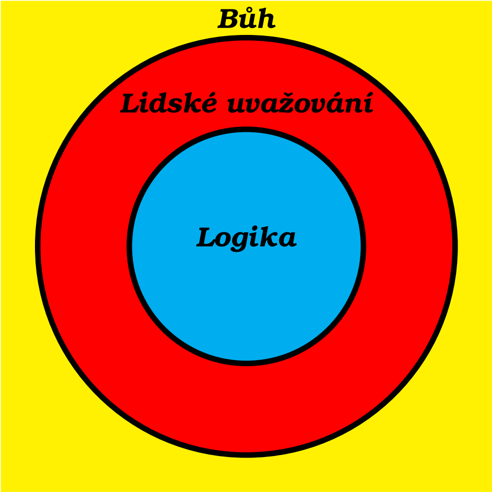
MATEMATICKÁ LOGIKA
Prezentace ke kurzu MA007

Antonín Kučera

2005

LOGIKA.



Bůh

Lidské uvažování

Logika

- *Logika* (z řeckého $\lambda o \gamma o \sigma$) zkoumá způsob vyvozování závěrů z předpokladů.
- V běžné řeči se „logikou" označuje myšlenková cesta, která vedla k daným závěrům.
- Logika nezkoumá lidské myšlení (psychologie) ani obecné poznání (epistemologie).
- *„Může (všemohoucí) Bůh stvořit kámen, který sám nedokáže uzvednout?"*

GIKA. *Neformální, formální, matematická.*

Neformální logika studuje problematiku správné argumentace v přirozeném jazyce.

Formální logika definuje a studuje abstraktní *odvozovací pravidla* (tj. *„formy úsudků"*), jejichž platnost nezávisí na významu pojmů, které v nich vystupují.

Pod pojem *matematická logika* jsou obvykle zahrnovány dvě různé oblasti výzkumu:

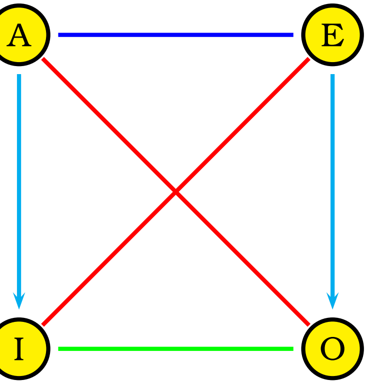
- aplikace poznatků z oblasti formální logiky na matematiku (např. snaha „vnořit" matematiku do logiky ve formě konečného systému axiomů a odvozovacích pravidel);
- aplikace matematických struktur a technik ve formální logice (např. teorie modelů, teorie důkazů, apod.)

ARISTOTELOVA LOGIKA.

Aristoteles (384-322 př. Kr.)

- Považován za zakladatele (formální) logiky.
- Zavedl a prozkoumal pojem *sylogismu*.
- Aristoteles zkoumal také pravdivostní módy a položil tak základy modální logiky.

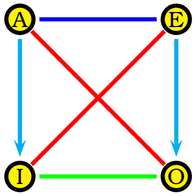
STOTELOVA LOGIKA. *Logický čtverec.*



Nechť S a P jsou *neprázdné* vlastnosti. Aristoteles rozlišuje následující základní *kategorická tvrzení*:

- A *všechna* S *jsou* P
- E *žádná* S *nejsou* P
- I *některá* S *jsou* P
- O *některá* S *nejsou* P
- Mnemonika: AffIrmo—nEgO (tvrdím—popírám)

ARISTOTELOVA LOGIKA. *Logický čtverec (pokr.)*



- A a O jsou kontradiktorická, tj. nemohou být současně pravdivá ani současně nepravdivá. I a E jsou rovněž kontradiktorická.
- A a E jsou kontrární, tj. mohou být současně nepravdivá ale ne současně pravdivá.
- I a O jsou subkontrární, tj. mohou být současně pravdivá ale ne současně nepravdivá.
- I je subalterní (podřízené) A, tj. I je pravdivé jestliže A je pravdivé, a současně A je nepravdivé jestliže I je nepravdivé. Podobně O je subalterní E.

STOTELOVA LOGIKA. *Sylogismy.*

Sylogismy jsou jednoduché úsudky tvaru

Hlavní premisa
Vedlejší premisa
$\therefore$ *Závěr*

Obě premisy i závěr jsou kategorická tvrzení tvaru A, E, I, O obsahující dohromady právě tři vlastnosti (označme je S, M, P), kde

- hlavní premisa obsahuje S a M;
- vedlejší premisa obsahuje P a M;
- závěr je tvaru S z P.

Lze tedy rozlišit následující čtyři *formy* sylogismů:

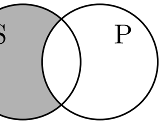
I:	M x P	II:	P x M	III:	M x P	IV:	P x M
	S y M		S y M		M y S		M y S
	$\therefore$ S z P		$\therefore$ S z P		$\therefore$ S z P		$\therefore$ S z P

Celkem tedy existuje $4 \cdot 4^3 = 256$ sylogismů.

ARISTOTELOVA LOGIKA. *Sylogismy (pokr.)*

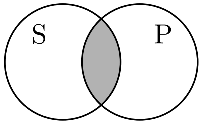
- Jen 24 sylogismů je *platných*:
  - → Forma I: AAA, AII, EAE, EIO (Barbara, Darii, Celarent, Ferio), AAI, EAO (subalterní módy);
  - → Forma II: AEE, EAE, AOO, EIO (Camestres, Cesare, Baroco, Festino), AEO, EAO (subalterní módy);
  - → Forma III: AAI, AII, EAO, EIO, OAO, IAI (Darapti, Datisi, Felapton, Ferison, Bocardo, Disamis);
  - → Forma IV: IAI, AAI, AEE, EAO, EIO (Dimatis, Bamalip, Calemes, Fesapo, Fresio), AEO (subalterní mód).
- O (ne)platnosti sylogismů se lze snadno přesvědčit pomocí *Vennových diagramů* (John Venn, 1834–1923).

STOTELOVA LOGIKA. *Platnost sylogismů.*



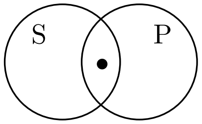
A

echna S jsou P)



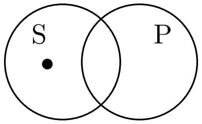
E

(žádná S nejsou P)



I

(některá S jsou P)



O

(některá S nejsou P)

šedé oblasti jsou prázdné;

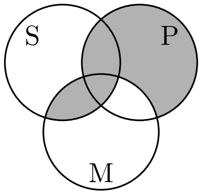
symbol „•“ označuje neprázdné oblasti;

bílé oblasti mohou být prázdné i neprázdné.

ARISTOTELOVA LOGIKA. *Platnost sylogismů (pokr.)*

- Uvažme nyní např. AEE sylogismus druhé formy (Camestres):

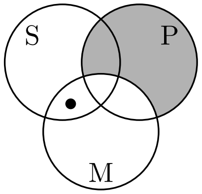
  Všechna P jsou M
  Žádná S nejsou M
  ∴ Žádná S nejsou P

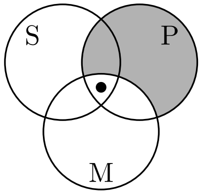


  Tento sylogismus je tedy platný.

- Pro AIO sylogismus druhé formy dostáváme:

  Všechna P jsou M
  Některá S jsou M
  ∴ Některá S nejsou P



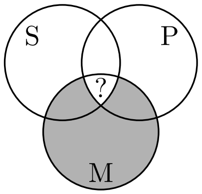


  Druhý diagram podává protipříklad, sylogismus platný není.

STOTELOVA LOGIKA. *Platnost sylogismů (pokr.)*

Rozeberme ještě AAI sylogismus třetí formy (Darapti):

Všechna M jsou P
Všechna M jsou S
∴ Některá S jsou P



Tento sylogismus je v Aristotelově logice považován za *platný*. Je však řeba použít předpoklad, že každá vlastnost je *neprázdná*. Tento předpoklad ale přináší jisté problémy:

Všechny skleněné hory jsou skleněné.
Všechny skleněné hory jsou hory.
∴ *Některé hory jsou skleněné.*

Hlavní i vedlejší premisa jsou na intuitivní úrovni pravdivá tvrzení, závěr však nikoliv.

BOOLEOVA „ALGEBRA LOGIKY.“

George Boole (1815–1864)

- Aplikoval algebraické techniky při formalizaci procesu odvozování. Nalezl souvislost mezi algebrou a sylogismy.
- Booleova „algebra logiky“ se chová podobně jako algebra čísel. Násobení odpovídá logické spojce „*a současně*“, sčítání logické spojce „*nebo*“, apod. (Odtud pocházejí pojmy „*logický součin*“ a „*logický součet*“.).

EBRA LOGIKY. *Motivační příklad.*

zme následující sylogismus:

šechna S jsou M

Žádná M nejsou P

. *Žádná S nejsou P*

ud vlastnosti identifikujeme se soubory objektů univerza, pro které , můžeme uvedený sylogismus přepsat na

$$\begin{array}{rcl} S & \subseteq & M \\ M \cap P & = & 0 \\ \therefore \quad S \cap P & = & 0 \end{array} \qquad \text{a dále na} \qquad \begin{array}{rcll} S \cap M' & = & 0 & (1) \\ M \cap P & = & 0 & (2) \\ \therefore \quad S \cap P & = & 0 & (3) \end{array}$$

usme se nyní „odvodit“ (3) z (1) a (2):

ALGEBRA LOGIKY. *Motivační příklad (pokr.)*

- Z toho, že $S \cap M' = 0$ a $X \cap 0 = 0$ pro libovolné X dostáváme

  $$(S \cap M') \cap P = 0 \qquad (4)$$

- Podobně z (2) plyne $(M \cap P) \cap S = 0$ (5).
- Ze (4), (5) a faktu, že $0 \cup 0 = 0$, plyne

  $$((S \cap M') \cap P) \cup ((M \cap P) \cap S) = 0 \qquad (6)$$

- Užitím asociativity a komutativity $\cup$ a $\cap$ dostáváme z (6)

  $$((S \cap P) \cap M') \cup ((S \cap P) \cap M) = 0 \qquad (7)$$

- Nyní podle distributivního zákona lze (7) přepsat na

  $$(S \cap P) \cap (M' \cup M) = 0 \qquad (8)$$

- Jelikož $X \cup X' = 1$ a $X \cap 1 = X$ pro libovolné X, dostáváme z (8) konečně

  $$S \cap P = 0$$

  což bylo dokázat.

EBRA LOGIKY. *Motivační příklad (pokr.)*

edchozím příkladu jsme k dokázání sylogismu použili symbolickou ipulaci se symboly S, M a P podle následujících *algebraických identit* ezabývali jsme se tím, jaký mají symboly $\cup$, $\cap$, 0, 1, a $'$ *význam*).

$$\begin{array}{rcl} X \cup X & = & X \\ X \cap X & = & X \\ X \cup Y & = & Y \cup X \\ X \cap Y & = & Y \cap X \\ X \cup (Y \cup Z) & = & (X \cup Y) \cup Z \\ X \cap (Y \cap Z) & = & (X \cap Y) \cap Z \\ X \cap (X \cup Y) & = & X \\ X \cup (X \cap Y) & = & X \\ X \cap (Y \cup Z) & = & (X \cap Y) \cup (X \cap Z) \\ X \cup (Y \cap Z) & = & (X \cup Y) \cap (X \cup Z) \end{array} \qquad \begin{array}{rcl} X \cup X' & = & 1 \\ X \cap X' & = & 0 \\ X'' & = & X \\ X \cup 1 & = & 1 \\ X \cap 1 & = & X \\ X \cup 0 & = & X \\ X \cap 0 & = & 0 \\ (X \cup Y)' & = & X' \cap Y' \\ (X \cap Y)' & = & X' \cup Y' \end{array}$$

ALGEBRA LOGIKY. *Motivační příklad (pokr.)*

- Tyto identity definují algebraickou strukturu, které se později začalo říkat *Booleva algebra* (případně *Booleův svaz*).
- V původní Booleově notaci se
  - místo $X \cap Y$ píše $X.Y$ (případně jen XY);
  - místo $X \cup Y$ píše $X + Y$;
  - místo X' píše $1 - X$.

  V této notaci pak identity dostávají „číselnou podobu“ a Boole sám se pokoušel převést další „číselné konstrukce“ (např. dělení, ale i Taylorův rozvoj) do své „algebry logiky“. Tyto úvahy však již byly zcela mylné.

GEBRA LOGIKY. *Dva základní problémy.*

Podle Boolea je každý sylogismus možné zapsat ve tvaru

$$\begin{aligned} F_1(P,M) &= 0\\ F_2(S,M) &= 0\\ \therefore\ F(S,P) &= 0 \end{aligned}$$

kde $F_1(P,M)$, $F_2(S,M)$, $F(S,P)$ jsou vhodné výrazy vytvořené ze symbolů 0, 1, $\cup$, $\cap$, $'$ a symbolů v závorkách.

Boole uvážil obecnější úsudky tvaru

$$\begin{aligned} F_1(A_1,\ldots,A_m,B_1,\ldots,B_n) &= 0\\ &\vdots\\ F_k(A_1,\ldots,A_m,B_1,\ldots,B_n) &= 0\\ \therefore\ F(B_1,\ldots,B_n) &= 0 \end{aligned}$$

Cílem jeho snah bylo vyvinout metodu, která umožní

1. zjistit, zda je daný úsudek *pravdivý*;
2. nalézt *nejobecnější* závěr (F) pro dané předpoklady (F_1,. . . ,F_k).

ALGEBRA LOGIKY. *Booleova metoda.*

Definice 1. *Nechť* $\vec{A} = A_1,\ldots,A_n$. $\vec{A}$-*konstituent je výraz tvaru* $\ell_1 \cap \cdots \cap \ell_n$, *kde* ℓ_i *je buď* A_i *nebo* A_i'.

Věta 2. *Pro každý výraz* $F(X_1,\cdots,X_n)$ *platí*

$$F(X_1,\cdots,X_n) = \bigcup_{\vec{v}\in\{0,1\}^n} F(\vec{v}) \cap \ell_1(\vec{v}) \cap \cdots \cap \ell_n(\vec{v})$$

kde $\ell_i(\vec{v})$ *je buď* X_i *nebo* X_i' *podle toho, zda je* $\vec{v}_i$ *rovno* 1 *nebo* 0.

