny gödelovské autoreferenční rovnice mají jednoznačně (až na dokazatelnou ekvivalenci) určené řešení.

Zdaleka ne všechny autoreferenční rovnice jsou gödelovské. Příkladem formule $\psi(x)$, na kterou se věta 5.3.27 nevztahuje, je formule $\mathsf{před\ každým\ důkazem\ sentence}\ x\ \mathsf{existuje\ menší\ důkaz\ její\ negace}\ \neg x$, jejímž řešením je Rosserova sentence, viz 4.5.6. O jisté variantě Rosserovy sentence je v článku [29] dokázáno, že není svou autoreferenční rovnicí určena jednoznačně. Žádná obecná věta o jednoznačné řešitelnosti autoreferenčních rovnic tedy neplatí.

O rovnicích $\vdash \varphi \equiv \mathsf{Pr}_\pi(\overline{\neg\varphi})$ a $\vdash \varphi \equiv \mathsf{Pr}_\pi(\overline{\varphi})$ víme víc než to, že jejich řešení existují a jsou jednoznačně určena. Jejich řešení lze *explicitně vyjádřit* bez užití autoreference, neboť, jak jsme už připomněli, řešením první je sentence $\mathsf{Con}(\pi)$, řešením druhé je sentence $0 = 0$. Nyní směřujeme k tvrzení, že toto je pravda vždy, řešení každé gödelovské autoreferenční rovnice lze explicitně vyjádřit, tj. sestavit z „parametrů“ rovnice pomocí logických spojek a formule $\mathsf{Pr}_\pi(x)$. Nejprve dokážeme *větu o interpolaci*, která je zajímavá i samostatně.

Věta 5.3.28 *Nechť* $\langle\, \Gamma, \Pi \Rightarrow \Delta, \Lambda \,\rangle$ *je sekvent dokazatelný v logice GL. Pak existuje modální formule* D*, která je sestavena pouze z takových atomů, jež se současně vyskytují v obou sekventech* $\langle\, \Gamma \Rightarrow \Delta \,\rangle$ *a* $\langle\, \Pi \Rightarrow \Lambda \,\rangle$*, a přitom taková, že oba sekventy* $\langle\, \Gamma \Rightarrow \Delta, D \,\rangle$ *a* $\langle\, \Pi, D \Rightarrow \Lambda \,\rangle$ *jsou dokazatelné v logice GL.*

Důkaz Postupujme analogicky jako v důkazu lemmatu 3.3.15, indukcí dle hloubky bezřezového důkazu daného sekventu. Případy, kdy v posledním kroku je užito některé výrokové pravidlo, jsou úplně stejné. Případy, kdy je užito kvantifikátorové pravidlo, zde ovšem odpadají. Zabývejme se podrobněji případem, kdy v posledním kroku důkazu je užito modální pravidlo. Máme tedy důkaz, jehož finální sekvent $\mathcal{S}$ je z předposledního sekventu odvozen pomocí pravidla $\Box$-r. Antecedent sekventu $\mathcal{S}$ tudíž obsahuje pouze formule začínající modalitou, jeho sukcedent obsahuje právě jednu formuli, která také začíná modalitou, a přitom jak antecedent, tak sukcedent sekventu $\mathcal{S}$ je sjednocením dvou množin modálních formulí. Sekvent $\mathcal{S}$ má tedy tvar $\langle\, \Box\Gamma, \Box\Pi \Rightarrow \Delta, \Lambda \,\rangle$, kde množina $\Delta \cup \Lambda$ obsahuje jedinou modální formuli $\Box A$. Předposlední sekvent našeho důkazu musí být $\langle\, \Gamma, \Pi, \Box\Gamma, \Box\Pi \Rightarrow A \,\rangle$. Poslední krok našeho důkazu má tedy jeden z tvarů

$$\frac{\langle\, \overbrace{\Gamma, \Box\Gamma}, \overbrace{\Box A, \Pi, \Box\Pi} \Rightarrow \overbrace{\ A} \,\rangle}{\langle\, \Box\Gamma, \Box\Pi \Rightarrow \underbrace{\ \Box A} \,\rangle} \qquad \frac{\langle\, \overbrace{\Gamma, \Box\Gamma, \Box A}, \overbrace{\Pi, \Box\Pi} \Rightarrow \overbrace{\ A\ } \,\rangle}{\langle\, \Box\Gamma, \Box\Pi \Rightarrow \underbrace{\ \Box A\ } \,\rangle},$$

kde složené závorky dole naznačují, že pro dané sjednocení $\{\Box A\} = \Delta \cup \Lambda$ sukcedentu sekventu $\mathcal{S}$ může platit $\Box A \in \Lambda$ nebo $\Box A \in \Delta$, kdežto složené závorky nahoře naznačují, jak jsme se tudíž rozhodli rozložit antecedent a sukcedent předposledního sekventu na dvě množiny. Ponecháváme na čtenáři, aby si rozmyslel,

že případ $\Delta = \Lambda = \{\Box A\}$ nemusíme uvažovat. V prvním (levém) případě dává indukční předpoklad formuli D, která je sestavena pouze z atomů vyskytujících se současně v sekventech $\langle\, \Gamma, \Box\Gamma \;\Rightarrow\; \rangle$ a $\langle\, \Pi, \Box\Pi, \Box A \;\Rightarrow\; A \,\rangle$ a která přitom splňuje podmínku, že sekventy $\langle\, \Gamma, \Box\Gamma \;\Rightarrow\; D \,\rangle$ a $\langle\, \Pi, \Box\Pi, \Box A, D \;\Rightarrow\; A \,\rangle$ jsou oba dokazatelné v logice GL. Ze sekventu $\langle\, \Gamma, \Box\Gamma \;\Rightarrow\; D \,\rangle$ lze odvodit sekvent $\langle\, \Box\Gamma \;\Rightarrow\; \Box D \,\rangle$, ze sekventu $\langle\, \Pi, \Box\Pi, \Box A, D \;\Rightarrow\; A \,\rangle$ lze odvodit sekvent $\langle\, \Box\Pi, \Box D \;\Rightarrow\; \Box A \rangle$. Formule $\Box D$ je tedy hledanou formulí, neboť obsahuje pouze atomy vyskytující se současně v obou sekventech $\langle\, \Box\Gamma \;\Rightarrow\; \rangle$ a $\langle\, \Box\Pi \;\Rightarrow\; \Box A \,\rangle$.

V druhém případě dává indukční předpoklad formuli D splňující požadavek na výrokové atomy a takovou, že sekventy $\langle\, \Gamma, \Box\Gamma, \Box A \;\Rightarrow\; A, D \,\rangle$ a $\langle\, \Pi, \Box\Pi, D \;\Rightarrow\; \rangle$ jsou oba dokazatelné v logice GL. Ponecháváme na čtenáři, aby domyslel, že v tom případě sekventy $\langle\, \Box\Gamma \;\Rightarrow\; \Box A, \neg\Box\neg D \,\rangle$ a $\langle\, \Box\Pi, \neg\Box\neg D \;\Rightarrow\; \rangle$ jsou oba dokazatelné a že formule $\neg\Box\neg D$ splňuje požadavek na výrokové atomy. V tomto případě je tedy formule $\neg\Box\neg D$ hledanou formulí. QED

Věta 5.3.29 *Nechť $A(p)$ je modální formule, v níž se atom p vyskytuje jen v modálním kontextu. Pak existuje formule D sestavená pouze z atomů formule $A(p)$ různých od p a taková, že ekvivalence $D \equiv A(D)$ je dokazatelná v logice GL.*

Důkaz Zvolme atom q nevyskytující se ve formuli $A(p)$. Pak formule $A(p)$ a atomy p a q jsou jako v tvrzeních 5.3.26(b) a 5.3.27 a můžeme pokračovat v odvozování v gentzenovském kalkulu, které v důkazu věty 5.3.27 skončilo řádkem (4):

5: $\langle\, A(p) \equiv A(q), A(p) \;\Rightarrow\; A(q) \,\rangle$.