Příklad 3. *Nechť* $F(A,B) = (A \cup B') \cap (A' \cup B)$. *Pak*

$$\begin{aligned} F(A,B) &= (F(0,0) \cap A' \cap B')\ \cup\ (F(0,1) \cap A' \cap B)\\ &\quad \cup (F(1,0) \cap A \cap B')\ \cup\ (F(1,1) \cap A \cap B)\\ &= (1 \cap A' \cap B')\ \cup\ (0 \cap A' \cap B)\ \cup\ (0 \cap A \cap B')\ \cup\ (1 \cap A \cap B)\\ &= (A' \cap B')\ \cup\ (A \cap B) \end{aligned}$$

GEBRA LOGIKY. *Řešení 1. problému.*

4. *Úsudek*

$$\begin{aligned} F_1(A_1,\ldots,A_m,B_1,\ldots,B_n) &= 0\\ &\vdots\\ F_k(A_1,\ldots,A_m,B_1,\ldots,B_n) &= 0\\ \therefore\ F(B_1,\ldots,B_n) &= 0 \end{aligned}$$

atný právě když každý $\vec{A},\vec{B}$-*konstituent výrazu* F *je* $\vec{A},\vec{B}$-*konstituentem erého* F_i.

lad 5. *Uvažme opět sylogismus*

$$\begin{aligned} S \cap M' &= 0\\ M \cap P &= 0\\ \therefore\ S \cap P &= 0 \end{aligned}$$

$\vec{A} = M$ *a* $\vec{B} = S,P$. *Uvažme* $\vec{A},\vec{B}$-*konstituenty jednotlivých výrazů:*

$$\begin{aligned} S \cap M' &: \quad M' \cap S \cap P,\quad M' \cap S \cap P'\\ M \cap P &: \quad M \cap S \cap P,\quad M \cap S' \cap P\\ S \cap P &: \quad M \cap S \cap P,\quad M' \cap S \cap P \end{aligned}$$

ALGEBRA LOGIKY. *Řešení 2. problému.*

Nechť $\vec{A} = A_1,\ldots,A_m$, $\vec{B} = B_1,\ldots,B_n$. Uvažme předpoklady tvaru

$$F_1(\vec{A},\vec{B}) = 0,\cdots,F_k(\vec{A},\vec{B}) = 0$$

Cílem je nalézt nejobecnější závěr tvaru $F(\vec{B}) = 0$. Označme

$$E(\vec{A},\vec{B}) = F_1(\vec{A},\vec{B}) \cup \cdots \cup F_k(\vec{A},\vec{B})$$

Věta 6. *Nejobecnější závěr* $F(\vec{B}) = 0$, *který plyne z* $E(\vec{A},\vec{B}) = 0$, *je tvaru*

$$F(\vec{B}) = \bigcap_{\vec{v}\in\{0,1\}^m} E(\vec{v},\vec{B})$$

Příklad 7. *Nejobecnější závěr* $F(S,P)$ *plynoucí z předpokladů* $S \cap M' = 0$ *a* $M \cap P = 0$ *je tvaru*

$$\begin{aligned} F(S,P) &= ((S \cap 0') \cup (0 \cap P)) \cap ((S \cap 1') \cup (1 \cap P))\\ &= S \cap P \end{aligned}$$

TAVBA FORMÁLNÍCH LOGICKÝCH SYSTÉMŮ.

Potřebujeme znát jisté pojmy a umět myslet (*metaúroveň*).

- Musí být např. jasné, co myslíme symbolem, konečnou posloupností, atd.
- Metapojmy a formální pojmy se bohužel často „značí“ stejně. Tím vzniká (nesprávný) dojem, že formální pojmy jsou definovány pomocí „sebe sama“ (typickým příkladem je *důkaz* nebo *množina*).
- Co všechno si lze na metaúrovni dovolit? (*potenciální* vs. *aktuální* nekonečno).

Základní kroky:

- Vymezení užívaných symbolů (abeceda).
- Syntaxe formulí.
- Sémantika (zde se objeví pojem *pravdivost*).
- Odvozovací systém (zde se objeví pojem *dokazatelnost*).

VÝROKOVÁ LOGIKA. *Syntaxe.*

Definice 8. *Abecedu výrokové logiky tvoří následující symboly:*

- *znaky pro výrokové proměnné* $A, B, C, \ldots$, *kterých je spočetně mnoho;*
- *logické spojky* $\wedge, \vee, \rightarrow, \neg$
- *závorky* $($ *a* $)$

Definice 9. *Formule výrokové logiky je slovo* φ *nad abecedou výrokové logiky, pro které existuje vytvořující posloupnost, tj. konečná posloupnost slov* $\psi_1, \cdots, \psi_k$, *kde* $k \geq 1$, ψ_k *je* φ, *a pro každé* $1 \leq i \leq k$ *má slovo* ψ_i *jeden z následujících tvarů:*

- *výroková proměnná,*
- $\neg\psi_j$ *pro nějaké* $1 \leq j < i$,
- $(\psi_j \circ \psi_{j'})$ *pro nějaká* $1 \leq j, j' < i$, *kde* $\circ$ *je jeden ze symbolů* $\wedge, \vee, \rightarrow$.

Poznámka 10. *Notace: vnější závorky budeme zpravidla vynechávat. Např. místo* $(A \vee \neg B)$ *budeme psát* $A \vee \neg B$.

ROKOVÁ LOGIKA. *Sémantika.*

nice 11. *Pravdivostní ohodnocení (valuace) je zobrazení* v, *které každé kové proměnné přiřadí hodnotu* 0 *nebo* 1.

amatematickou indukcí k délce vytvořující posloupnosti lze každou aci v jednoznačně rozšířit na všechny výrokové formule:

$v(A)$ je již definováno;

$$v(\neg\psi) = \begin{cases} 0 & \text{jestliže } v(\psi) = 1; \\ 1 & \text{jinak.} \end{cases}$$

$$v((\psi_1 \wedge \psi_2)) = \begin{cases} 0 & \text{jestliže } v(\psi_1) = 0 \text{ nebo } v(\psi_2) = 0; \\ 1 & \text{jinak.} \end{cases}$$

$$v((\psi_1 \vee \psi_2)) = \begin{cases} 0 & \text{jestliže } v(\psi_1) = 0 \text{ a současně } v(\psi_2) = 0; \\ 1 & \text{jinak.} \end{cases}$$

$$v((\psi_1 \rightarrow \psi_2)) = \begin{cases} 0 & \text{jestliže } v(\psi_1) = 1 \text{ a současně } v(\psi_2) = 0; \\ 1 & \text{jinak.} \end{cases}$$

VÝROKOVÁ LOGIKA. *Sémantika (pokr.)*

Definice 12. *Výroková formule* φ *je*

- *pravdivá (resp. nepravdivá) při valuaci* v, *pokud* $v(\varphi) = 1$ *(resp.* $v(\varphi) = 0$*);*
- *splnitelná, jestliže existuje valuace* v *taková, že* $v(\varphi) = 1$;
- *tautologie (také (logicky) pravdivá), jestliže* $v(\varphi) = 1$ *pro každou valuaci* v.

Soubor T *výrokových formulí je splnitelný, jestliže existuje valuace* v *taková, že* $v(\varphi) = 1$ *pro každé* φ *z* T.

Definice 13. *Formule* φ *a* ψ *jsou ekvivalentní, psáno* $\varphi \approx \psi$, *právě když pro každou valuaci* v *platí, že* $v(\varphi) = v(\psi)$.

Příklad 14. *Nechť* φ, ψ, ξ *jsou výrokové formule. Pak:*

$$\begin{aligned} \varphi \wedge \psi &\approx \psi \wedge \varphi \\ \varphi \wedge (\psi \wedge \xi) &\approx (\varphi \wedge \psi) \wedge \xi \\ \varphi \wedge (\psi \vee \xi) &\approx (\varphi \wedge \psi) \vee (\varphi \wedge \xi) \\ \neg(\varphi \wedge \psi) &\approx \neg\varphi \vee \neg\psi \\ \neg\neg\varphi &\approx \varphi \end{aligned}$$

ROKOVÁ LOGIKA. *Sémantika (pokr.)*

námka 15. *„Identity“ z příkladu 14 umožňují dále zpřehlednit zápis*
ulí. Např. místo $(A \vee B) \vee C$ můžeme (nejednoznačně) psát $A \vee B \vee C$.
nejednoznačnost nevede k problémům, neboť příslušné definice a
ení „fungují“ pro libovolné možné uzávorkování.

námka 16. *V teorii výpočetní složitosti se dokazuje, že problém zda*
á výroková formule φ je splnitelná (resp. tautologie) je NP-úplný (resp.
P-úplný). Otázka, zda existuje efektivní (polynomiální) algoritmus pro
lené problémy, je ekvivalentní otázce zda P = NP.

nice 17. *Formule φ je tautologickým důsledkem souboru formulí T,*
no $T \models \varphi$, jestliže $v(\varphi) = 1$ pro každou valuaci v takovou, že $v(\psi) = 1$ pro
lou formuli ψ ze souboru T. Jestliže $T \models \varphi$ pro prázdný soubor T, píšeme
ce $\models \varphi$.

VÝROKOVÁ LOGIKA. *Pravdivostní tabulky.*

Někdy se sémantika výrokových spojek definuje „předem“ pomocí *pravdivostních tabulek*:

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

X	Y	$X \vee Y$
0	0	0
0	1	1
1	0	1
1	1	1

X	Y	$X \to Y$
0	0	1
0	1	1
1	0	0
1	1	1

X	$\neg X$
0	1
1	0

Pojmy „pravdivostní tabulka“ a „výroková spojka“ je možné dále zobecnit a uvážit formální logické systémy budované na obecnějším základu:

Definice 18. *Výroková funkce je funkce $F : \{0,1\}^n \to \{0,1\}$, kde $n \geq 1$.*

ROKOVÁ LOGIKA. *Formální systém $\mathcal{L}(F_1, \cdots, F_k)$.*

nt' $F_1, \cdots, F_k$ je konečný soubor výrokových funkcí. Definujeme formální
ký systém $\mathcal{L}(F_1, \cdots, F_k)$, kde

Abeceda je tvořena znaky pro výrokové proměnné, závorkami a znaky
$\mathcal{F}_1, \cdots, \mathcal{F}_k$ pro uvedené výrokové funkce.

V definici vytvořující posloupnosti formule (viz *definice 48*) požadujeme,
aby ψ_i bylo buď výrokovou proměnnou nebo tvaru $\mathcal{F}_j(\psi_{j_1}, \cdots, \psi_{j_n})$, kde
$\leq j_1, \cdots, j_n < i$ a n je arita F_j.

Valuace rozšíříme z výrokových proměnných na formule předpisem

$$v(\mathcal{F}(\psi_1, \cdots, \psi_n)) = F(v(\psi_1), \cdots, v(\psi_n))$$

mto smyslu je pak dosud uvažovaný systém výrokové logiky systémem
$\vee, \to, \neg)$. Dříve zavedené sémantické pojmy (splnitelnost, pravdivost,
se opírají pouze o pojem valuace a „fungují“ tedy v *libovolném*
ému $\mathcal{L}(F_1, \cdots, F_k)$.

VÝROKOVÁ LOGIKA. *Formální systém $\mathcal{L}(F_1, \cdots, F_k)$.*

Pro účely následující definice zvolme libovolné (ale dále pevné) lineární uspořádání $\sqsubseteq$ na souboru všech výrokových proměnných.

Definice 19. *Nechť φ je formule $\mathcal{L}(F_1, \cdots, F_k)$ a nechť $X_1, \cdots, X_n$ je vzestupně uspořádaná posloupnost (vzhledem k $\sqsubseteq$) všech výrokových proměnných, které se ve φ vyskytují. Formule φ jednoznačně určuje výrokovou funkci $F_\varphi : \{0,1\}^n \to \{0,1\}$ danou předpisem $F_\varphi(\vec{u}) = v(F)$, kde v je valuace definovaná takto: $v(X_i) = \vec{u}(i)$ pro každé $1 \leq i \leq n$, $v(Y) = 0$ pro ostatní Y.*

Definice 20. *Systém $\mathcal{L}(F_1, \cdots, F_k)$ je plnohodnotný, jestliže pro každou výrokovou funkci F existuje formule φ systému $\mathcal{L}(F_1, \cdots, F_k)$ taková, že $F = F_\varphi$.*

ROKOVÁ LOGIKA. *Plnohodnotnost systémů.*

a 21. *Systém $\mathcal{L} = (\wedge, \vee, \neg)$ je plnohodnotný.*

az. Nechť $F : \{0,1\}^n \to \{0,1\}$ je výroková funkce a nechť $\vec{u}_1, \cdots, \vec{u}_k$ jsou
hny vektory z $\{0,1\}^n$, pro které nabývá F hodnoty 1. Pokud žádný
vý vektor není (tj. $k = 0$), klademe $\varphi = X_1 \wedge \neg X_1 \wedge X_2 \wedge \cdots \wedge X_n$. Jinak

$$\varphi = \bigvee_{i=1}^{k} \ell_1(u_i) \wedge \cdots \wedge \ell_k(u_i)$$

$\ell_j(u_i)$ je buď X_j nebo $\neg X_j$ podle toho, zda $u_i(j) = 1$ nebo $u_i(j) = 0$. Nyní
hce ověří, že $F = F_\varphi$. □

VÝROKOVÁ LOGIKA. *Plnohodnotnost systémů (pokr.)*

Uvažme následující výrokové funkce:

X	Y	$X \curlywedge Y$
0	0	1
0	1	0
1	0	0
1	1	0

X	Y	$X \mid Y$
0	0	1
0	1	1
1	0	1
1	1	0

X	Y	Z	$\odot(X, Y, Z)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

- Funkce $\curlywedge$ se nazývá *Schröderův* operátor. Platí $\varphi \curlywedge \psi \approx \neg\varphi \wedge \neg\psi$.
- Funkce $\mid$ se nazývá *Shefferův* operátor. Platí $\varphi \mid \psi \approx \neg(\varphi \wedge \psi)$.