Tento sekvent je snadno dokazatelný, neboť je tautologický.

6: $\langle\, \Box(p \equiv A(p)), \Box(q \equiv A(q)) \;\Rightarrow\; A(p) \equiv A(q) \,\rangle$; 2, 4, Cut

7: $\langle\, \Box(p \equiv A(p)), \Box(q \equiv A(q)), A(p) \;\Rightarrow\; A(q) \,\rangle$; 5, 6, Cut.

První a třetí formule antecedentu sekventu (7) neobsahuje atom q, druhá formule $\Box(q \equiv A(q))$ a formule $A(q)$ v sukcedentu neobsahují atom p. Věta 5.3.28 říká, že existuje modální formule D, která neobsahuje atomy p ani q, obsahuje pouze atomy vyskytující se ve formuli A a přitom následující dva sekventy

8: $\langle\, \Box(p \equiv A(p)), A(p) \;\Rightarrow\; D \,\rangle$

9: $\langle\, \Box(q \equiv A(q)), D \;\Rightarrow\; A(q) \,\rangle$

jsou dokazatelné v logice GL. Vezměme důkaz sekventu (8) a substituujme v něm formuli D za všechny výskyty atomu p. Dále vezměme důkaz sekventu (9) a substituujme v něm formuli D za všechny výskyty atomu q. Tím získáme důkazy sekventů

10: $\langle\, \Box(D \equiv A(D)), A(D) \;\Rightarrow\; D \,\rangle$

11: $\langle\, \Box(D \equiv A(D)), D \;\Rightarrow\; A(D) \,\rangle$.

Formule D se totiž substituce nedotkne, neboť ta atomy p a q neobsahuje. Takže:

12: $\langle\, \Box(D \equiv A(D)) \;\Rightarrow\; D \equiv A(D) \,\rangle$; 10, 11

13: $\langle\, \Rightarrow\; \Box(D \equiv A(D)) \,\rangle$; $\Box$-r

14: $\langle\, \Rightarrow\; D \equiv A(D) \,\rangle$; 12, 13, Cut.

QED

Nejen v Peanově aritmetice, nýbrž i v logice dokazatelnosti můžeme uvažovat autoreferenční rovnice tvaru $\vdash p \equiv A(p)$ s atomem p vyskytujícím se ve formuli A pouze v modálním kontextu. Věta 5.3.29 zaručuje řešitelnost takových rovnic. Na aritmetické straně to znamená, že o gödelovských autoreferenčních rovnicích můžeme říci více než to, že mají jednoznačně určené řešení: jejich řešení lze *vypočítat*. Mějme například rovnici $\vdash \varphi \equiv \mathsf{Pr}_\pi(\overline{\varphi}) \to \lambda$, která se vyskytla v důkazu Löbovy věty, a počítejme její řešení, tj. hledejme modální formuli D takovou, že substituujeme-li ji za atom p do formule $p \equiv \Box p \to r$, dostaneme formuli dokazatelnou v logice GL. Pracnou analýzou důkazu věty 5.3.29 (a věty 5.3.28), nebo několika pokusy a s trochou štěstí lze zjistit, že hledaná formule je formule $\Box r \to r$. To znamená, že explicitním řešením rovnice $\vdash \varphi \equiv \mathsf{Pr}_\pi(\overline{\varphi}) \to \lambda$ je aritmetická sentence $\mathsf{Pr}_\pi(\overline{\lambda}) \to \lambda$.

Z našich příkladů důkazů v logice GL víme, že existuje modální formule $A(p)$, ve které se atom p vyskytuje pouze v modálním kontextu, a přitom taková, že formule $\Box(p \equiv A(p)) \to (\neg\Box\bot \to \neg\Box p)$ je dokazatelná v logice GL. Položme si otázku, zda existuje modální formule $A(p)$, v níž se atom p vyskytuje opět pouze v modálním kontextu a která splňuje silnější podmínku

$$\mathrm{GL} \vdash \Box(p \equiv A(p)) \to (\neg\Box\bot \to \neg\Box p \,\&\, \neg\Box\neg p). \qquad (*)$$

Pokud ano, mohli bychom užít větu o korektnosti logiky GL vůči aritmetické sémantice spolu s větou o autoreferenci a dokázat existenci aritmetické sentence φ, pro kterou platí

$$\mathsf{PA} \vdash \mathsf{Con}(\pi) \to \neg\mathsf{Pr}_\pi(\overline{\varphi}) \,\&\, \neg\mathsf{Pr}_\pi(\overline{\neg\varphi}). \qquad (**)$$

Měli bychom tedy alternativní (modální) důkaz klasické verze Rosserovy věty 4.5.6. Rozmysleme si, že takto větu 4.5.6 dokazovat nelze. Kdyby totiž existovala modální formule A splňující podmínku $(*)$, díky větě 5.3.29 by existovala i modální formule D taková, že v logice GL lze dokázat formuli $\neg\Box\bot \to \neg\Box D \,\&\, \neg\Box\neg D$. Taková modální formule D ale neexistuje, viz cvičení 20. Avšak ve cvičeních 21 a 22 je ukázáno, že Rosserovu větu lze přesto dokázat jistými úvahami o logice dokazatelnosti, totiž využitím věty 5.3.30 o úplnosti logik GL a GL^ω vůči aritmetické sémantice.

5.3.5 Aritmetická úplnost

Úplnost logik GL a GL^ω vůči jejich aritmetickým interpretacím dokázal R. Solovay v článku [86]. Hlavní metoda použitá v důkazu je autoreference v množném čísle, tj. užití věty 4.5.11: v důkazu věty 5.3.30 vystupují sentence $\lambda_1, \ldots, \lambda_n$, a každá z nich je „definována“ tím, co tvrdí o sobě a o ostatních λ_i. Připadá nám pozoruhodné, že v důkazu úplnosti modálních logik, které mají vztah k autoreferenci, se uplatňuje

opět autoreferenční konstrukce, a to jedna z nejzajímavějších vůbec. A je asi docela případné zakončit náš text, ve kterém autoreference hrála dost podstatnou roli, právě tímto důkazem.