ROKOVÁ LOGIKA. *Plnohodnotnost systémů (pokr.)*

edující systémy výrokové logiky jsou plnohodnotné:

$\mathcal{L}(\wedge, \vee, \neg)$	*Věta 21*.
$\mathcal{L}(\wedge, \neg)$	$\varphi \vee \psi \approx \neg(\neg\varphi \wedge \neg\psi)$
$\mathcal{L}(\vee, \neg)$	$\varphi \wedge \psi \approx \neg(\neg\varphi \vee \neg\psi)$
$\mathcal{L}(\to, \neg)$	$\varphi \vee \psi \approx \neg\varphi \to \psi$
$\mathcal{L}(\curlywedge)$	$\neg\varphi \approx \varphi \curlywedge \varphi, \quad \varphi \vee \psi \approx (\varphi \curlywedge \varphi) \curlywedge (\varphi \curlywedge \varphi)$
$\mathcal{L}(\mid)$	$\neg\varphi \approx \varphi \mid \varphi, \quad \varphi \wedge \psi \approx (\varphi \mid \psi) \mid (\varphi \mid \psi)$
$\mathcal{L}(\odot)$	$\neg\varphi \approx \odot(\varphi, \varphi, \varphi),$ $\varphi \to \psi \approx \odot(\varphi, \odot(\varphi, \varphi, \varphi), \odot(\varphi, \psi, \odot(\varphi, \varphi, \varphi)))$

edující systémy plnohodnotné nejsou:

$\mathcal{L}(\wedge)$, $\mathcal{L}(\vee)$, $\mathcal{L}(\to)$, $\mathcal{L}(\neg)$, atd.

VÝROKOVÁ LOGIKA. *Shefferovské spojky.*

Definice 22. *Výroková funkce F je Shefferovská jestliže $\mathcal{L}(F)$ je plnohodnotný systém.*

Věta 23. *Nechť $S(n)$ značí počet všech Shefferovských funkcí arity $n \geq 1$. Pak $S(n) = 2^{(2^{n-1}-1)}(2^{(2^{n-1}-1)} - 1)$.*

Pro $n = 1, 2, 3, 4, 5, \ldots$ dostáváme postupně $0, 2, 56, 16256, 1073709056, \ldots$

Důsledek 24. *Jelikož $\lim_{n\to\infty} \frac{S(n)}{2^{2^n}} = 1/4$, je (pro velká n) zhruba čtvrtina ze všech výrokových funkcí arity n Shefferovská.*

Poznámka 25. *Výsledky o Shefferovských funkcích nalézají uplatnění při výrobě logických obvodů; na „podkladové desce“ se např. vytvoří hustá síť binárních $\mid$-hradel. Obvody různé funkce se pak realizují jejich vhodným propojením.*

ROKOVÁ LOGIKA. *Normální formy.*

nice 26.

- *Literál je formule tvaru X nebo $\neg X$, kde X je výroková proměnná;*
- *Klauzule je formule tvaru $\ell_1 \vee \cdots \vee \ell_n$, kde $n \geq 1$ a každé ℓ_i je literál.*
- *Duální klauzule je formule tvaru $\ell_1 \wedge \cdots \wedge \ell_n$, kde $n \geq 1$ a každé ℓ_i je iterál.*
- *Formule v konjunktivním normálním tvaru (CNF) je formule tvaru $C_1 \wedge \cdots \wedge C_m$, kde $m \geq 1$ a každé C_i je klauzule.*
- *Formule v disjunktivním normálním tvaru je formule tvaru $C_1 \vee \cdots \vee C_m$, kde $m \geq 1$ a každé C_i je duální klauzule.*

mžitým důsledkem *věty 21* je následující:

27. *Pro každou formuli φ existuje ekvivalentní formule v disjunktivním nálním tvaru.*

VÝROKOVÁ LOGIKA. *Normální formy (pokr.)*

Věta 28. *Pro každou formuli φ existuje ekvivalentní formule v konjunktivním normálním tvaru.*

Důkaz. Podle *Věty 27* existuje k φ ekvivalentní formule v disjunktivním normálním tvaru, tj. $\varphi \approx \bigvee_{i=1}^{n} D_i$, kde $n \geq 1$ a každé D_i je duální klauzule. Metaindukcí vzhledem k n:

- $n = 1$. Pak $\bigvee_{i=1}^{n} D_i$ je současně v CNF.
- *Indukční krok:* Nechť $D_1 = \ell_1 \wedge \cdots \wedge \ell_k$. Platí

$$\bigvee_{i=1}^{n+1} D_i \approx D_1 \vee \bigvee_{i=2}^{n+1} D_i \approx D_1 \vee \bigwedge_{i=1}^{m} C_i \approx \bigwedge_{i=1}^{m} D_1 \vee C_i \approx \bigwedge_{i=1}^{m} \bigwedge_{j=1}^{k} (\ell_j \vee C_i)$$

□

Příklad 29. *Formuli $(A \to B) \wedge (B \to C) \wedge (C \to A)$ lze v CNF reprezentovat jako $(\neg A \vee B) \wedge (\neg B \vee C) \wedge (\neg C \vee A)$ nebo $(\neg A \vee C) \wedge (\neg C \vee B) \wedge (\neg B \vee A)$. CNF tedy není určena jednoznačně až na pořadí klauzulí a literálů.*

ROKOVÁ LOGIKA. *Věta o kompaktnosti.*

30 (o kompaktnosti). *Nechť T je soubor formulí výrokové logiky. T je itelný právě když každá konečná část T je splnitelná.*

az. Směr „⇒“ je triviální. Dokážeme „⇐“. Zavedeme pomocný pojem: bor V výrokových formulí je *dobrý*, jestliže každý konečný podsoubor V lnitelný. Nechť $\psi_1, \psi_2, \ldots$ je posloupnost *všech* formulí výrokové logiky. amatematickou indukcí definujeme pro každé $i \geq 1$ *dobrý* soubor S_i:

$S_1 = T$. Soubor S_1 je dobrý neboť T je dobrý.

$$S_{i+1} = \begin{cases} S_i \cup \{\psi_i\} & \text{jestliže } S_i \cup \{\psi_i\} \text{ je dobrý;} \\ S_i \cup \{\neg\psi_i\} & \text{jinak.} \end{cases}$$

Alespoň jeden ze souborů $S_i \cup \{\psi_i\}$ a $S_i \cup \{\neg\psi_i\}$ *musí* být dobrý; jinak existují konečné $V_1 \subseteq S_i \cup \{\psi_i\}$ a $V_2 \subseteq S_i \cup \{\neg\psi_i\}$, které nejsou splnitelné. Jestliže $V_1 \subseteq S_i$ nebo $V_2 \subseteq S_i$, máme ihned spor s tím, že S_i je dobrý; jinak $V_1 \cup V_2$ obsahuje ψ i $\neg\psi$, proto i $(V_1 \cup V_2) \setminus \{\psi_i, \neg\psi_i\} \subseteq S_i$ je nesplnitelný, spor.)

VÝROKOVÁ LOGIKA. *Věta o kompaktnosti.*

Nechť $S = \bigcup_{i=1}^{\infty} S_i$. Dokážeme, že S má následující vlastnosti:

- *S obsahuje φ právě když S neobsahuje $\neg\varphi$.*

  S nutně obsahuje φ nebo $\neg\varphi$. Jestliže S obsahuje φ i $\neg\varphi$, existuje S_i obsahující φ i $\neg\varphi$; tedy $\{\varphi, \neg\varphi\}$ je nesplnitelný podsoubor S_i, spor.
- *S obsahuje $\varphi \wedge \psi$ právě když S obsahuje φ i ψ;*
- *S obsahuje $\varphi \vee \psi$ právě když S obsahuje φ nebo ψ;*
- *S obsahuje $\varphi \to \psi$ právě když S neobsahuje φ nebo obsahuje ψ.*

Buď v valuace definovaná takto: $v(A) = 1$ právě když A patří do S. Indukcí k délce vytvořující posloupnosti se nyní snadno ověří (s využitím výše uvedených vlastností S), že:

- *S obsahuje φ právě když $v(\varphi) = 1$.*

Tedy S (a proto i T) je splnitelný. □

ROKOVÁ LOGIKA. *Věta o kompaktnosti (použití).*

ím *věty 30* lze snadno dokázat řadu dalších tvrzení.

Graf $\mathcal{G}$ je dvojice (U, H), kde U je nejvýše spočetný soubor *uzlů* a H je areflexivní a symetrická relace na U.

Podgraf grafu $\mathcal{G}$ je graf $\mathcal{G}' = (U', H')$, kde $U' \subseteq U$ a $H' \subseteq H$.

Graf $\mathcal{G} = (U, H)$ je k-*obarvitelný* jestliže existuje funkce $f : U \to \{1, \cdots, k\}$ aková, že $f(u) \neq f(v)$ pro každé $(u, v) \in H$.

VÝROKOVÁ LOGIKA. *Věta o kompaktnosti (použití).*

Věta 31. *Graf $\mathcal{G} = (U, H)$ je k-obarvitelný právě když každý konečný podgraf $\mathcal{G}$ je k-obarvitelný.*

Důkaz. Nechť $B_{u,i}$ je výroková proměnná pro každý uzel u a každé $1 \leq i \leq k$. Buď T soubor tvořený následujícími formulemi:

- $B_{u,1} \vee \cdots \vee B_{u,k}$ pro každý uzel u;
- $B_{u,i} \to \neg B_{u,j}$ pro každý uzel u a každé $1 \leq i, j \leq k$, kde $i \neq j$;
- $B_{u,i} \to \neg B_{v,i}$ pro každé $(u, v) \in H$ a $1 \leq i \leq k$.

Platí následující pozorování:

- Graf $\mathcal{G}$ je k-obarvitelný právě když soubor T je splnitelný.
- Každý konečný podgraf $\mathcal{G}$ je k-obarvitelný právě když každý konečný podsoubor T je splnitelný.

Nyní stačí aplikovat *větu 30*. □

ROKOVÁ LOGIKA. *Odvozovací systém pro $\mathcal{L}(\to, \neg)$*

o části se soustředíme na $\mathcal{L}(\to, \neg)$. Uvažme následující odvozovací ém pro $\mathcal{L}(\to, \neg)$ (Lukasiewicz, 1928):

émata axiómů:

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

A2: $(\varphi \to (\psi \to \xi)) \to ((\varphi \to \psi) \to (\varphi \to \xi))$

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

ozovací pravidlo:

MP: Z φ a $\varphi \to \psi$ odvoď ψ. (modus ponens)

VÝROKOVÁ LOGIKA. *Odvozovací systém pro $\mathcal{L}(\to, \neg)$*

Definice 32. *Buď T soubor formulí.*

- *Důkaz formule ψ z předpokladů T je konečná posloupnost formulí $\varphi_1, \cdots, \varphi_k$, kde φ_k je ψ a pro každé φ_i, kde $1 \leq i \leq k$, platí alespoň jedna z následujících podmínek:*
  - *φ_i je prvek T;*
  - *φ_i je instancí jednoho ze schémat A1–A3;*
  - *φ_i uznikne aplikací pravidla MP na formule φ_m, φ_n pro vhodné $1 \leq m, n < i$.*
- *Formule ψ je dokazatelná z předpokladů T, psáno $T \vdash \psi$, jestliže existuje důkaz ψ z předpokladů T. Jestliže $T \vdash \psi$ pro prázdné T, říkáme že ψ je dokazatelná a píšeme $\vdash \psi$.*

ROKOVÁ LOGIKA. *Odvozovací systém pro* $\mathcal{L}(\to,\neg)$

lad 33. *Pro libovolnou formuli* φ *platí* $\vdash \varphi \to \varphi$.

az. Následující posloupnost formulí je důkazem $\varphi \to \varphi$.

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

□

VÝROKOVÁ LOGIKA. *Odvozovací systém pro* $\mathcal{L}(\to,\neg)$

Příklad 34. *Pro libovolné formule* φ, ψ *platí* $\{\varphi, \neg\varphi\} \vdash \psi$.

Důkaz. Následující posloupnost formulí je důkazem ψ z $\{\varphi, \neg\varphi\}$:

1)	$\neg\varphi \to (\neg\psi \to \neg\varphi)$	A1
2)	$\neg\varphi$	předpoklad
3)	$\neg\psi \to \neg\varphi$	MP na 2), 1)
4)	$(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$	A3
5)	$\varphi \to \psi$	MP na 3), 4)
6)	φ	předpoklad
7)	ψ	MP na 6), 5)

□

ROKOVÁ LOGIKA. *Věta o dedukci.*

35 (o dedukci). *Nechť* φ, ψ *jsou formule a* T *soubor formulí. Pak*
$\psi\} \vdash \varphi$ *právě když* $T \vdash \psi \to \varphi$.

az.

Nechť $\xi_1, \cdots, \xi_k$ je důkaz formule $\psi \to \varphi$ z předpokladů T. Pak
$\cdot, \xi_k, \psi, \varphi$ je důkaz formule φ z předpokladů $T \cup \{\psi\}$ (poslední formule
kne aplikací MP na ψ a ξ_k).

Nechť $\xi_1, \cdots, \xi_k$ je důkaz φ z předpokladů $T \cup \{\psi\}$. Metaindukcí k j
ážeme, že $T \vdash \psi \to \xi_j$ pro každé $1 \leq j \leq k$.

$= 1$. Je-li ξ_1 instance axiómu nebo formule z T, platí $T \vdash \xi_1$. K důkazu
ξ_1 z T nyní připojíme formule $\xi_1 \to (\psi \to \xi_1)$, $\psi \to \xi_1$. První formule je
nstancí A1, druhá aplikací MP na ξ_1 a první formuli. Máme tedy důkaz
$\psi \to \xi_1$ z T.

Je-li ξ_1 formule ψ, platí $T \vdash \psi \to \psi$ podle *příkladu 33*.

VÝROKOVÁ LOGIKA. *Věta o dedukci.*

- *Indukční krok:* Je-li formule ξ_j instancí axiómu nebo prvek $T \cup \{\psi\}$, postupujeme stejně jako výše (místo ξ_1 použijeme ξ_j).

  Je-li ξ_j výsledkem aplikace MP na ξ_m, ξ_n, kde $1 \leq m, n < j$, je ξ_n tvaru $\xi_m \to \xi_j$. Podle I.P. navíc platí $T \vdash \psi \to \xi_m$ a $T \vdash \psi \to (\xi_m \to \xi_j)$. Důkazy $\psi \to \xi_m$ a $\psi \to (\xi_m \to \xi_j)$ z T nyní zřetězíme za sebe a připojíme následující formule:

  → $(\psi \to (\xi_m \to \xi_j)) \to ((\psi \to \xi_m) \to (\psi \to \xi_j))$

  → $(\psi \to \xi_m) \to (\psi \to \xi_j)$

  → $\psi \to \xi_j$

  První formule je instancí A2, další dvě vzniknou aplikací MP. Máme tedy důkaz formule $\psi \to \xi_j$ z T.