Věta 5.3.30 (Solovay, 1975) *(a) Každá* PA*-platná modální formule je dokazatelná v logice GL.*
(b) Každá **N***-platná modální formule je dokazatelná v logice* GL^ω*.*

Důkaz Zpočátku uvažujme o obou tvrzeních souběžně. Předpokládejme, že A je modální formule, která není dokazatelná v logice GL či v logice GL^ω. Chceme dokázat, že formule A není PA-platná resp. **N**-platná, tj. že existuje aritmetický překlad $\sharp$ či $\flat$ takový, že $\mathsf{PA} \nvdash A^\sharp$ resp. $\mathbf{N} \not\models A^\flat$. Máme větu o úplnosti vůči kripkovské sémantice: formule A má nějaký konečný kripkovský protipříklad K. Jako obvykle můžeme předpokládat, že ten vrchol modelu K, ve kterém formule A není splněna, je v modelu K kořenem. Dále předpokládejme, že celkový počet vrcholů v modelu K je n, že jsou označeny $1, \ldots, n$ a že kořen má označení 1. Tedy

$$K = \langle W, R, \Vdash\!\!- \rangle, \qquad W = \{1, \ldots, n\}, \qquad 1 \not\Vdash\!\!- A.$$

V (b) navíc platí, že kořen 1 je A-korektní. Model K a formuli A pokládejme v celém důkazu za pevně dané. O modelu K můžeme mluvit i uvnitř Peanovy aritmetiky. Například R je konečná množina dvojic, uvnitř PA je popsána konečně mnoho podmínkami tvaru $\overline{i}\ R\ \overline{j}$ a $\neg(\overline{i}\ R\ \overline{j})$. Také pravdivostní relace $\Vdash\!\!-$ je popsána jen konečně mnoha podmínkami (alespoň pokud se týká atomů vyskytujících se ve formuli A). Označme $S(i)$ množinu $\{\ j\ ;\ i\ R\ j\ \}$. Množina $S(i)$ je množina všech vrcholů rámce $\langle \{1, \ldots, n\}, R\rangle$ modelu K dosažitelných z vrcholu i. Navíc položme $S(0) = \{1, \ldots, n\}$.

Naším plánem je na základě rámce $\langle \{1, \ldots, n\}, R\rangle$ sestrojit sentence $\lambda_1, \ldots, \lambda_n$ (jejich počet je rovný počtu vrcholů rámce) a potom z nich a z relace $\Vdash\!\!-$ sestrojit aritmetický překlad $\sharp$ resp. $\flat$. Jak už jsme řekli, sentence $\lambda_1, \ldots, \lambda_n$ si opatříme na základě autoreference v množném čísle. To znamená, že každou sentenci λ_i budeme definovat jako výrok o rámci $\langle W, R\rangle$ a o číslech $\overline{\lambda_1}, \ldots, \overline{\lambda_n}$. Mysleme si tedy, že máme v ruce numerály $\overline{\lambda_1}, \ldots, \overline{\lambda_n}$ a v PA s jejich pomocí definujme funkci g:

$$g(0) = 0,$$
$$g(x+1) = \begin{cases} \overline{j} & \text{když } \mathsf{Proof}_\pi(\overline{\neg\lambda_j}, x) \text{ a přitom } g(x)\ R\ \overline{j} \text{ nebo } g(x) = 0 \\ g(x) & \text{jinak.} \end{cases}$$

Zdůrazněme ještě jednou, že toto je definice funkce *uvnitř* Peanovy aritmetiky. Na metamatematické úrovni jsme napsali Σ-formuli s volnými proměnnými x a y, kterou čteme číslo y je funkční hodnota funkce g v bodě x. Uvažujme v PA o průběhu funkce g. Možné hodnoty funkce g jsou buď číslo 0, nebo prvky $1, \ldots, n$ modelu K. Funkce g začíná v nule. V každém okamžiku buď stojí na místě, nebo skočí do některého vrcholu kripkovského rámce. Po prvním skoku jsou možné i další skoky, ale vždy jen do vrcholů dosažitelných z dosavadní hodnoty. Z toho je (Peanově

aritmetice) jasné, že skoků nemůže být nekonečně mnoho, a tedy že funkce g po jisté době nabude definitivní hodnoty:

1: $\vdash \exists x \forall y \geq x (g(y) = \overline{0}) \vee \ldots \vee \exists x \forall y \geq x (g(y) = \overline{n})$.

Domluvme se opět, že vypouštíme „PA“ před znakem dokazatelnosti. O definitivní hodnotě můžeme mluvit jako o *limitě*. Podmínku (1) tedy můžeme přepsat na

2: $\vdash \lim g = \overline{0} \vee \ldots \vee \lim g = \overline{n}$.

Pokud se funkce g v nějakém okamžiku octne ve vrcholu $\overline{i}$, pak tam buď zůstane, nebo skončí v některém vrcholu z množiny $S(i)$:

3: $\vdash \exists x (g(x) = \overline{i}) \rightarrow \lim g = \overline{i} \vee \bigvee_{j \in S(i)} \lim g = \overline{j}$.

Tím jsme získali postačující informaci o tom, *kam* a *jak* funkce g skáče. Ptejme se ještě, *kdy* či *proč* skáče. Skok do vrcholu $\overline{i}$ mohl nastat jen v okamžiku nalezení důkazu sentence $\overline{\neg\lambda_i}$:

4: Je-li $i \neq 0$, pak $\vdash \exists x (g(x) = \overline{i}) \rightarrow \mathsf{Pr}_\pi(\overline{\neg\lambda_i})$.

Je-li funkce g v nějakém okamžiku x ve vrcholu $\overline{i}$ a už tam zůstane, znamená to, že za číslem x nebyl nalezen důkaz žádné sentence $\overline{\neg\lambda_j}$ pro $j \in S(i)$. To ale znamená, že každá taková sentence $\overline{\neg\lambda_j}$ nemá *žádný* důkaz, protože každá dokazatelná sentence jistě má neomezeně velké důkazy. Takže

5: $\vdash \lim g = \overline{i} \rightarrow \bigwedge_{j \in S(i)} \neg\mathsf{Pr}_\pi(\overline{\neg\lambda_j})$.

Teď jsme schopni definovat sentence $\lambda_1, \ldots, \lambda_n$:

$$\vdash \lambda_i \equiv \lim g = \overline{i}, \qquad 1 \leq i \leq n.$$

K tomu přidejme ještě sentenci λ_0:

$$\vdash \lambda_0 \equiv \lim g = \overline{0}.$$

Sentence λ_0 je na rozdíl od sentencí λ_i pro $1 \leq i \leq n$ definována přímo, bez užití autoreference. V definicích všech sentencí $\lambda_0, \ldots, \lambda_n$ vystupují numerály $\overline{\lambda_1}, \ldots, \overline{\lambda_n}$, nikoliv numerál $\overline{\lambda_0}$. Sentence λ_i mají následující vlastnosti:

6: $\vdash \bigvee_{i=0}^{n} \lambda_i$; 2

7: $\vdash \lambda_i \rightarrow \bigwedge_{j \in S(i)} \neg\mathsf{Pr}_\pi(\overline{\neg\lambda_j})$; 5

8: Je-li $i \neq j$, pak $\vdash \lambda_i \rightarrow \neg\lambda_j$,

neboť funkce g nemůže mít dvě různé limity. Dále platí

9: Je-li $i \neq 0$, pak $\vdash \lambda_i \rightarrow \mathsf{Pr}_\pi(\overline{\neg\lambda_i})$; 4.

O průběhu funkce g uvažujeme vlastně na třech úrovních: ve skutečnosti, uvnitř PA, a roli hrají také některé fakty, o kterých je dokazatelné, že jsou dokazatelné. Uvnitř PA zatím můžeme říci, že funkce g skáče modelem K ve směru relace dosažitelnosti R, ale dost neochotně. Skok do vrcholu $\overline{i}$ může nastat pouze v případě, je-li po ruce důkaz, že $\overline{i}$ není definitivní hodnota.

Je-li i listem v modelu K, pak sentence λ_i je ekvivalentní s $\exists x(g(x) = \overline{i})$, což je Σ-sentence. Není-li i listem, platí alespoň jedna implikace:

$$\vdash \lambda_i \to \exists x(g(x) = \overline{i}).$$

Z toho můžeme usoudit

10: $\vdash \lambda_i \to \mathsf{Pr}_\pi(\overline{\exists x(g(x) = \overline{i})})$; Formalizovaná Σ-úplnost

$\vdash \exists x(g(x) = \overline{i}) \to \lambda_i \vee \bigvee_{j \in S(i)} \lambda_j$; 3

11: $\vdash \mathsf{Pr}_\pi(\overline{\exists x(g(x) = \overline{i}) \to \lambda_i \vee \bigvee_{j \in S(i)} \lambda_j})$; D1

12: $\vdash \lambda_i \to \mathsf{Pr}_\pi(\overline{\lambda_i \vee \bigvee_{j \in S(i)} \lambda_j})$; 11, D2, 10

13: Je-li $i \neq 0$, pak $\vdash \lambda_i \to \mathsf{Pr}_\pi(\overline{\bigvee_{j \in S(i)} \lambda_j})$; 12, 9.

Podmínka (13) říká, že pokud funkce g provede vůbec nějaký skok a skončí ve vrcholu $\overline{i}$, pak je dokazatelné, že neskončí v $\overline{i}$, nýbrž v některém vrcholu $\overline{j}$ dosažitelném z $\overline{i}$. Podmínka (7) říká, že žádné takové $\overline{j}$ není vyloučeno, a to ani v případě, kdy funkce g žádný skok neprovede, tj. v případě, kdy $i = 0$. To jsou fakty známé o průběhu funkce g uvnitř Peanovy aritmetiky. Zbývá zjistit, co se stane ve skutečnosti.

14: $\mathbf{N} \models \mathsf{Pr}_\pi(\overline{\neg\lambda_i}) \to \neg\lambda_i$; Schéma reflexe

Je-li $i \neq 0$, pak $\mathbf{N} \models \lambda_i \to \neg\lambda_i$. ; 9, 14

15: Je-li $i \neq 0$, pak $\mathbf{N} \models \neg\lambda_i$.

16: $\mathbf{N} \models \lambda_0$; 15, 6

$\mathbf{N} \models \bigwedge_{i=1}^{n} \neg\mathsf{Pr}_\pi(\overline{\neg\lambda_i})$; 7 (pro $i = 0$), 16

17: Každá λ_i, pro $1 \leq i \leq n$, je s PA bezesporná.

Podmínky (16) a (17) říkají, že v Peanově aritmetice nelze dokázat žádnou sentenci $\neg\lambda_i$ pro $0 \leq i \leq n$. Z toho a z (8) plyne, že nelze dokázat ani žádnou sentenci λ_i. Všechny sentence $\lambda_0, \ldots, \lambda_n$ jsou tedy na PA nezávislé, v $\mathbf{N}$ platí λ_0. To je zároveň odpověď na otázku, co se stane ve skutečnosti: nikdy se nestane nic, funkce g neopustí nulu.

Dosud zjištěné vlastnosti funkce g a sentencí λ_i se použijí v důkazech obou tvrzení (a) a (b).

Víme, že aritmetický překlad je zadán svými hodnotami na výrokových atomech. V (a) použijeme překlad $\sharp$, který definujeme takto: pro každý atom p zjistíme, ve kterých vrcholech modelu K je splněn, a atom p pak přeložíme na disjunkci příslušných sentencí λ_i:

$$p^\sharp = \bigvee\{\, \lambda_i \,;\, 1 \leq i \leq n \;\&\; i \Vdash p \,\}.$$

Překlad $\sharp$ má vlastnosti vyjádřené v následujícím tvrzení.

Sublemma A *Nechť $1 \leq i \leq n$ a nechť B je modální formule. Když $i \Vdash B$, pak $\vdash \lambda_i \to B^\sharp$. Když naopak $i \nVdash B$, pak $\vdash \lambda_i \to \neg B^\sharp$.*

Toto sublemma dokážeme indukcí podle složitosti modální formule B. Je-li B atom a $i \Vdash B$, pak $B^\sharp$ je disjunkce sentencí, mezi nimiž je λ_i, a tedy opravdu $\vdash \lambda_i \to B^\sharp$. Když $i \nVdash B$, pak z (8) plyne $\vdash \lambda_i \to \neg B^\sharp$. Případ, kdy formule B je sestavena z jednodušších formulí pomocí některé logické spojky, je přímočarý, a jeho ověření přenecháváme čtenáři. Nechť B začíná modalitou, tj. má tvar $\Box D$. Předpokládejme $i \Vdash \Box D$. Pak

$$\begin{aligned}
&\forall j(i\ R\ j \ \Rightarrow\ j \Vdash D) \\
&\forall j(i\ R\ j \ \Rightarrow\ \vdash \lambda_j \to D^\sharp) && \text{; Indukční předpoklad} \\
&\vdash \textstyle\bigvee_{j \in S(i)} \lambda_j \to D^\sharp \\
&\vdash \mathsf{Pr}_\pi(\overline{\textstyle\bigvee_{j \in S(i)} \lambda_j}) \to \mathsf{Pr}_\pi(\overline{D^\sharp}) && \text{; D1, D2} \\
&\vdash \lambda_i \to \mathsf{Pr}_\pi(\overline{D^\sharp}) && \text{; 13.}
\end{aligned}$$

Předpokládejme, že naopak $i \nVdash \Box D$. V tom případě existuje j takové, že $i\ R\ j$ a $j \nVdash D$. Pak

$$\begin{aligned}
&\vdash \lambda_j \to \neg D^\sharp && \text{; Indukční předpoklad} \\
&\vdash \mathsf{Pr}_\pi(\overline{\lambda_j \to \neg D^\sharp}) && \text{; D1} \\
&\vdash \lambda_i \to \neg \mathsf{Pr}_\pi(\overline{D^\sharp}) && \text{; 7.}
\end{aligned}$$

V obou případech jsme dokázali, co bylo třeba, neboť $(\Box D)^\sharp$ je sentence $\mathsf{Pr}_\pi(\overline{D^\sharp})$. Tím jsme dokončili důkaz sublemmatu A.

Z dokázaného sublemmatu okamžitě vyplývá platnost tvrzení (a): protože $1 \nVdash A$, máme $\vdash \lambda_1 \to \neg A^\sharp$. Ze (17) plyne $\nvdash A^\sharp$.

V důkazu tvrzení (b) máme navíc předpoklad, že vrchol 1 modelu K je A-korektní. Jedna z hodnot funkce g je nula, kterou jsme dosud považovali za počáteční hodnotu nemající nic společného s modelem K. Nyní prohlašme číslo 0 za nový kořen a každému atomu vyskytujícímu se ve formuli A v něm přidělme tutéž pravdivostní hodnotu, kterou má ve vrcholu 1. To znamená, že jsme model K přepracovali na model K' tak, jak je znázorněno na obrázku 5.3.3. Lemma 5.3.20 říká, že nový kořen 0 je A-korektním vrcholem modelu K' a že každá podformule formule A má ve vrcholech 0 a 1 tutéž pravdivostní hodnotu. Aritmetický překlad $\flat$ se nyní definuje takto:

$$p^\flat = \bigvee\{\, \lambda_i \,;\, 0 \leq i \leq n \ \&\ i \Vdash p \,\}.$$

Překlad $\flat$ se liší od překladu $\sharp$ tím, že v disjunkci se někdy vyskytne i sentence λ_0, a to přesně tehdy, když tam je i sentence λ_1. Pro *podformule* původní formule A platí skoro stejné pomocné tvrzení jako v důkazu tvrzení (a).