□

36 (o korektnosti). *Nechť* φ *je formule a* T *soubor formulí. Jestliže*
φ, *pak* $T \models \varphi$.

az. Nechť $\xi_1, \cdots, \xi_k$ je důkaz φ z T. Indukcí vzhledem k j dokážeme, že
ξ_j pro každé $1 \le j \le k$. (Stačí ověřit, že každá instance A1–A3 je
ologie, a že jestliže $T \models \psi$ a $T \models \psi \to \xi$, pak také $T \models \xi$). $\square$

Lema 37. *Nechť* φ, ψ *jsou formule. Pak*

(a) $\vdash \neg\varphi \to (\varphi \to \psi)$

(b) $\vdash \neg\neg\varphi \to \varphi$

(c) $\vdash \varphi \to \neg\neg\varphi$

(d) $\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$

(e) $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$

(f) $\vdash (\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$

Důkaz.

➠ (a): Podle *příkladu 34* platí $\{\varphi, \neg\varphi\} \vdash \psi$, proto $\vdash \neg\varphi \to (\varphi \to \psi)$ opakovaným užitím věty o dedukci.

b): Platí

1)	$\vdash \neg\neg\varphi \to (\neg\varphi \to \neg\neg\neg\varphi)$	podle (a)
2)	$\{\neg\neg\varphi\} \vdash \neg\varphi \to \neg\neg\neg\varphi$	věta o dedukci
3)	$\vdash (\neg\varphi \to \neg\neg\neg\varphi) \to (\neg\neg\varphi \to \varphi)$	A3
4)	$\{\neg\neg\varphi\} \vdash \neg\neg\varphi \to \varphi$	MP na 2), 3)
5)	$\{\neg\neg\varphi\} \vdash \varphi$	věta o dedukci
6)	$\vdash \neg\neg\varphi \to \varphi$	věta o dedukci

c): Platí

1)	$\vdash \neg\neg\neg\varphi \to \neg\varphi$	podle (b)
2)	$\vdash (\neg\neg\neg\varphi \to \neg\varphi) \to (\varphi \to \neg\neg\varphi)$	A3
3)	$\vdash \varphi \to \neg\neg\varphi$	MP na 1), 2)

➠ (d): Platí

1)	$\{\varphi \to \psi\} \vdash \varphi \to \psi$	
2)	$\{\neg\neg\varphi\} \vdash \varphi$	podle (b) a věty o dedukci
3)	$\{\varphi \to \psi, \neg\neg\varphi\} \vdash \psi$	MP na 2), 1)
4)	$\vdash \psi \to \neg\neg\psi$	podle (c)
5)	$\{\varphi \to \psi, \neg\neg\varphi\} \vdash \neg\neg\psi$	MP na 3), 4)
6)	$\{\varphi \to \psi\} \vdash \neg\neg\varphi \to \neg\neg\psi$	věta o dedukci
7)	$\vdash (\neg\neg\varphi \to \neg\neg\psi) \to (\neg\psi \to \neg\varphi)$	A3
8)	$\{\varphi \to \psi\} \vdash \neg\psi \to \neg\varphi$	MP na 6), 7)
9)	$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$	věta o dedukci

ROKOVÁ LOGIKA. *Věta o úplnosti.*

e): Platí

1) $\{\varphi, \varphi \to \psi\} \vdash \psi$

2) $\{\varphi\} \vdash (\varphi \to \psi) \to \psi$ věta o dedukci

3) $\vdash ((\varphi \to \psi) \to \psi) \to (\neg\psi \to \neg(\varphi \to \psi))$ podle (d)

4) $\{\varphi\} \vdash \neg\psi \to \neg(\varphi \to \psi)$ MP na $2), 3)$

5) $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$ věta o dedukci

---

VÝROKOVÁ LOGIKA. *Věta o úplnosti.*

➠ (f): Platí

1) $\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi))$ podle (d)

2) $\{\varphi \to \psi, \neg\psi\} \vdash \neg\varphi$ 2x MP na $1)$

3) $\{\varphi \to \psi, \neg\psi, \neg\varphi \to \psi\} \vdash \psi$ MP na $2), \neg\varphi \to \psi$

4) $\{\varphi \to \psi, \neg\varphi \to \psi\} \vdash \neg\psi \to \psi$ věta o dedukci

5) $\vdash \neg\psi \to (\neg\psi \to \neg(\neg\psi \to \psi))$ podle (e)

6) $\{\neg\psi\} \vdash \neg(\neg\psi \to \psi)$ 2x věta o dedukci

7) $\vdash \neg\psi \to \neg(\neg\psi \to \psi)$ věta o dedukci

8) $\vdash (\neg\psi \to \neg(\neg\psi \to \psi)) \to ((\neg\psi \to \psi) \to \psi)$ A3

9) $\vdash (\neg\psi \to \psi) \to \psi$ MP na $7), 8)$

10) $\{\varphi \to \psi, \neg\varphi \to \psi\} \vdash \psi$ MP na $4), 9)$

11) $\vdash (\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$ 2x věta o dedukci

□

ROKOVÁ LOGIKA. *Věta o úplnosti.*

nice 38. *Nechť v je valuace a φ formule. Jestliže $v(\varphi) = 1$, označuje bol φ^v formuli φ. Jinak φ^v označuje formuli $\neg\varphi$.*

a 39 (A. Church). *Nechť v je valuace, φ formule, a $\{X_1, \cdots, X_k\}$ konečný bor výrokových proměnných, kde všechny proměnné vyskytující se ve φ mezi $\{X_1, \cdots, X_k\}$. Pak $\{X_1^v, \cdots, X_k^v\} \vdash \varphi^v$.*

az. Indukcí k délce vytvořující posloupnosti pro φ.

Je-li $\varphi = X$, pak X je mezi $\{X_1, \cdots, X_k\}$ a tedy $\{X_1^v, \cdots, X_k^v\} \vdash X^v$.

Je-li $\varphi = \neg\psi$, kde $\{X_1^v, \cdots, X_k^v\} \vdash \psi^v$, rozlišíme dvě možnosti:

→ $v(\psi) = 0$. Pak $\psi^v = \neg\psi$ a $\varphi^v = \neg\psi$, není co dokazovat.

→ $v(\psi) = 1$. Pak $\psi^v = \psi$ a $\varphi^v = \neg\neg\psi$. Podle *lematu 37 (c)* platí $\vdash \psi \to \neg\neg\psi$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \neg\neg\psi$ užitím MP.

VÝROKOVÁ LOGIKA. *Věta o úplnosti.*

➠ Je-li $\varphi = \psi \to \xi$, kde $\{X_1^v, \cdots, X_k^v\} \vdash \psi^v$ a $\{X_1^v, \cdots, X_k^v\} \vdash \xi^v$ rozlišíme následující možnosti:

→ $v(\psi \to \xi) = 1$. Máme tedy dokázat, že $\{X_1^v, \cdots, X_k^v\} \vdash \psi \to \xi$.

- Jestliže $v(\psi) = 0$, platí $\{X_1^v, \cdots, X_k^v\} \vdash \neg\psi$. Podle *lematu 37 (a)* dále platí $\vdash \neg\psi \to (\psi \to \xi)$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \psi \to \xi$ užitím MP.
- Jestliže $v(\xi) = 1$, platí $\{X_1^v, \cdots, X_k^v\} \vdash \xi$. Podle A1 platí $\vdash \xi \to (\psi \to \xi)$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \psi \to \xi$ užitím MP.

→ $v(\psi \to \xi) = 0$. Pak $\{X_1^v, \cdots, X_k^v\} \vdash \psi$ a $\{X_1^v, \cdots, X_k^v\} \vdash \neg\xi$. Máme dokázat, že $\{X_1^v, \cdots, X_k^v\} \vdash \neg(\psi \to \xi)$. Podle *lematu 37 (e)* platí $\vdash \psi \to (\neg\xi \to \neg(\psi \to \xi))$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \neg(\psi \to \xi)$ opakovaným užitím MP.

□

ROKOVÁ LOGIKA. *Věta o úplnosti.*

40 (o úplnosti). *Nechť* φ *je formule a* T *soubor formulí. Jestliže* $T \models \varphi$, $T \vdash \varphi$.

az. Nejprve uvážíme případ, kdy T je *prázdný* soubor. Nechť φ je ologie a $X_1, \cdots, X_k$ všechny výrokové proměnné, které se ve φ vyskytují.

Podle Churchova lematu platí $\{X_1^v, \cdots, X_k^v\} \vdash \varphi$ pro *libovolnou* valuaci v.

Ukážeme, že všechny X_i^v lze postupně „eliminovat“, až dostaneme důkaz φ z prázdného souboru formulí.

poládejme, že pro dané $0 \leq n < k$ jsme již prokázali, že

$$\{X_1^v, \cdots, X_n^v, X_{n+1}^v\} \vdash \varphi$$

libovolnou valuaci v. Dokážeme, že pak také $\{X_1^u, \cdots, X_n^u\} \vdash \varphi$ pro volnou valuaci u.

VÝROKOVÁ LOGIKA. *Věta o úplnosti.*

Buď tedy u libovolná valuace. Nechť u_1, u_2 jsou valuace definované takto: $u_1(X_k) = 1$, $u_2(X_k) = 0$, a pro každé $Y \neq X_k$ platí $u_1(Y) = u_2(Y) = v(Y)$. Platí

1) $\{X_1^u, \cdots, X_n^u, X_{n+1}\} \vdash \varphi$ předpoklad pro $v = u_1$
2) $\{X_1^u, \cdots, X_n^u, \neg X_{n+1}\} \vdash \varphi$ předpoklad pro $v = u_2$
3) $\{X_1^u, \cdots, X_n^u\} \vdash X_{n+1} \rightarrow \varphi$ věta o dedukci na 1)
4) $\{X_1^u, \cdots, X_n^u\} \vdash \neg X_{n+1} \rightarrow \varphi$ věta o dedukci na 2)
5) $\vdash (X_{n+1} \rightarrow \varphi) \rightarrow ((\neg X_{n+1} \rightarrow \varphi) \rightarrow \varphi)$ podle *lematu 37 (f)*
6) $\{X_1^u, \cdots, X_n^u\} \vdash \varphi$ 2x MP na 5) s využitím 3), 4)

ROKOVÁ LOGIKA. *Věta o úplnosti.*

uvážíme obecný případ. Buď T *libovolný* soubor formulí a φ formule vá, že $T \models \varphi$. Podle věty o kompaktnosti existuje konečný soubor $\cdots, \psi_n\}$ formulí z T takový, že $\{\psi_1, \cdots, \psi_n\} \models \varphi$. Lehce se ověří, že

$$\models \psi_1 \rightarrow (\psi_2 \rightarrow (\psi_3 \rightarrow \cdots (\psi_n \rightarrow \varphi) \cdots)$$

e předchozího bodu tedy platí

$$\vdash \psi_1 \rightarrow (\psi_2 \rightarrow (\psi_3 \rightarrow \cdots (\psi_n \rightarrow \varphi) \cdots)$$

aplikacích věty o dedukci dostáváme $\{\psi_1, \cdots, \psi_n\} \vdash \varphi$, tedy také φ. □

VÝROKOVÁ LOGIKA. *Historické poznámky.*

- Výroková logika byla nebyla rozvíjena samostatně, ale jako součást složitějších formálních systémů.
- *Gottlob Frege* (1848–1925) položil základy predikátové logiky a zavedl „moderní“ odvozovací systém. „Výrokový fragment“ tohoto systému vypadá takto (verze z roku 1879):
  - 1: $P \rightarrow (Q \rightarrow P)$
  - 2: $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$
  - 3: $(P \rightarrow (Q \rightarrow R)) \rightarrow (Q \rightarrow (P \rightarrow R))$
  - 4: $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$
  - 5: $\neg\neg P \rightarrow P$
  - 6: $P \rightarrow \neg\neg P$
  - Odvozovací pravidla: MP a substituce

  Fregeho výsledky byly vědeckou komunitou ignorovány zhruba 20 let.

ROKOVÁ LOGIKA. *Historické poznámky.*

Giuseppe Peano (1858-1932) doporučil na mezinárodním natematickém kongresu v Paříži (rok 1900) mladému *Bertrandu Russellovi* (1872-1970) studovat Fregeho práce. Russell v roce 1901 bjevil inkonzistenci ve Fregeho systému (Russelův paradox), současně lně docenil Fregeho myšlenky. V letech 1910-1913 byla publikována řídílná *Principia Mathematica* (autoři Whitehead, Russel). Tato nonografie měla hluboký vliv na vývoj logiky v následujících lesetiletích. Věnována byla Fregemu. Pro fragment výrokové logiky byly oužity následující axiómy a odvozovací pravidla:

- 1: $(P \vee P) \rightarrow P$
- 2: $Q \rightarrow (P \vee Q)$
- 3: $(P \vee Q) \rightarrow (Q \vee P)$
- 4: $(P \vee (Q \vee R)) \rightarrow (Q \vee (P \vee R))$
- 5: $(Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow (P \vee R))$
- Odvozovací pravidla: MP a substituce

VÝROKOVÁ LOGIKA. *Historické poznámky.*

- V roce 1917 nalezl Jean Nicod následující zjednodušení axiomatického systému z *Principia Mathematica*:
  - 1: $(P \vee P) \rightarrow P$
  - 2: $P \rightarrow (P \vee Q)$
  - 4: $(P \vee (Q \vee R)) \rightarrow (Q \vee (P \vee R))$
  - 5: $(Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow (P \vee R))$
  - Odvozovací pravidla: MP a substituce
- Ve stejném roce publikoval Henry Sheffer následující axiomatický systém založený na Shefferově operátoru:
  - Axióm: $(P|(Q|R))|((S|(S|S))|((U|Q)|((P|U)|(P|U))))$
  - Odvozovací pravidla: substituce a „z F a $F|(G|H)$ odvoď H“

ROKOVÁ LOGIKA. *Historické poznámky.*

David Hilbert (1862–1943) a Wilhelm Ackermann (1896-1962) oublikovali v roce 1928 následující systém:

- 1: $(P \vee P) \rightarrow P$
- 2: $P \rightarrow (P \vee Q)$
- 4: $(P \vee Q) \rightarrow (Q \vee P)$
- 5: $(Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow (P \vee R))$
- Odvozovací pravidla: MP a substituce

/ roce 1927 navrhl John von Neumann (1903-1957) aplikovat substituci pouze na axiómy. Vznikly systémy založené na *schématech axiómů*.

Jan Lukasiewicz (1878–1956) prezentoval svůj odvozovací systém použitý v přednášce) v roce 1928.

VÝROKOVÁ LOGIKA. *Historické poznámky.*

- Další odvozovací systémy:
  - V roce 1947 zjednodušili Götling a Rasiowa systém z *Principia Mathematica* do následující podoby:
    - 1: $(P \vee P) \rightarrow P$
    - 2: $P \rightarrow (P \vee Q)$
    - 3: $(Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow (P \vee R))$
    - Odvozovací pravidla: MP a substituce
  - V roce 1953 prezentoval Meredith systém s jediným schématem a jediným odvozovacím pravidlem:
    - Schéma axiómu: $((((\varphi \rightarrow \psi) \rightarrow (\neg\rho \rightarrow \neg\xi)) \rightarrow \rho) \rightarrow \gamma) \rightarrow ((\gamma \rightarrow \varphi) \rightarrow (\xi \rightarrow \varphi))$
    - Odvozovací pravidlo: MP

EDIKÁTOVÁ LOGIKA. *Vznik a vývoj.*

Predikátová logika (také *logika prvního řádu*) se opírá o pojem *vlastnosti* (tj. *predikátu*). Umožňuje formulovat tvrzení o vlastnostech objektů s využitím *kvantifikátorů*.

Např. Aristotelova logika je z dnešního pohledu fragmentem predikátové logiky.

Formule prvního řádu byly součástí Fregeho systému, později se objevily ve 3. dílu Schröderovy monografie *Algebra der Logik* (1910) a monografii *Principia Mathematica* (Whitehead, Russel).

Logika prvního řádu byla definována jako samostatný systém až v monografii Hilberta a Ackermanna *Grundzügen der theoretischen Logik* (1928).

PREDIKÁTOVÁ LOGIKA. *Syntaxe.*

Definice 41. *Jazyk (stejně jako jazyk s rovností) je systém predikátových symbolů a funkčních symbolů, kde u každého symbolu je dána jeho četnost (arita), která je nezáporným celým číslem.*

Poznámka 42.

- *Predikáty arity nula v jistém smyslu odpovídají výrokovým proměnným, funkční symboly arity nula jsou symboly pro konstanty.*
- *Predikátovým a funkčním symbolům se také říká mimologické symboly. Jazyk je tedy plně určen mimologickými symboly.*
- *Rozdíl mezi jazykem a jazykem s rovností se projeví v tom, že do predikátové logiky pro jazyk s rovností přidáme speciální logický symbol* $=$ *jehož sémantika bude definována speciálním způsobem.*

EDIKÁTOVÁ LOGIKA. *Syntaxe.*

lad 43.

Jazyk teorie množin je jazykem s rovností, který obsahuje jeden predikátový symbol $\in$ *arity* 2.

Jazyk teorie pologrup je jazykem s rovností, který obsahuje jeden funkční symbol „$\cdot$*“ arity* 2.

nice 44. *Abecedu predikátové logiky pro jazyk* $\mathcal{L}$ *tvoří následující boly:*

Znaky pro proměnné $x, y, z, \ldots$*, kterých je spočetně mnoho*

Mimologické symboly, tj. predikátové a funkční symboly jazyka $\mathcal{L}$.

Je-li $\mathcal{L}$ *jazyk s rovností, obsahuje abeceda speciální znak* $=$ *pro rovnost.*

Logické spojky $\rightarrow$ *a* $\neg$.

Symbol $\forall$ *pro univerzální kvantifikátor.*

Závorky $($ *a* $)$.

PREDIKÁTOVÁ LOGIKA. *Syntaxe.*

Definice 45. *Termem jazyka* $\mathcal{L}$ *je slovo* t *nad abecedou predikátové logiky pro jazyk* $\mathcal{L}$*, pro které existuje vytvořující posloupnost slov* $t_1, \cdots, t_k$*, kde* $k \geq 1$, t_k *je* t*, a pro každé* $1 \leq i \leq k$ *má slovo* t_i *jeden z následujících tvarů:*

- *proměnná,*
- $f(t_{i_1}, \cdots, t_{i_n})$*, kde* $1 \leq i_1, \cdots, i_n < k$, f *je funkční symbol jazyka* $\mathcal{L}$*, a* n *je arita* f.

Term je uzavřený, jestliže neobsahuje proměnné.

Poznámka 46. *U binárních funkčních symbolů (a později také predikátů) dovolíme pro větší čitelnost infixový zápis. U funkčních (a predikátových) symbolů arity nula budeme psát* c *místo* $c()$.

Příklad 47.

- $(x \cdot y) \cdot z$ *je termem jazyka pologrup (v prefixové notaci* $\cdot(\cdot(x, y), z)$*)*
- $0 + (S(0) + S(S(0)))$ *je termem jazyka* $0, S, +$*, kde* 0, S *a* $+$ *jsou po řadě*

unkční symboly arity nula, jedna a dva.

Definice 48. *Formule predikátového počtu jazyka $\mathcal{L}$ je slovo φ nad abecedou predikátové logiky pro jazyk $\mathcal{L}$, pro které existuje vytvořující posloupnost slov $\psi_1, \cdots, \psi_k$, kde $k \geq 1$, ψ_k je φ, a pro každé $1 \leq i \leq k$ má slovo ψ_i jeden z následujících tvarů:*

- $P(t_1, \cdots, t_n)$, *kde P je predikátový symbol jazyka $\mathcal{L}$ arity n a $t_1, \cdots, t_n$ jsou termy jazyka $\mathcal{L}$.*
- $t_1 = t_2$, *je-li $\mathcal{L}$ jazyk s rovností a t_1, t_2 jsou termy jazyka $\mathcal{L}$.*
- $\neg\psi_j$ *pro nějaké $1 \leq j < i$,*
- $(\psi_j \to \psi_{j'})$ *pro nějaká $1 \leq j, j' < i$,*
- $\forall x\, \psi_j$, *kde x je proměnná a $1 \leq j < i$.*

---

námka 49. *Ve zbytku přednášky budeme používat následující atky“:*

- $\exists x\, \varphi$ *značí* $\neg\forall x \neg\varphi$
- $\varphi \vee \psi$ *značí* $\neg\varphi \to \psi$
- $\varphi \wedge \psi$ *značí* $\neg(\varphi \to \neg\psi)$.
- $\varphi \leftrightarrow \psi$ *značí* $(\varphi \to \psi) \wedge (\psi \to \varphi)$, *kde symbol $\wedge$ dále „rozvineme“ podle předchozího bodu.*

lady formulí:

- $\forall x\, P(x, y) \wedge \exists x\, (P(x, x) \vee Q(c))$
- $\forall x\, \exists x\, (P(x, x) \vee \forall y\, \forall x\, Q(x))$

Definice 50. *Každý výskyt proměnné ve formuli predikátového počtu je buď volný nebo vázaný podle následujícího induktivního předpisu:*

- *Ve formuli tvaru $P(t_1, \cdots, t_n)$ jsou všechny výskyty proměnných volné.*
- *Výrokové spojky nemění charakter výskytů proměnných, tj. je-li daný výskyt proměnné ve formuli ψ volný (resp. vázaný), je odpovídající výskyt ve formulích $\neg\psi$, $\varphi \to \psi$, $\psi \to \varphi$ rovněž volný (resp. vázaný).*
- *Ve formuli $\forall x\, \psi$ je každý výskyt proměnné x (včetně výskytu za kvantifikátorem) vázaný; byl-li výskyt proměnné různé od x volný (resp. vázaný) ve formuli ψ, je odpovídající výskyt ve formuli $\forall x\, \psi$ rovněž volný (resp. vázaný).*

Příklady (volné výskyty jsou *červené*):

- $\forall x\, P(x, y) \vee \forall y\, P(x, y)$
- $\forall x\, (P(x, y) \vee \forall y\, P(x, y))$

DIKÁTOVÁ LOGIKA. *Syntaxe.*

nice 51.

Proměnná se nazývá volnou (resp. vázanou) ve formuli, má-li v ní volný resp. vázaný) výskyt.

Formule je otevřená, jestliže v ní žádná proměnná nemá vázaný výskyt.

Formule je uzavřená (také sentence), jestliže v ní žádná proměnná nemá volný výskyt.

Zápis $\varphi(x_1,\cdots,x_n)$ značí, že všechny volné proměnné ve formuli φ jsou mezi $x_1,\cdots,x_n$ (nemusí nutně platit, že každá z těchto proměnných je volná ve φ).

Univerzální uzávěr formule φ je formule tvaru $\forall x_1\cdots\forall x_n\,\varphi$, kde $_1,\cdots,x_n$ jsou právě všechny volné proměnné formule φ.

PREDIKÁTOVÁ LOGIKA. *Substituce.*

Definice 52. *Term t je substituovatelný za proměnnou x ve formuli φ, jestliže žádný výskyt proměnné v termu t se nestane vázaným po provedení substituce termu t za každý volný výskyt proměnné x ve formuli φ. Je-li t substituovatelný za x ve φ, značí zápis $\varphi(x/t)$ formuli, která vznikne nahrazením každého volného výskytu x ve φ termem t.*

Příklady:

- Term $y+3$ je substituovatelný za x ve formuli $\exists z\, x{+}y{=}z$
- Term $y+z$ není substituovatelný za x ve formuli $\exists z\, x{+}y{=}z$
- $(P(x,y)\ \wedge\ \forall x\, P(x,y))(x/3)$ je formule $P(3,y)\ \wedge\ \forall x\, P(x,y)$
- $P(x,y)(x/y)(y/x)$ je formule $P(x,x)$

DIKÁTOVÁ LOGIKA. *Substituce.*

nice 53. *Nechť φ je formule a $t_1,\cdots,t_n$ termy, které jsou v uvedeném dí substituovatelné za proměnné $x_1,\cdots,x_n$ ve φ (předpokládáme, že $\cdot,x_n$ jsou různé). Symbol $\varphi(x_1/t_1,\cdots,x_n/t_n)$ značí formuli, která kne „simultánním nahrazením“ každého volného výskytu x_i termem t_i každé $1\le i\le n$. Přesněji, $\varphi(x_1/t_1,\cdots,x_n/t_n)$ je formule $/z_1)\cdots(x_n/z_n)(z_1/t_1)\cdots(z_n/t_n)$, kde $z_1,\cdots,z_n$ jsou (různé) proměnné, é se nevyskytují v $t_1,\cdots,t_n$ ani mezi $x_1,\cdots,x_n$.*

lad:

$P(x,y)(x/y,y/x)$ je formule $P(y,x)$

PREDIKÁTOVÁ LOGIKA. *Realizace jazyka.*

Definice 54. *Realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je zadána*

- *neprázdným souborem M, nazývaným univerzem (případně nosičem). Prvky univerza nazýváme individui.*
- *přiřazením, které každému n-árnímu predikátovému symbolu P přiřadí n-ární relaci P_M na M*
- *přiřazením, které každému m-árnímu funkčnímu symbolu přiřadí funkci $f_M : M^m \to M$.*

Ohodnocení je zobrazení přiřazující proměnným prvky univerza M.

DIKÁTOVÁ LOGIKA. *Realizace jazyka.*

nice 55. *Realizaci termu* t *při ohodnocení* e *v relizaci* $\mathcal{M}$*, psáno* $t^{\mathcal{M}}[e]$ *adně jen* $t[e]$ *je-li* $\mathcal{M}$ *jasné z kontextu), definujeme induktivně takto:*

$[e] = e(x)$

$(t_1, \cdots, t_m)[e] = f_M(t_1[e], \cdots, t_m[e])$
pro $m = 0$ *je na pravé staně uvedené definující rovnosti* $f_M(\emptyset)$*).*

PREDIKÁTOVÁ LOGIKA. *Realizace jazyka.*

Definice 56 (A. Tarski)**.** *Buď* $\mathcal{M}$ *realizace jazyka* $\mathcal{L}$, e *ohodnocení a* φ *formule predikátového počtu jazyka* $\mathcal{L}$*. Ternární vztah* $\mathcal{M} \models \varphi[e]$ *definujeme indukcí ke struktuře* φ*:*

- $\mathcal{M} \models P(t_1, \cdots, t_m)[e]$ *právě když* $(t_1[e], \cdots, t_m[e]) \in P_{\mathcal{M}}$.
- *Jestliže* $\mathcal{L}$ *je jazyk s rovností, definujeme* $\mathcal{M} \models (t_1 = t_2)[e]$ *právě když* $t_1[e]$ *a* $t_2[e]$ *jsou stejná individua.*
- $\mathcal{M} \models \neg\psi[e]$ *právě když není* $\mathcal{M} \models \psi[e]$.
- $\mathcal{M} \models (\psi \to \xi)[e]$ *právě když* $\mathcal{M} \models \xi[e]$ *nebo není* $\mathcal{M} \models \psi[e]$.
- $\mathcal{M} \models \forall x\, \psi[e]$ *právě když* $\mathcal{M} \models \psi[e(x/a)]$ *pro každý prvek* a *univerza* M.