Sublemma B *Nechť $0 \leq i \leq n$ a nechť B je podformule formule A. Když $i \Vdash B$, pak $\vdash \lambda_i \to B^\flat$. Když naopak $i \nVdash B$, pak $\vdash \lambda_i \to \neg B^\flat$.*

V důkazu tohoto sublemmatu opět postupujeme indukcí podle složitosti formule B. Stačí zabývat se pouze případem, kdy $i = 0$ a $i \Vdash \Box D$. Všechny ostatní případy jsou stejné jako v důkazu sublemmatu A. Nechť tedy $0 \Vdash \Box D$. Pak formule D je splněna ve všech vrcholech $1, \ldots, n$ původního rámce, a díky A-korektnosti vrcholu 0 je splněna i ve vrcholu 0. Tedy

$$\begin{aligned} &\forall j(0 \leq j \leq n \Rightarrow \vdash \lambda_j \to D^\flat) && \text{; Indukční předpoklad} \\ &\vdash \textstyle\bigvee_{j=0}^{n} \lambda_j \to D^\flat \\ &\vdash D^\flat && \text{; 6.} \end{aligned}$$

Z posledního řádku plyne $\vdash \mathsf{Pr}_\pi(\overline{D^\flat})$, a tedy i $\vdash \lambda_0 \to \mathsf{Pr}_\pi(\overline{D^\flat})$.

Ze sublemmatu B opět téměř bezprostředně vyplývá platnost tvrzení (b): z lemmatu 5.3.20 plyne $0 \Vdash\!\!\!/\ A$, neboť $1 \Vdash\!\!\!/\ A$, ze sublemmatu B plyne $\vdash \lambda_0 \to \neg A^\flat$ a dále z řádku (16) plyne $\mathbf{N} \not\models A^\flat$. QED

Výsledky týkající se logiky dokazatelnosti, které jsme ukázali v tomto oddílu, zdaleka nevyčerpávají problematiku aplikací modální logiky v metamatematice. Existují další modální logiky, ve kterých se kromě modality nutnosti připouštějí dodatečné „modality“, vhodné pro popis různých autoreferenčních konstrukcí (uvozovky jsme užili proto, že tyto dodatečné modality nemají žádný vztah k modalitám v přirozené řeči). Například v článku [29] se zkoumají modální logiky, jejichž „jazyk“ kromě logických spojek a symbolu $\Box$ obsahuje ještě symboly $\preceq$ a $\prec$. Každý z těchto symbolů je binární operátor, který je povoleno aplikovat pouze na formule začínající symbolem $\Box$; podmínky v definici aritmetického překladu týkající se symbolů $\preceq$ a $\prec$ pak jsou

$$\begin{aligned} (\Box A \preceq \Box B)^* &= \exists x(\mathsf{Pr}_\pi(\overline{A^*}) \mathbin{\&} \forall v{<}x\, \neg\mathsf{Pr}_\pi(\overline{B^*})), \\ (\Box A \prec \Box B)^* &= \exists x(\mathsf{Pr}_\pi(\overline{A^*}) \mathbin{\&} \forall v{\leq}x\, \neg\mathsf{Pr}_\pi(\overline{B^*})). \end{aligned}$$

Symbolům $\preceq$ a $\prec$ se říká symboly pro *porovnávání svědků*, logiky obsahující tyto symboly jsou vhodné k popisu rosserovských konstrukcí, jako byla ta z věty 4.5.6. Jiná užitečná možnost, jak rozšířit jazyk modální logiky, je přidat binární symbol $\rhd$ pro interpretovatelnost (ve smyslu z oddílu 3.6). Tento symbol je aplikovatelný na všechny dvojice modálních formulí; jemu příslušná podmínka v definici aritmetického překladu pak je $(A \rhd B)^* = \mathsf{Intp}(\overline{A^*}, \overline{B^*})$, kde $\mathsf{Intp}(x, y)$ je aritmetická formule existuje interpretace teorie $(\pi + y)$ v teorii $(\pi + x)$. Modální logice se symbolem $\rhd$ pro interpretovatelnost axiomatických teorií se říká *logika interpretovatelnosti*. Z (formalizace v PA) tvrzení 4.5.8(b) například plyne, že modální formule $\neg\Box\bot \to \neg(\neg\bot \rhd \neg\Box\bot)$ je tautologie v různých variantách logiky interpretovatelnosti. Zájemcům o tuto problematiku doporučujeme přehledový článek A. Vissera [96]. Zájemcům o aplikace modálních logik v metamatematice různých teorií (jiných než Peanova aritmetika) doporučujeme kromě článku [96] také článek [6] a práci [43].

Cvičení

1. Dokažte Löbovu větu přímo, bez užití autoreference.

   Návod. Aplikujte Druhou Gödelovu větu na teorii $(T + \neg\varphi)$. Uvažte, že sentence $\neg\mathsf{Con}(\tau + \overline{\neg\varphi})$, která vyjadřuje její spornost, je ekvivalentní se sentencí $\mathsf{Pr}_\tau(\overline{\varphi})$.

2. Dokažte, že důkaz Löbovy věty by také šlo založit na jiné sentenci λ, která by splňovala podmínku $\vdash \lambda \equiv \mathsf{Pr}_\tau(\overline{\lambda \to \varphi})$.

3. Dokažte, že formule $\Box(p \vee q) \to \Box p \vee \Box q$ a $(\Box p \to \Box q) \to \Box(p \to q)$ nejsou **N**-platné.

4. Dokažte v logice K4 formule $\Box(A \,\&\, B) \to \Box A \,\&\, \Box B$, $\Box A \vee \Box B \to \Box(A \vee B)$ a $\neg\Box\bot \to (\Box A \to \neg\Box\neg A)$.

5. Dokažte, že pro každou z logik GL a K4 platí omezená verze věty o dedukci: když $\Box B \vdash A$, pak $\vdash \Box B \to A$.

6. Dokažte aritmetickou korektnost Löbova axiomu přímo, tj. nikoliv oklikou přes Löbovo pravidlo.

   Návod. Podobně jako důkaz Druhé Gödelovy věty byl vlastně formalizací důkazu (klasické verze) První Gödelovy věty, lze k důkazu Löbovy věty přidat druhou část, která je formalizací dosavadní části.

7. Dokažte pomocí vzájemné simulovatelnosti kalkulů, že gentzenovský kalkulus pro logiku K4 lze založit na pravidle $\langle\, \Gamma, \Box\Gamma \Rightarrow A \,\rangle \,/\, \langle\, \Box\Gamma \Rightarrow \Box A \,\rangle$.

8. Dokažte, že logika vzniklá přidáním schématu $\Box(\Box A \equiv A) \to \Box A$ k logice K4 je ekvivalentní s logikou GL.

   Návod. Z předpokladu $\Box(\Box A \to A)$ a z daného schématu použitého na formuli $\Box A$ dokažte v logice K4 formuli $\Box A$.

9. Dokažte, že axiom L3 je v logice GL redundantní.

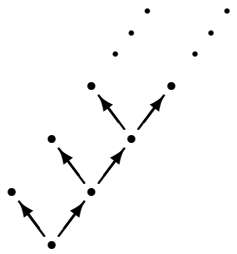
   Návod. Užijte axiom L4 na formuli $A \,\&\, \Box A$.