Jestliže $\mathcal{M} \models \varphi[e]$*, říkáme, že* φ *je pravdivá v* $\mathcal{M}$ *při ohodnocení* e*. Jestliže* $\mathcal{M} \models \varphi[e]$ *pro každé* e*, je* φ *pravdivá v* $\mathcal{M}$*, psáno* $\mathcal{M} \models \varphi$*.*

DIKÁTOVÁ LOGIKA. *Realizace jazyka.*

lad 57. *Buď* $\mathcal{L}$ *jazyk s jedním unárním predikátem* P *a* $\mathcal{M}$ *jeho realizace univerzem* $M = \{a, b\}$*, kde* $P_M = \{a\}$*. Pak*

Platí $\mathcal{M} \models \exists x\, (P(x) \to (P(x) \wedge \neg P(x)))$

Neplatí $\mathcal{M} \models P(x) \to \forall x\, P(x)$

Neplatí $\mathcal{M} \models (\forall x\, P(x) \to \forall x\, \neg P(x)) \to \forall x\, (P(x) \to \neg P(x))$

PREDIKÁTOVÁ LOGIKA. *Teorie.*

Definice 58. *Buď* $\mathcal{L}$ *jazyk (příp. jazyk s rovností).*

- *Teorie (s jazykem* $\mathcal{L}$*) je soubor* T *formulí predikátového počtu jazyka* $\mathcal{L}$*. Prvky* T *se nazývají axiómy teorie* T*.*
- *Realizace* $\mathcal{M}$ *jazyka* $\mathcal{L}$ *je model teorie* T*, psáno* $\mathcal{M} \models T$*, jestliže* $\mathcal{M} \models \varphi$ *pro každé* φ *z* T*.*
- *Teorie je splnitelná, jestliže má model.*
- *Je-li* $\mathcal{M}$ *realizace jazyka* $\mathcal{L}$*, pak* $Th(\mathcal{M})$ *označuje teorii tvořenou právě všemi uzavřenými formulemi, které jsou v* $\mathcal{M}$ *pravdivé.*
- *Formule* φ *je sémantickým důsledkem teorie* T*, psáno* $T \models \varphi$*, jestliže* φ *je pravdivá v každém modelu teorie* T*.*

DIKÁTOVÁ LOGIKA. *Teorie.*

lad 59. *Uvažme jazyk s rovností obsahující jeden binární funkční bol "$\cdot$" a jednu konstantu* 1. *Nechť* T *je tvořena následujícími formulemi:*

$\forall x\,\forall y\,\forall z\;\; x\cdot(y\cdot z)=(x\cdot y)\cdot z$

$\forall x\;\; (x\cdot 1=x)\land(1\cdot x=x)$

$\forall x\,\exists y\;\; (x\cdot y=1)\land(y\cdot x=1)$

formule $\forall x\,\forall y\;\; (x\cdot y)=(y\cdot x)$ *není sémantickým důsledkem* T, *zatímco ule* $x\cdot(1\cdot y)=(1\cdot x)\cdot y$ *ano.*

PREDIKÁTOVÁ LOGIKA. *Odvozovací systém.*

- Schémata *výrokových axiómů*:
  - P1: $\varphi\to(\psi\to\varphi)$
  - P2: $(\varphi\to(\psi\to\xi))\to((\varphi\to\psi)\to(\varphi\to\xi))$
  - P3: $(\neg\varphi\to\neg\psi)\to(\psi\to\varphi)$
- Schéma *axiómu specifikace*:
  - P4: $\forall x\,\varphi\to\varphi(x/t)$, kde t je substituovatelný za x ve φ.
- Schéma *axiómu distribuce*:
  - P5: $(\forall x\,(\varphi\to\psi))\to(\varphi\to\forall x\,\psi)$, kde x nemá volný výskyt ve φ.
- Odvozovací pravidla:
  - MP: Z φ a $\varphi\to\psi$ odvoď ψ. (*modus ponens*)
  - GEN: Z φ odvoď $\forall x\,\varphi$. (*generalizace*)

DIKÁTOVÁ LOGIKA. *Odvozovací systém.*

$\mathcal{L}$ jazyk s rovností, přidáme dále následující *axiómy rovnosti*:

R1: $x=x$

R2: $(x_1{=}y_1\land\cdots\land x_n{=}y_n\land P(x_1,\cdots,x_n))\to P(y_1,\cdots,y_n)$,
kde P je predikátový symbol arity n.

R3: $(x_1{=}y_1\land\cdots\land x_m{=}y_m)\to(f(x_1,\cdots,x_m){=}f(y_1,\cdots,y_m))$,
kde f je funkční symbol arity m.

PREDIKÁTOVÁ LOGIKA. *Odvozovací systém.*

Definice 60. *Buď* T *teorie jazyka* $\mathcal{L}$.

- *Důkaz formule* ψ *v teorii* T *je konečná posloupnost formulí* $\varphi_1,\cdots,\varphi_k$, *kde* φ_k *je* ψ *a pro každé* φ_i, *kde* $1\le i\le k$, *platí alespoň jedna z následujících podmínek:*
  - φ_i *je prvek* T*;*
  - φ_i *je instancí jednoho ze schémat P1–P5;*
  - $\mathcal{L}$ *je jazyk s rovností a* φ_i *je instancí jednoho ze schémat R1–R3;*
  - φ_i *vznikne aplikací pravidla MP na formule* φ_m, φ_n *pro vhodné* $1\le m,n<i$.
  - φ_i *vznikne aplikací pravidla GEN na formuli* φ_m *pro vhodné* $1\le m<i$.

DIKÁTOVÁ LOGIKA. *Odvozovací systém.*

Formule ψ je dokazatelná v teorii T, psáno $T \vdash \psi$, jestliže existuje důkaz ψ v T. Jestliže $T \vdash \psi$ pro prázdné T, říkáme že ψ je dokazatelná a píšeme $\vdash \psi$.

Formule ψ je vyvratitelná v teorii T, jestliže $T \vdash \neg\psi$

Teorie T je sporná (též inkonzistentní), jestliže každá formule predikátové ogiky jazyka $\mathcal{L}$ je v T dokazatelná.

Teorie je bezesporná (též konzistentní), jestliže není nekonzistentní.

PREDIKÁTOVÁ LOGIKA. *Důkazy.*

Poznámka 61 (Princip dosazení do tautologie výrokového počtu)**.** *Je-li φ tautologií $\mathcal{L}(\neg, \rightarrow)$, ve které nahradíme výrokové proměnné formulemi predikátové logiky tak, že daná výroková proměnná je nahrazena vždy touž formulí, obdržíme formuli predikátové logiky, která je dokazatelná v odvozovacím systému predikátové logiky pouze pomocí P1–P3 a MP.*

Poznámka 62 (Neplatnost „obecné“ věty o dedukci)**.** *Za předpokladu korektnosti odvozovacího systému pro predikátovou logiku neplatí $\vdash \varphi \rightarrow \forall x\, \varphi$. Platí ovšem $\{\varphi\} \vdash \forall x\, \varphi$. Proto obecně neplatí, že $T \models \varphi \rightarrow \psi$ právě když $T \cup \{\varphi\} \models \psi$.*

DIKÁTOVÁ LOGIKA. *Věta o dedukci.*

63 (o dedukci)**.** *Nechť T je teorie jazyka $\mathcal{L}$, ψ uzavřená formule jazyka φ (libovolná) formule jazyka $\mathcal{L}$. Pak $T \vdash \psi \rightarrow \varphi$ právě když $T \cup \{\psi\} \vdash \varphi$.*

az.

az je velmi podobný důkazu *věty 35*:

Nechť $\xi_1, \cdots, \xi_k$ je důkaz formule $\psi \rightarrow \varphi$ v T. Pak $\xi_1, \cdots, \xi_k, \psi, \varphi$ je az formule φ v $T \cup \{\psi\}$ (poslední formule vznikne aplikací MP na ψ a ξ_k).

Nechť $\xi_1, \cdots, \xi_k$ je důkaz φ v $T \cup \{\psi\}$. Metaindukcí k j dokážeme, že $\psi \rightarrow \xi_j$ pro každé $1 \leq j \leq k$.

$= 1$. Je-li ξ_1 instance axiómu nebo formule z T, platí $T \vdash \xi_1$. K důkazu ξ_1 z T nyní připojíme formule $\xi_1 \rightarrow (\psi \rightarrow \xi_1)$, $\psi \rightarrow \xi_1$. První formule je nstancí P1, druhá aplikací MP na ξ_1 a první formuli. Máme tedy důkaz $\psi \rightarrow \xi_1$ v T.

Je-li ξ_1 formule ψ, platí $T \vdash \psi \rightarrow \psi$ podle *příkladu 33* a *poznámky 62*.

PREDIKÁTOVÁ LOGIKA. *Věta o dedukci.*

- *Indukční krok:* Je-li formule ξ_j instancí axiómu nebo prvek $T \cup \{\psi\}$, postupujeme stejně jako výše (místo ξ_1 použijeme ξ_j).
  - Je-li ξ_j výsledkem aplikace MP na ξ_m, ξ_n, kde $1 \leq m, n < j$, je ξ_n tvaru $\xi_m \rightarrow \xi_j$. Podle I.P. navíc platí $T \vdash \psi \rightarrow \xi_m$ a $T \vdash \psi \rightarrow (\xi_m \rightarrow \xi_j)$. Důkazy $\psi \rightarrow \xi_m$ a $\psi \rightarrow (\xi_m \rightarrow \xi_j)$ v T nyní zřetězíme za sebe a připojíme následující formule:

    → $(\psi \rightarrow (\xi_m \rightarrow \xi_j)) \rightarrow ((\psi \rightarrow \xi_m) \rightarrow (\psi \rightarrow \xi_j))$
    → $(\psi \rightarrow \xi_m) \rightarrow (\psi \rightarrow \xi_j)$
    → $\psi \rightarrow \xi_j$

    První formule je instancí P2, další dvě vzniknou aplikací MP. Máme tedy důkaz formule $\psi \rightarrow \xi_j$ v T.

DIKÁTOVÁ LOGIKA. *Věta o dedukci.*

➠ Je-li ξ_j výsledkem aplikace GEN na ξ_m, kde $1 \leq m < j$, je ξ_j tvaru $\forall x\, \xi_m$. Podle I.P. platí $T \vdash \psi \to \xi_m$. K tomuto důkazu nyní stačí připojit formule

→ $\forall x\, (\psi \to \xi_m)$

→ $\forall x\, (\psi \to \xi_m) \to (\psi \to \forall x\, \xi_m)$

→ $\psi \to \forall x\, \xi_m$.

První vznikne aplikací GEN, druhá je instancí P5, třetí vznikne aplikací MP. Dostaneme tak důkaz formule $\psi \to \xi_j$ v T.

□

PREDIKÁTOVÁ LOGIKA. *Vlastnosti kvantifikace.*

Lema 64. *Pro každé formule φ a ψ platí:*

1. $\vdash (\forall x\, (\varphi \to \psi)) \leftrightarrow (\varphi \to \forall x\, \psi)$, *pokud x není volná ve formuli φ;*

2. $\vdash (\forall x\, (\varphi \to \psi)) \leftrightarrow (\exists x\, \varphi \to \psi)$, *pokud x není volná ve formuli ψ;*

3. $\vdash (\exists x\, (\varphi \to \psi)) \leftrightarrow (\varphi \to \exists x\, \psi)$, *pokud x není volná ve formuli φ;*

4. $\vdash (\exists x\, (\varphi \to \psi)) \leftrightarrow (\forall x\, \varphi \to \psi)$, *pokud x není volná ve formuli ψ.*

Důkaz. Pozorování:

(a) Jestliže $\vdash \varphi \to \psi$ a současně $\vdash \psi \to \varphi$, pak $\vdash \varphi \leftrightarrow \psi$. To plyne z toho, že $(A \to B) \to ((B \to A) \to (A \leftrightarrow B))$ je výroková tautologie (viz *poznámka 61*).

(b) (tranzitivita implikace). Jestliže $T \vdash \varphi \to \xi$ a současně $T \vdash \xi \to \psi$, pak $T \vdash \varphi \to \psi$. Stačí použít *poznámku 61* a tautologii $(A \to C) \to ((C \to B) \to (A \to B))$.

DIKÁTOVÁ LOGIKA. *Vlastnosti kvantifikace.*

Necht’ $\varphi(x)$, $\psi(x)$ jsou formule. Pak $\vdash \forall x\, (\varphi \to \psi) \to \forall x\, (\neg\psi \to \neg\varphi)$, neboť

1)	$\vdash \forall x\, (\varphi \to \psi) \to (\varphi \to \psi)$	P4
2)	$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$	výr. tautologie
3)	$\vdash \forall x\, (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$	tranz. impl. na 1), 2)
4)	$\forall x\, (\varphi \to \psi) \vdash \neg\psi \to \neg\varphi$	věta o dedukci
5)	$\forall x\, (\varphi \to \psi) \vdash \forall x\, (\neg\psi \to \neg\varphi)$	GEN
6)	$\vdash \forall x\, (\varphi \to \psi) \to \forall x\, (\neg\psi \to \neg\varphi)$	věta o dedukci

ení 1.–4. teď dokážeme za předpokladu, že $\varphi(x)$ a $\psi(x)$. Obecná podoba yne užitím věty konstantách (viz dále).

PREDIKÁTOVÁ LOGIKA. *Vlastnosti kvantifikace.*

1. Platí $\vdash (\forall x\, (\varphi \to \psi)) \to (\varphi \to \forall x\, \psi)$, neboť tato formule je instancí P5. Důkaz opačné implikace vypadá takto:

1)	$\vdash \forall x\, \psi \to \psi$	P4
2)	$\vdash (\forall x\, \psi \to \psi) \to ((\varphi \to \forall x\, \psi) \to (\varphi \to \psi))$ $(A \to B) \to ((C \to A) \to (C \to B))$ je tautologie, viz *pozn. 61*	
3)	$\vdash (\varphi \to \forall x\, \psi) \to (\varphi \to \psi)$	MP na 1), 2)
4)	$\varphi \to \forall x\, \psi \vdash \varphi \to \psi$	věta o dedukci
5)	$\varphi \to \forall x\, \psi \vdash \forall x\, (\varphi \to \psi)$	GEN
6)	$\vdash (\varphi \to \forall x\, \psi) \to (\forall x\, (\varphi \to \psi))$	věta o dedukci

DIKÁTOVÁ LOGIKA. *Vlastnosti kvantifikace.*

Nejprve ukážeme, že $\vdash \forall x\,(\varphi \to \psi) \to (\exists x\,\varphi \to \psi)$.