10. Dokažte, že v modální logice s axiomy L1 a L2 a pravidly MP, Nec a LR nelze dokázat axiom L3, a tedy ani axiom L4.

    Návod. Dokažte korektnost uvedené logiky vůči třídě všech rámců $\langle W, R\rangle$ takových, že relace R^{-1} je fundovaná. Pak navrhněte model $\langle W, R, \|\!-\rangle$, ve kterém relace R^{-1} je fundovaná, ale některá instance axiomu L3 v něm neplatí. Relace R ovšem nemůže být tranzitivní.

11. Dokažte, že přidáním axiomu $\neg\Box\bot \to \neg\Box\neg\Box\bot$ k logice K4 nevznikne logika ekvivalentní s logikou GL.

    Návod. Uvažujte takovýto nekonečný rámec:



12. Dokažte, že v logice K4 nelze dokázat formuli z předchozího cvičení.

13. Dokažte, že každá konečná část Δ množiny
$$\Gamma = \{\Diamond p_0, \Box(p_0 \to \Diamond p_1), \Box(p_1 \to \Diamond p_2), \dots\}$$
je splnitelná v (dokonce Δ-korektním) kořenu některého (dokonce konečného) kripkovského modelu pro logiku GL, ale celá množina Γ najednou splnitelná není.

14. Je-li jakákoliv disjunkce $\Box A_1 \vee \ldots \vee \Box A_n$ dokazatelná v logice GL, pak i některá formule A_i je dokazatelná v logice GL. Dokažte s pomocí kripkovské sémantiky logiky GL.

15. Podobně dokažte, že $\mathrm{GL} \vdash \boxdot A \to B$, právě když $\mathrm{GL} \vdash \Box A \to \Box B$.

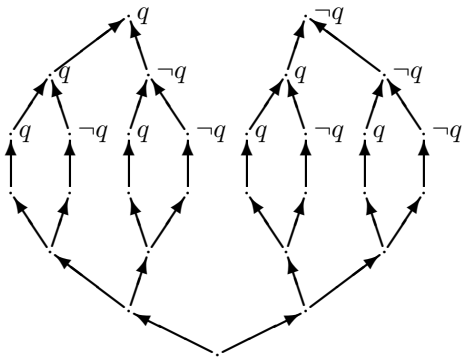
16. Dokažte tvrzení z předchozích dvou cvičení důkazově teoreticky, tj. úvahou o bezřezových důkazech.

17. Dokažte, že logika vzniklá přidáním pravidla DiR k logice K4 je uzavřená na Löbovo pravidlo. Zdůvodněte, že všechna tři rozšíření logiky K4, totiž pomocí Löbova axiomu, Löbova pravidla, nebo pravidla DiR, jsou spolu ekvivalentní.

    Návod. Napište modální verzi důkazu Löbovy věty.

18. Pomocí „ruční simulace“ procedury z důkazy věty 5.3.22 zjistěte, zda sekvent $\langle\, \Box(\Box p \to q) \vee \Box\neg(p \vee q), \neg\Box q \;\Rightarrow\; \Box(\Box\bot \to \neg p), p \,\rangle$ platí v každém kripkovském modelu pro logiku dokazatelnosti.

19. Nechť $\Box^n A$ a $\Diamond^n A$ označuje formuli vzniklou z formule A pomocí n-násobné aplikace modality $\Box$ resp. $\Diamond$. Nechť ∇_m je formule $\Diamond^m\top \& \Box^{m+1}\bot$. Zdůvodněte, že formule ∇_m platí ve vrcholu a kripkovského modelu pro logiku dokazatelnosti právě tehdy, když hloubka vrcholu a (tj. délka nejdelší cesty začínající v a) je m. Pro $0 \le j \le m$ nechť formule $E_{m,j}$ jsou definovány následující rekurzí:
$$\begin{aligned} E_{m,0} &= \nabla_m \\ E_{m,j+1} &= \Diamond(\nabla_{m+j} \,\&\, \Box(\nabla_{m-1-j} \to q)) \,\&\, \Diamond(\nabla_{m+j} \,\&\, \Box(\nabla_{m-1-j} \to \neg q)) \,\& \\ &\quad \& \,\Box(\nabla_{m+j} \to E_{m,j}). \end{aligned}$$
    Zdůvodněte, že model, který následuje, je nejmenší protipříklad na formuli $E_{3,3}$. Dále zdůvodněte, že počet prvků minimálního protipříkladu na formuli $E_{m,m}$ roste exponenciálně s m.



20. Zdůvodněte, že je-li A libovolná aritmetická formule, v níž se atom p vyskytuje pouze v modálním kontextu, pak formule $\Box(p \equiv A(p)) \to (\neg\Box\bot \to \neg\Box p \,\&\, \neg\Box\neg p)$ není dokazatelná v logice GL.

    Návod. Kdyby ano, vzhledem k větě 5.3.29 by existovala i modální formule D neobsahující atom p taková, že formule $\neg\Box\bot \to \neg\Box D \,\&\, \neg\Box\neg D$ je dokazatelná v logice GL. Úvahou o dvouprvkovém modelu (s kořenem a listem) zdůvodněte, že to není pravda.

21. Z Druhé Gödelovy věty pro teorii $(\mathsf{PA} + \mathsf{Con}(\pi))$ plyne, že sentence $\mathsf{Con}(\pi)$ splňuje jen první tři z následujících podmínek pro sentenci φ:

    - $\mathsf{PA} \nvdash \varphi$
    - $\mathsf{PA} \nvdash \neg\varphi$
    - $\mathsf{PA} \vdash \mathsf{Con}(\pi) \to \neg\mathsf{Pr}_\pi(\overline{\varphi})$
    - $\mathsf{PA} \vdash \mathsf{Con}(\pi) \to \neg\mathsf{Pr}_\pi(\overline{\neg\varphi})$.

    Dokažte, že existuje sentence φ, která splňuje všechny čtyři.

    Návod. Zdůvodněte, že $\Box(\neg\Box\bot \to \neg\Box p) \,\&\, \Box(\neg\Box\bot \to \neg\Box\neg p) \to \Box p \vee \Box\neg p$ je formule nedokazatelná v logice GL^ω. Věta o aritmetické úplnosti logiky GL^ω dává aritmetický protipříklad $*$ na tuto formuli. Uvažujte sentenci p^*.

22. Analyzujte důkaz věty o aritmetické úplnosti logik GL a GL^ω a zdůvodněte, že

    (a) Je-li i listem v rámci $\langle W, R, \Vdash\!\!-\rangle$, pak sentence λ_i je PA-ekvivalentní s jistou Σ-sentencí.

    (b) splňuje-li atom p ve $\langle W, R, \Vdash\!\!-\rangle$ podmínku $\forall a \forall b(a \leq b \;\&\; a \Vdash\!\!- p \;\Rightarrow\; b \Vdash\!\!- p)$, pak sentence $p^\sharp$ (i sentence $p^\flat$) je PA-ekvivalentní s jistou Σ-sentencí.

    Zdůvodněte, že existuje dokonce Σ-sentence φ, která splňuje podmínky z předchozího cvičení.

23. Zdůvodněte úvahou podobnou jako v předchozích cvičeních, že existují Σ-sentence θ a λ takové, že v PA nelze dokázat žádnou z implikací $\theta \to \lambda$, $\theta \to \neg\lambda$, $\neg\theta \to \lambda$, $\neg\theta \to \neg\lambda$.

Literatura

[1] A. V. Aho, J. E. Hopcroft a J. Ullman. *The Design and Analysis of Computer Algorithms.* Addison-Wesley, 1974.

[2] B. Balcar a P. Štěpánek. *Teorie množin.* Academia, Praha, 2001.