1)	$\vdash \forall x\,(\neg\psi \to \neg\varphi) \to (\neg\psi \to \forall x\,\neg\varphi)$	podle 1.
2)	$\vdash \forall x\,(\varphi \to \psi) \to \forall x\,(\neg\psi \to \neg\varphi)$	podle (c)
3)	$\vdash \forall x\,(\varphi \to \psi)) \to (\neg\psi \to \forall x\,\neg\varphi)$	tranz. impl. na 2), 1)
4)	$\vdash (\neg\psi \to \forall x\,\neg\varphi) \to (\neg\forall x\,\neg\varphi \to \psi)$	taut. $(\neg B \to A) \to (\neg A \to B)$
5)	$\vdash \forall x\,(\varphi \to \psi) \to (\neg\forall x\,\neg\varphi \to \psi)$	tranz. impl. na 3), 4)
6)	$\vdash \forall x\,(\varphi \to \psi) \to (\exists x\,\varphi \to \psi)$	reformulace

---

PREDIKÁTOVÁ LOGIKA. *Vlastnosti kvantifikace.*

Nyní opačný směr $\vdash (\exists x\,\varphi \to \psi) \to \forall x\,(\varphi \to \psi)$:

1)	$\vdash (\neg\psi \to \forall x\,\neg\varphi) \to \forall x\,(\neg\psi \to \neg\varphi)$	podle 1.
2)	$\vdash (\neg\forall x\,\neg\varphi \to \psi) \to (\neg\psi \to \forall x\,\neg\varphi)$	taut. $(\neg B \to A) \to (\neg A \to B)$
3)	$\vdash (\neg\forall x\,\neg\varphi \to \psi) \to \forall x\,(\neg\psi \to \neg\varphi)$	tranz. impl. na 1), 2)
4)	$\exists x\,\varphi \to \psi \vdash \forall x\,(\neg\psi \to \neg\varphi)$	věta o dedukci
5)	$\exists x\,\varphi \to \psi \vdash \neg\psi \to \neg\varphi$	P4 a MP
6)	$\exists x\,\varphi \to \psi \vdash \varphi \to \psi$	$(\neg A \to \neg B) \to (A \to B)$ a MP
7)	$\exists x\,\varphi \to \psi \vdash \forall x\,(\varphi \to \psi)$	GEN
8)	$\vdash (\exists x\,\varphi \to \psi) \to \forall x\,(\varphi \to \psi)$	věta o dedukci

□

DIKÁTOVÁ LOGIKA. *Věta o korektnosti.*

a 65. *Nechť T je teorie a φ formule jazyka teorie T. Jestliže $T \vdash \varphi$, pak* φ.

az. Stačí ověřit následující tvrzení:

Je-li ψ instancí jednoho ze schémat P1–P5 (příp. také R1–R3, pokud azyk teorie T je jazyk s rovností) a $\mathcal{M}$ je model T, pak $\mathcal{M} \models \psi$.

Je-li $\mathcal{M}$ model T a ψ, ξ formule jazyka teorie T, kde $\mathcal{M} \models \psi$ a $\mathcal{M} \models \psi \to \xi$, pak $\mathcal{M} \models \xi$.

Je-li $\mathcal{M}$ model T a ψ formule jazyka teorie T, kde $\mathcal{M} \models \psi$, pak $\mathcal{M} \models \forall x\,\psi$.

aindukcí vzhledem k i je pak již triviální ukázat, že je-li $\psi_1, \cdots, \psi_k$ az formule φ v T a $\mathcal{M}$ je model T, pak $T \models \psi_i$ pro každé $1 \leq i \leq k$. □

PREDIKÁTOVÁ LOGIKA. *Věta o úplnosti (úvod).*

Lema 66. *Následující tvrzení jsou ekvivalentní:*

1. *Pro každou teorii T a pro každou formuli φ jazyka teorie T platí, že jestliže $T \models \varphi$, pak $T \vdash \varphi$.*
2. *Každá bezesporná teorie má model.*

Důkaz.

$(1. \Rightarrow 2.)$ Buď T bezesporná teorie. Pak existuje formule φ jazyka teorie T, která není v T dokazatelná (tj. $T \nvdash \varphi$). Obměnou 1. pak ale dostáváme, že φ není sémantickým důsledkem T (tj. $T \not\models \varphi$). To znamená, že existuje takový model T, kde není pravdivá φ. Zejména má tedy T model.

DIKÁTOVÁ LOGIKA. *Věta o úplnosti (úvod).*

› 1.) Užitím 2. dokážeme obměnu 1. Nechť tedy $T \nvdash \varphi$, a nechť $\overline{\varphi}$ je univerzální uzávěr φ. Ukážeme, že $T \cup \{\neg\overline{\varphi}\}$ je bezesporná; pak podle 2. má $T \cup \{\neg\overline{\varphi}\}$ model, tedy $T \nvDash \varphi$.

$T \cup \{\neg\overline{\varphi}\}$ je bezesporná: Předpokládejme naopak, že $T \cup \{\neg\overline{\varphi}\}$ je sporná. Pak

1)	$T \cup \{\neg\overline{\varphi}\} \vdash \overline{\varphi}$	$T \cup \{\neg\overline{\varphi}\}$ je sporná
2)	$T \vdash \neg\overline{\varphi} \to \overline{\varphi}$	věta o dedukci
3)	$\vdash (\neg\overline{\varphi} \to \overline{\varphi}) \to \overline{\varphi}$	$(A \to B) \to B$ je tautologie, viz pozn. 62
4)	$T \vdash \overline{\varphi}$	MP na 2), 3)
5)	$T \vdash \varphi$	opakovaně P4 a MP

Obdrželi jsme tedy spor s tím, že $T \nvdash \varphi$.

□

PREDIKÁTOVÁ LOGIKA. *Věta o úplnosti (úvod).*

Cílem dalšího postupu je dokázat, že každá bezesporná teorie má model. Tato konstrukce obsahuje dva základní obraty:

- Zavede se pojem *kanonické struktury* pro danou teorii T. Tato struktura obecně *není* modelem T. Ukážeme, že pokud T vyhovuje dalším podmínkám (je *henkinovská* a *úplná*), pak kanonická struktura *je* modelem T.
- Ukážeme, že každou bezespornou teorii je možné vhodným způsobem *rozšířit* tak, aby byla henkinovská a úplná.

DIKÁTOVÁ LOGIKA. *Rozšíření teorie.*

nice 67.

Teorie S je rozšíření teorie T, jestliže jazyk teorie S obsahuje jazyk teorie T a v teorii S jsou dokazatelné všechny axiómy teorie T.

Rozšíření S teorie T se nazývá konzervativní, jestliže každá formule azyka teorie T, která je dokazatelná v S, je dokazatelná i v T.

Teorie S a T jsou ekvivalentní, jestliže S je rozšířením T a současně T je rozšířením S.

PREDIKÁTOVÁ LOGIKA. *Věta o konstantách.*

Věta 68 (o konstantách). *Nechť S je rozšíření T vzniklé obohacením jazyka teorie T o nové navzájem různé konstanty $c_1, \cdots, c_k$ (nové axiómy nepřidáváme), a nechť $x_1, \cdots, x_k$ jsou navzájem různé proměnné. Pak pro každou formuli φ jazyka teorie T platí, že $T \vdash \varphi$ právě když $S \vdash \varphi(x_1/c_1, \cdots, x_k/c_k)$.*

Důkaz. Jelikož $c_1, \cdots, c_k$ jsou navzájem různé, stačí dokázat, že $T \vdash \varphi$ právě když $S \vdash \varphi(x/c)$.

$\Rightarrow$: K důkazu φ v T připojíme formule $\forall x\, \varphi$, $\forall x\, \varphi \to \varphi(x/c)$, $\varphi(x/c)$ a obdržíme tak důkaz formule $\varphi(x/c)$ v S.

$\Leftarrow$: Nechť $\psi_1, \cdots, \psi_k$ je důkaz $\varphi(x/c)$ v S. Nechť y je proměnná, která se nevyskytuje v tomto důkazu. Indukcí k i ukážeme, že pro každé $1 \le i \le k$ je $\psi_1(c/y), \cdots, \psi_i(c/y)$ důkaz v T. Rozlišíme tyto možnosti:

DIKÁTOVÁ LOGIKA. *Věta o konstantách.*

Je-li ψ_i instancí P1–P5 (příp. R1–R3), je také $\psi_i(c/y)$ instancí téhož schématu.

Je-li ψ_i axióm teorie T, pak se v ψ_i nevyskytuje c a formule ψ_i a $\psi_i(c/y)$ sou tedy totožné.

Jestliže ψ_i vyplývá z ψ_j a ψ_m pomocí MP, je ψ_m tvaru $\psi_j \to \psi_i$ a formule $\psi_m(c/y)$ je tedy formulí $\psi_j(c/y) \to \psi_i(c/y)$. Takže formule $\psi_i(c/y)$ yplývá z $\psi_j(c/y)$ a $\psi_m(c/y)$ pomocí MP.

Jestliže ψ_i vyplývá z ψ_j pomocí GEN, je ψ_i tvaru $\forall x\, \psi_j$. Stačí si uvědomit, že $(\forall x\, \psi_j)(c/y)$ je tatáž formule jako $\forall x\, (\psi_j(c/y))$, neboť x a y sou různé.

PREDIKÁTOVÁ LOGIKA. *Věta o konstantách.*

Ukázali jsme, že $T \vdash \varphi(x/c)(c/y)$. Dále

1)	$T \vdash \varphi(x/y)$	$\varphi(x/y)$ je totéž co $\varphi(x/c)(c/y)$
2)	$T \vdash \forall y\, \varphi(x/y)$	GEN
3)	$\vdash \forall y\, \varphi(x/y) \to (\varphi(x/y)(y/x))$	P4
4)	$T \vdash \varphi(x/y)(y/x)$	MP na 2), 3)
5)	$T \vdash \varphi$	$\varphi(x/y)(y/x)$ je totéž co φ

□

DIKÁTOVÁ LOGIKA. *Henkinovské a úplné teorie.*

nice 69.

Teorie T je henkinovská, jestliže pro každou formuli φ jazyka teorie T s jednou volnou proměnnou x existuje v jazyce teorie T konstanta c aková, že $T \vdash \exists x\, \varphi \to \varphi(x/c)$.

Teorie T je úplná, jestliže je bezesporná a pro každou uzavřenou formuli φ jejího jazyka platí buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$.

PREDIKÁTOVÁ LOGIKA. *Henkinovské a úplné teorie.*

Věta 70 (o henkinovské konstantě). *Buď T teorie a $\varphi(x)$ formule jejího jazyka. Je-li S rozšíření T, které vznikne přidáním nové konstanty c_φ a formule $\exists x\, \varphi \to \varphi(x/c_\varphi)$, pak S je konzervativní rozšíření T.*

Důkaz. Nejprve ukážeme, že pro libovolnou formuli $\xi(x)$ platí $\vdash \exists x \xi \to \exists y \xi(x/y)$:

1)	$\{\forall y \neg\xi(x/y)\} \vdash \forall y \neg\xi(x/y)$	
2)	$\{\forall y \neg\xi(x/y)\} \vdash \neg\xi(x/y)(y/x)$	P4 a MP
3)	$\{\forall y \neg\xi(x/y)\} \vdash \neg\xi$	přepis
4)	$\{\forall y \neg\xi(x/y)\} \vdash \forall x \neg\xi$	GEN
5)	$\vdash \forall y \neg\xi(x/y) \to \forall x \neg\xi$	dedukce
6)	$\vdash \exists x \xi \to \exists y \xi(x/y)$	taut. $(A \to B) \to (\neg B \to \neg A)$ a MP.

nt’ R značí teorii vzniklou pouhým přidáním konstanty c_φ k T. Nechť ψ
rmule jazyka teorie T taková, že $S \vdash \psi$. Nechť y je proměnná, která se
skytuje ani ve φ, ani v ψ. Platí:

1)	$S \vdash \psi$	předpoklad
2)	$R \vdash (\exists x\varphi \to \varphi(x/c_\varphi)) \to \psi$	$S = R \cup \{\exists x\varphi \to \varphi(x/c_\varphi)\}$ a dedukce
3)	$T \vdash (\exists x\varphi \to \varphi(x/y)) \to \psi$	věta o konstantách
4)	$T \vdash \forall y((\exists x\varphi \to \varphi(x/y)) \to \psi)$	GEN
5)	$T \vdash \exists y(\exists x\varphi \to \varphi(x/y)) \to \psi$	*lema 64 (2)* a MP
6)	$\vdash (\exists x\varphi \to \exists y\varphi(x/y)) \to \exists y(\exists x\varphi \to \varphi(x/y))$	*lema 64 (3)*
7)	$T \vdash (\exists x\varphi \to \exists y\varphi(x/y)) \to \psi$	tranz. implikace
8)	$\vdash \exists x\varphi \to \exists y\varphi(x/y)$	dokázáno výše
9)	$T \vdash \psi$	MP

☐

Věta 71 (o henkinovském rozšíření). *Ke každé teorii existuje henkinovská teorie, která je jejím konzervativním rozšířením.*

Důkaz. Buď T (libovolná) teorie. Pro každé $n \geq 0$ definujeme teorii T_n takto:

- $T_0 = T$. Teorie T_{i+1} vznikne z T_i tak, že pro každou formuli $\varphi(x)$ jazyka teorie T_i přidáme novou konstantu c_φ a formuli $\exists x\varphi \to \varphi(x/c_\varphi)$.

Metaindukcí vzhledem k n ukážeme, že T_n je konzervativní rozšíření T.

- Pro $n = 0$ není co dokazovat. V indukčním kroku si stačí uvědomit, že je-li $T_{i+1} \vdash \psi$, může být v důkazu formule ψ použito jen *konečně mnoho* axiómů $\xi_1, \cdots, \xi_k$, které nepatří do T_i. Užitím věty o henkinovské konstantě k-krát po sobě dostáváme $T_i \vdash \psi$, proto $T \vdash \psi$ podle I.P.

Uvažme teorii $S = \bigcup_{n=0}^{\infty} T_n$. Teorie S je konzervativní rozšíření T, neboť každý důkaz v S používá jen konečně mnoho axiómů a je tedy důkazem v nějaké T_m. Teorie S je zjevně henkinovská. ☐

---

sledující větě předpokládáme existenci *dobrého* uspořádání na
boru všech uzavřených formulí daného jazyka. Je-li uvažovaný jazyk
početný, opírá se tento předpoklad o *axióm výběru*.

a 72 (o zúplňování teorií). *Ke každé bezesporné teorii existuje její
íření se stejným jazykem, které je úplnou teorií.*

az. Buď T teorie, a nechť $\preceq$ je *dobré* uspořádání na množině všech
řených formulí jazyka teorie T. Pro každou uzavřenou formuli φ
ka teorie T definujeme teorii T_φ induktivně takto:

Je-li φ nejmenší prvek v uspořádání $\preceq$, klademe $T_\varphi = T$,

$$\text{Jinak } T_\varphi = \begin{cases} \bigcup\limits_{\xi \prec \varphi} T_\xi \cup \{\varphi\} & \text{je-li } \bigcup\limits_{\xi \prec \varphi} T_\xi \cup \{\varphi\} \text{ bezesporná;} \\ \bigcup\limits_{\xi \prec \varphi} T_\xi \cup \{\neg\varphi\} & \text{jinak.} \end{cases}$$

Indukcí vzhledem k $\preceq$ dokážeme, že každé T_φ je bezesporné rozšíření T.