[3] J. L. Balcázar, J. Díaz a J. Gabarró. *Structural Complexity I.* Springer, 1988.

[4] J. Barwise, Ed. *Handbook of Mathematical Logic.* North-Holland, 1977.

[5] J. Barwise. An introduction to first-order logic. V *Handbook of Mathematical Logic* [4], kap. A.1, str. 5–46.

[6] A. Berarducci a R. Verbrugge. On the provability logic of bounded arithmetic. *Annals Pure Appl. Logic 61*, 1–2 (1993), 75–93.

[7] G. Boolos a G. Sambin. Provability: the emergence of a mathematical modality. *Studia Logica L*, 1 (1991), 1–23.

[8] G. Boolos. *The Logic of Provability.* Cambridge University Press, 1993.

[9] P. Burdová. Některé sémantické metody v intuicionistické logice. Diplomová práce, Filozofická fakulta Univerzity Karlovy, katedra logiky, 1998.

[10] S. R. Buss. *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.

[11] S. R. Buss. Weak Formal Systems and Connections to Computational Complexity. Lecture Notes for a Topics Course, University of California, Berkeley, leden–květen 1988.

[12] P. Cohen. Decision procedures for real and p-adic fields. *Comm. Pure Appl. Math. xxii* (1969), 131–151.

[13] S. Cook. The complexity of theorem proving procedures. V *Proc. 3rd ACM Symp. of Theory of Computing* (1971), str. 151–158.

[14] D. van Dalen. Intuitionistic logic. V Gabbay and Guenthner [23], kap. III.4, str. 225–340.

[15] O. Demuth, R. Kryl a A. Kučera. Teorie algoritmů. Skriptum, Matematicko-fyzikální fakulta UK, 1989.

[16] L. van den Dries. Alfred Tarski's elimination theory for real closed fields. *J. Symbolic Logic 53*, 1 (březen 1988).

[17] L. van den Dries. O-minimal structures. V *Logic Colloquium '93* (Keele, 1996), W. Hodges et al., ed., Clarendon Press, Oxford.

[18] M. Dummett. A propositional calculus with denumerable matrix. *J. Symbolic Logic 25* (1959), 97–106.

[19] H.-D. Ebbinghaus a J. Flum. *Finite Model Theory*. Springer, 1995.

[20] S. Feferman. Arithmetization of metamathematics in a general setting. *Fundamenta Mathematicae 49* (1960), 35–92.

[21] J. Ferrante a C. W. Rackow. *The Computational Complexity of Logical Theories*. Springer, 1979.

[22] M. C. Fitting. *Intuitionistic Logic, Model Theory and Forcing*. North-Holland, 1969.

[23] D. Gabbay a F. Guenthner, Ed. *Handbook of Philosophical Logic*. Č. 164–167 řady Synthese Library. Kluwer, Dordrecht, 1983, 1984, 1986, 1989 (čtyři díly).

[24] M. Garey a D. Johnson. *Computers and Intractability: A Guide to the Theory of NP-completeness*. Freeman, San Francisco, 1978.

[25] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik 37* (1931), 349–360.

[26] K. Gödel. Zum intuitionistischen Aussagenkalkül. *Anzeiger Akademie der Wissenschaften Wien, Math.-naturwissensch. Klasse 69* (1932), 65–66. Viz též Ergebnisse eines matematischen Kolloquiums 4 (1933), 40.

[27] S. Gottwald. *Mehrwertige Logik*. Akademie-Verlag, Berlin, 1988.

[28] S. Gottwald. *Fuzzy Sets and Fuzzy Logic*. Vieweg, Wiesbaden, 1993.

[29] D. Guaspari a R. M. Solovay. Rosser sentences. *Annals of Math. Logic 16* (1979), 81–99.

[30] P. Hájek a M. Hájková. On interpretability in theories containing arithmetic. *Fundamenta Mathematicae 76* (1972), 131–137.

[31] P. Hájek a P. Pudlák. *Metamathematics of First Order Arithmetic*. Springer, 1993.

[32] P. Hájek a V. Švejdar. Matematická logika. Praha, listopad 1994. Předběžný učební text, v elektronické podobě.

[33] P. Hájek. Logische Kategorien. *Archiv für Matematische Logik und Grundlagenforschung 13* (1970), 168–193.

[34] P. Hájek. *Metamathematics of Fuzzy Logic.* Kluwer, 1998.

[35] G. H. Hardy a E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, Oxford, 1979.

[36] A. Heyting. Die formalen Regeln der intuitionistischen Logik. V *Sitzungsberichte der Preussischen Akademie der Wissenschaften zu Berlin*, Math. Kl. Preussische Akademie der Wissenschaften, Berlin, 1930, str. 42–56.

[37] D. Hofstadter. *Gödel, Escher, Bach: An Eternal Golden Braid.* Basic Books, Inc., New York, duben 1979. Znovu vydáno nakladatelstvím Random House, New York, 1989.

[38] G. Hughes a M. Cresswell. *A Companion to Modal Logic.* Methuen & Co. Ltd, 1984.

[39] G. Hughes a M. Cresswell. *New Introduction to Modal Logic.* Routledge, London, 1996.

[40] C. C. Chang a H. J. Keisler. *Model Theory.* North-Holland, 1973.

[41] A. Church. A note on the Entscheidungsproblem. *J. Symbolic Logic 1* (1930), 40–41.

[42] A. Church. An unsolvable problem of elementary number theory. *Amer. J. Math. 58* (1930), 345–363.

[43] E. Jeřábek. Provability Logic of the Alternative Set Theory. Diplomová práce, Filozofická fakulta Univerzity Karlovy, katedra logiky, 2001.

[44] N. D. Jones a W. T. Laaser. Complete problems for deterministic polynomial time. *Theoretical Comput. Sci. 3* (1976), 105–118.

[45] D. H. J. de Jongh a F. Veltman. Intensional Logic. Skriptum, Philosophy Department, University of Amsterdam, Amsterdam, 1988.

[46] R. M. Karp. Reducibility among combinatorial problems. V *Complexity of Computer Computation*, R. Miller a J. Thatcher, ed. Plenum Press, New York, 1972, str. 85–104.

[47] R. Kaye. *Models of Peano Arithmetic.* Oxford University Press, 1991.

[48] L. A. S. Kirby a J. B. Paris. Accessible independence results for Peano arithmetic. *Bull. London Math. Soc. 14* (1982), 285–293.

[49] S. C. Kleene. *Introduction to Metamathematics.* D. van Nostrand, 1952.

[50] J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory.* Č. 60 řady Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1995.

[51] G. Kreisel a J. L. Krivine. *Elements of Mathematical logic (Model Theory).* North-Holland, Amsterdam, 1971.

[52] L. Kučera. *Kombinatorické algoritmy.* SNTL, Praha, 1983.

[53] I. Kylar. Eliminace řezů v klasické predikátové logice. Diplomová práce, Filozofická fakulta Univerzity Karlovy, katedra logiky, 2000.

[54] R. Ladner. The computational complexity of provability in systems of modal logic. *SIAM J. Comput. 6*, 3 (1977), 467–480.

[55] M. H. Löb. Solution of a problem of Leon Henkin. *J. Symbolic Logic 20* (1955), 115–118.

[56] J. Łukasiewicz. *Selected Works.* Studies in Logic and the Foundations of Mathematics. North-Holland a PWN Warszawa, 1970.

[57] V. Mařík, O. Štěpánková, J. Lažanský et al. Umělá inteligence 4. Vyjde v nakl. Academia.

[58] E. Mendelson. *Introduction to Mathematical Logic.* Van Nostrand, 1964.

[59] J. D. Monk. *Mathematical Logic.* Springer, 1976.

[60] V. Novák, I. Perfilieva a J. Močkoř. *Mathematical Principles of Fuzzy Logic.* Kluwer, 1999.

[61] P. Odifreddi. *Classical Recursion Theory.* North-Holland, Amsterdam, 1989.

[62] C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[63] J. B. Paris a L. Harrington. A mathematical incompleteness in Peano arithmetic. V Barwise [4], kap. D.8, str. 1133–1142.

[64] J. B. Paris a L. A. S. Kirby. Σ_n-collection schemas in arithmetic. V *Logic Colloquium '77*, A. Macintyre, L. Pacholski a J. Paris, ed., Studies in Logic and the Foundations of Mathematics. North-Holland, Amsterdam, 1978, str. 199–209.

[65] E. L. Post. Introduction to a general theory of elementary propositions. *Amer. J. Math. 43* (1921), 163–185.

[66] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. V *Comptes Rendus du I*$^{\text{er}}$ *Congrès des Mathématiciens des Pays Slaves* (Warszawa, 1929), str. 92–101.

[67] P. Pudlák. On the lengths of proofs of finitistic consistency statements in first-order theories. V *Logic Colloquium '84* (1984), J. Barwise et al., ed., North-Holland, str. 165–196.

[68] P. Pudlák. Cuts, consistency statements, and interpretations. *J. Symbolic Logic 50* (1985), 423–441.

[69] P. Pudlák. The lengths of proofs. V *Handbook of Proof Theory*, S. R. Buss, ed., č. 137 řady Studies in Logic and the Foundations of Mathematics. Elsevier, 1998, kap. VIII, str. 547–637.

[70] M. O. Rabin. Decidable theories. V Barwise [4], kap. C.3, str. 595–630.

[71] H. Rogers, Jr. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, New York, 1967.

[72] J. B. Rosser. Extensions of some theorems of Gödel and Church. *J. Symbolic Logic 1* (1936), 87–91.

[73] C. Ryll-Nardzewski. The role of the axiom of induction in elementary arithmetic. *Fundamenta Mathematicae 39* (1952), 239–263.

[74] G. Sambin a S. Valentini. The modal logic of provability: The sequential approach. *Journal of Philosophical Logic 11* (1982), 311–342.

[75] J. R. Shoenfield. *Mathematical Logic.* Addison-Wesley, 1967.

[76] H. Schwichtenberg. Proof theory. V Barwise [4], kap. D.2, str. 867–896.

[77] M. Sipser. *Introduction to the Theory of Computation.* PWS Publishing Company (a division of International Thomson Publishing Inc.), 1997.

[78] C. Smoryński. The incompleteness theorems. V Barwise [4], kap. D.1, str. 819–843.

[79] C. Smoryński. Modal logic and self-reference. V Gabbay and Guenthner [23], kap. II.9, str. 441–496.

[80] C. Smoryński. *Self-Reference and Modal Logic.* Springer, New-York, 1985.

[81] C. Smoryński. Hilbert's programme. *CWI Quarterly 1*, 4 (1988).

[82] C. Smoryński. *Logical Number Theory I.* Springer, 1991.

[83] C. Smoryński. Metamathematics of Arithmetic, Chapter III: Representability and Semi-Representability. Nepublikovaný rukopis, circa 1978.

[84] C. Smoryński. Nonstandard Models of Arithmetic. Poznámky k přednášce (rukopis), 1978.

[85] A. Sochor. *Klasická matematická logika.* Karolinum, Praha, 2001.

[86] R. M. Solovay. Provability interpretations of modal logic. *Israel J. Math. 25* (1976), 287–304.

[87] R. Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Comput. Sci. 9* (1979), 67–72.

[88] P. Štěpánek. Matematická logika. Skriptum, Matematicko-fyzikální fakulta UK, Praha, 1982.

[89] V. Švejdar a K. Bendová. On inter-expressibility of logical connectives in Gödel fuzzy logic. *Soft Computing 4*, 2 (2000), 103–105.

[90] V. Švejdar. On provability logic. *Nordic Journal of Philosophical Logic 4*, 2 (2000), 95–116.

[91] G. Takeuti. *Proof Theory.* North-Holland, Amsterdam, 1975.

[92] A. Tarski, A. Mostowski a R. M. Robinson. *Undecidable Theories.* North-Holland, Amsterdam, 1953.

[93] S. Tennenbaum. Non-archimedean models for arithmetic. *Notices of the AMS 270* (1959).

[94] A. S. Troelstra a H. Schwichtenberg. *Basic Proof Theory.* Cambridge University Press, 1996.

[95] A. S. Troelstra. Aspects of constructive mathematics. V Barwise [4], kap. D.5, str. 973–1052.

[96] A. Visser. An overview of Interpretability Logic. Logic Group Preprint Series 174, Department of Philosophy, Utrecht University, Utrecht, 1997.

[97] B. L. van der Waerden. *Algebra I, II.* Springer, 1971, 1967.

[98] A. J. Wilkie a J. B. Paris. On the scheme of induction for bounded arithmetical formulas. *Annals Pure Appl. Logic 35* (1987), 261–302.

[99] A. J. Wilkie. Model completeness results for expansions of the real field by restricted Pfaffian functions and the exponential function. *J. of the AMS 9* (1996), 1051–1094.

[100] L. A. Zadeh. Fuzzy sets. *Information and Control 8*, 3 (1965), 338–353.

Rejstřík

E

Nakladatelství Academia Vás zve do tří svých exkluzivních knihkupectví s literární kavárnou a galerií — mají otevřeno 7 dní v týdnu a nabízejí největší výběr kvalitní literatury v centru Prahy, Brna a Ostravy:

- **Václavské nám. 34, 110 00 Praha 1**, tel. 224 223 511–13, e-mail knihy.vaclavskenam@academia.cz,
- **Náměstí Svobody 13, 602 00 Brno**, tel. 542 217 954–56, e-mail knihy.brno@academia.cz,
- **Zámecká 2, 702 00 Ostrava**, tel. 596 114 578, 580, e-mail knihy.ostrava@academia.cz.

Další knihkupectví Academia:

- **Národní třída 7, 110 00 Praha 1**, tel. 224 240 547, e-mail: knihy.narodni@academia.cz,
- **Na Florenci 3, 110 00 Praha 1** tel. 224 814 621, e-mail knihy.naflorenci@academia.cz.

Knihy z nakladatelství Academia si můžete objednat na adrese:

ACADEMIA — expedice
Rozvojová 135, 165 02 Praha 6
tel. 296 780 510
e-mail expedice@academia.cz
www.academia.cz

RNDr. VÍTĚZSLAV ŠVEJDAR, CSc.

LOGIKA
neúplnost, složitost a nutnost

Vydala Academia
nakladatelství Akademie věd České republiky
Legerova 61, 120 00 Praha 2
s podporou Akademie věd České republiky

Jazyková revize: doc. RNDr. Vladimír Petkevič, CSc.
Grafická úprava a sazba systémem LaTeX: autor
Návrh obálky: Robin Brichta
Redaktorka publikace: Ing. Jitka Zykánová

Vydání 1., Praha 2002
Ediční číslo 1571

Tisk SERIFA, s. r. o., Jinonická 80, Praha 5

ISBN 80-200-1005-X