- Je-li φ nejmenší prvek v uspořádání $\preceq$, není co dokazovat.
- Indukční krok: Označme symbolem S teorii $\bigcup_{\xi \prec \varphi} T_\xi$.
  - Teorie S je nutně bezesporná. Jinak $S \vdash \psi \wedge \neg\psi$ pro nějakou formuli ψ. Jelikož tento důkaz používá jen konečně mnoho axiómů teorie S, nutně existuje $\xi \prec \varphi$ takové, že T_ξ obsahuje všechny použité axiómy. Proto $T_\xi \vdash \psi \wedge \neg\psi$, což je spor s IP.
  - Je-li $T_\varphi = S \cup \{\varphi\}$, je T_φ bezesporná.
  - Je-li $T_\varphi = S \cup \{\neg\varphi\}$, je teorie $S \cup \{\varphi\}$ sporná. Pokud by byla sporná také teorie $S \cup \{\neg\varphi\}$, platilo by $S \cup \{\varphi\} \vdash \neg\varphi$ a $S \cup \{\neg\varphi\} \vdash \varphi$, proto i $S \vdash \varphi \to \neg\varphi$ a $S \vdash \neg\varphi \to \varphi$ (užitím věty o dedukci). Z toho dostáváme $S \vdash \psi \wedge \neg\psi$ pro libovolné ψ, neboť $(A \to \neg A) \to ((\neg A \to A) \to (\psi \wedge \neg\psi))$ je výroková tautologie (použijeme 2x MP). Tedy i S je sporná, což je spor s předchozím bodem.

DIKÁTOVÁ LOGIKA. *Henkinovské a úplné teorie.*

zme teorii U která vznikne sjednocením všech T_φ. Zjevně U je rozšíření
má stejný jazyk jako T. Pokud by U byla sporná, existoval by důkaz
$\neg\psi$ v U. Tento důkaz využívá pouze konečně mnoho axiómů U, proto
$\neg\psi$ je dokazatelná i v nějaké T_φ, což je spor. □

PREDIKÁTOVÁ LOGIKA. *Kanonická struktura.*

Definice 73. *Buď T teorie, kde jazyk teorie T obsahuje alespoň jednu konstantu. Kanonická struktura teorie T je realizace $\mathcal{M}$ jazyka teorie T, kde*

- *univerzum M je tvořeno všemi uzavřenými termy jazyka teorie T;*
- *relizace funkčního symbolu f arity n je funkce f_M, která uzavřeným termům $t_1, \cdots, t_n$ přiřadí uzavřený term $f(t_1, \cdots, t_n)$;*
- *realizace predikátového symbolu P arity m je predikát P_M definovaný takto: $P_M(t_1, \cdots, t_m)$ platí právě když $T \vdash P(t_1, \cdots, t_m)$.*

DIKÁTOVÁ LOGIKA. *Kanonická struktura.*

74 (o kanonické struktuře). *Nechť T je úplná henkinovské teorie, a
ť jazyk teorie T je jazykem bez rovnosti. Pak kanonická struktura teorie
modelem T.*

az. Nechť $\mathcal{M}$ je kanonická struktura teorie T. Ukážeme, že pro
volnou formuli φ jazyka teorie T platí následující:

Jestliže $\hat\varphi$ je uzavřená instance formule φ, pak $T \vdash \hat\varphi$ právě když $\mathcal{M} \models \hat\varphi$.

kož lze (bez újmy na obecnosti) předpokládat, že prvky T jsou *uzavřené*
ule, plyne z výše uvedeného, že $\mathcal{M}$ je model T.

kcí ke struktuře φ:

$\varphi \equiv P(t_1, \cdots, t_n)$. Buď $P(t'_1, \cdots, t'_n)$ libovolná uzavřená instance. Podle
definice kanonické struktury $\mathcal{M} \models P(t'_1, \cdots, t'_n)$ právě když
$T \vdash P(t'_1, \cdots, t'_n)$.

PREDIKÁTOVÁ LOGIKA. *Kanonická struktura.*

- $\varphi \equiv \neg\psi$. Buď $\neg\hat\psi$ libovolná uzavřená instance. Jelikož $\hat\psi$ je uzavřená instance ψ, podle IP platí $T \vdash \hat\psi$ právě když $\mathcal{M} \models \hat\psi$. Dále $T \vdash \neg\hat\psi$ právě když $T \nvdash \hat\psi$ (T je bezesporná) právě když $\mathcal{M} \not\models \hat\psi$ (IP) právě když $\mathcal{M} \models \neg\hat\psi$.
- $\varphi \equiv \psi \rightarrow \xi$. Každá uzavřená instance této formule je tvaru $\hat\psi \rightarrow \hat\xi$, kde $\hat\psi$ je uzavřená instance ψ a $\hat\xi$ je uzavřená instance ξ.
  - → Nechť $T \vdash \hat\psi \rightarrow \hat\xi$. Jelikož $\hat\psi$ je uzavřená formule a T je uplná, platí buď $T \vdash \hat\psi$ nebo $T \vdash \neg\hat\psi$. V prvém případě dále $T \vdash \hat\xi$ (MP) a užitím IP celkem dostáváme $\mathcal{M} \models \hat\psi$ a $\mathcal{M} \models \hat\xi$. Proto také $\mathcal{M} \models \hat\psi \rightarrow \hat\xi$. V druhém případě $T \nvdash \hat\psi$ (T je bezesporná), proto $\mathcal{M} \not\models \hat\psi$ (IP), tudíž $\mathcal{M} \models \hat\psi \rightarrow \hat\xi$.
  - → Nechť $\mathcal{M} \models \hat\psi \rightarrow \hat\xi$. Pak buď $\mathcal{M} \not\models \hat\psi$ nebo $\mathcal{M} \models \hat\xi$. V prvém případě $T \nvdash \hat\psi$ podle IP, tudíž $T \vdash \neg\hat\psi$ neboť T je úplná. Proto $T \vdash \hat\psi \rightarrow \hat\xi$ užitím tautologie $\neg A \rightarrow (A \rightarrow B)$ a MP. V druhém případě $T \vdash \hat\xi$, proto $T \vdash \hat\psi \rightarrow \hat\xi$ užitím tautologie $A \rightarrow (B \rightarrow A)$ a MP.

$\varphi \equiv \forall x\, \psi$. Buď $\forall x\, \bar{\psi}$ libovolná uzavřená instance. Pak $\bar{\psi}(x)$, jinak by $\forall x\, \bar{\psi}$ nebyla uzavřená.

- Nechť $T \vdash \forall x\, \bar{\psi}$. Pak pro libovolný uzavřený term t platí $T \vdash \bar{\psi}(x/t)$ (P4 a MP). Podle IP $\mathcal{M} \models \bar{\psi}(x/t)$. Jelikož tento argument funguje pro *libovolný* uzavřený term t, platí také $\mathcal{M} \models \forall x\, \bar{\psi}$.
- Nechť $T \nvdash \forall x\, \bar{\psi}$. Pak také $T \nvdash \forall x \neg\neg\bar{\psi}$ (kdyby $T \vdash \forall x \neg\neg\bar{\psi}$, dostaneme dále $T \vdash \neg\neg\bar{\psi}$ (P4 a MP) a $T \vdash \bar{\psi}$ (tautologie $\neg\neg A \rightarrow A$ a MP), $T \vdash \forall x\, \bar{\psi}$ (GEN), spor).

  Jelikož $T \nvdash \forall x \neg\neg\bar{\psi}$, platí $T \vdash \neg\forall x \neg\neg\bar{\psi}$ neboť T je úplná. Tedy $T \vdash \exists x \neg\bar{\psi}$. Jelikož T je henkinovská, platí $T \vdash \exists x \neg\bar{\psi} \rightarrow \neg\bar{\psi}(x/c)$. Tedy $T \vdash \neg\bar{\psi}(x/c)$ a proto $T \nvdash \bar{\psi}(x/c)$ neboť T je bezesporná. Podle IP $\mathcal{M} \not\models \bar{\psi}(x/c)$, tedy $\mathcal{M} \models \neg\bar{\psi}(x/c)$. Proto $\mathcal{M} \not\models \forall x \bar{\psi}$.

□

Věta 75. *Nechť T je úplná henkinovské teorie, a nechť jazyk teorie T je jazykem s rovností. Pak T má model.*

Důkaz. Buď S teorie (s jazykem bez rovnosti), která vznikne rozšířením T o nový binární predikátový symbol $=$ a axiomy R1–R3. Symbol $=$ v teorii S je tedy *mimologický* a může být realizován „jakkoliv“. Axiomy R1–R3 jsou v S „normální“ axiómy. Stačí nám ukázat, že S má takový model, kde $=$ je realizován jako identita. Takový model pak jistě bude i modelem T (kde $=$ je chápáno jako logický symbol).

$\mathcal{M}$ kanonická struktura teorie S, a nechť $\sim$ je realizace $=$ v S (tj. $t_1 \sim t_2$ ě když $S \vdash t_1 = t_2$). Dokážeme, že $\sim$ je nutně ekvivalence:

reflexivita: $S \vdash x{=}x$ (R1), $S \vdash \forall x\, x{=}x$ (GEN), $S \vdash \forall x\, x{=}x \rightarrow t{=}t$ (P4), $S \vdash t{=}t$ MP). Tedy $t \sim t$.

symetrie: nechť $s \sim t$, tj. $S \vdash s{=}t$. Platí $S \vdash (x_1{=}y_1 \wedge x_2{=}y_2) \rightarrow (x_1{=}x_2 \rightarrow y_1{=}y_2)$ (R2, $=$ hraje i roli P). Užitím GEN, P4 a MP dostaneme $S \vdash (s{=}t \wedge s{=}s) \rightarrow (s{=}s \rightarrow t{=}s)$. Užitím MP dostaneme $S \vdash t{=}s$.

Tranzitivita: podobně.

Nyní již můžeme definovat strukturu $\mathcal{O}$ pro jazyk teorie S:

- Nosičem $\mathcal{O}$ jsou třídy rozkladu nosiče $\mathcal{M}$ podle $\sim$.
- Funkční symbol f arity n je realizován takto:

$$f_{\mathcal{O}}([t_1], \cdots, [t_n]) = [f_{\mathcal{M}}(t_1, \cdots, t_n)]$$

- Predikátový symbol P arity m je realizován takto:

$$P_{\mathcal{O}}([t_1], \cdots, [t_m]) \text{ právě když } P_{\mathcal{M}}(t_1, \cdots, t_m)$$

Korektnost této definice (tj. nezávislost na volbě reprezentantů) se dokáže pomocí R1–R3 podobným stylem jako výše. Snadno se ověří, že realizací uzavřeného termu t je ve struktuře $\mathcal{O}$ je $[s]$ právě když $S \vdash s{=}t$. To znamená, že predikátový symbol $=$ je v $\mathcal{O}$ realizován jako identita.

DIKÁTOVÁ LOGIKA. *Kanonická struktura.*

á ukázat, že $\mathcal{O}$ je modelem S. Podobně jako ve *větě 75* budeme chtít ázat, že pro libovolnou formuli $\varphi(x_1,\ldots,x_n)$ jazyka teorie S platí:

Jestliže $t_1,\cdots,t_n$ jsou uzavřené termy jazyka teorie S, pak $\vdash \varphi(x_1/t_1,\cdots,x_n/t_n)$ právě když $\mathcal{O} \models \varphi(x_1/[t_1],\cdots,x_n/[t_n])$.

ož S je henkinovská a úplná, platí podle *věty 75*

$\vdash \varphi(x_1/t_1,\cdots,x_n/t_n)$ právě když $\mathcal{M} \models \varphi(x_1/t_1,\cdots,x_n/t_n)$

í tedy ukázat, že

$\models \varphi(x_1/t_1,\cdots,x_n/t_n)$ právě když $\mathcal{O} \models \varphi(x_1/[t_1],\cdots,x_n/[t_n])$

ze lehce provést indukcí ke struktuře φ. □

PREDIKÁTOVÁ LOGIKA. *Věta o úplnosti.*

Kurt Gödel (1906–1978)

Věta 76 (o úplnosti, Kurt Gödel). *Každá bezesporná teorie má model. Pro každou teorii T a každou formuli jejího jazyka tedy platí, že jestliže $T \models \varphi$, pak $T \vdash \varphi$.*

Důkaz. Jde o jednoduchý důsledek předchozích vět. □

DIKÁTOVÁ LOGIKA. *Věta o kompaktnosti.*

77. *Teorie T má model, právě když každá její podteorie s konečně ha axiómy (a s minimálním jazykem, v němž jsou tyto axiómy ulovatelné) má model.*

az. Směr „⇒“ je triviální. Pro opačnou implikaci stačí ukázat, že T je sporná (pak T má model podle věty o úplnosti). Kdyby T byla sporná, oval by důkaz formule $\psi \wedge \neg\psi$ v T. Tento důkaz je konečný, využívá jen konečně mnoho axiómů T, které tvoří spornou podteorii T, . □

PREDIKÁTOVÁ LOGIKA. *Löwenheimova-Skolemova věta.*

Poznámka 78. *Z důkazu věty 71 plyne, že každá bezesporná teorie s jazykem bez rovnosti má model kardinality $\max\{|L|,\aleph_0\}$ (při rozšíření teorie na henkinovskou bylo přidáno $|L|\cdot\aleph_0$ nových konstant). Toto pozorování neplatí pro teorie s jazykem s rovností (např. pro $T=\{\forall x\, x{=}c\}$. Nicméně lze dokázat následující:*

Věta 79. *Nechť T je teorie a nechť pro každé $n \in \mathbb{N}$ existuje model teorie T jehož nosič má mohutnost alespoň n. Pak T má nekonečný model.*

Důkaz. Je-li jazyk teorie T jazykem bez rovnosti, plyne tvrzení ihned z *poznámky 78*. Jinak pro každé $n \in \mathbb{N}$ definujeme formuli $\varphi_n \equiv \forall x_1 \cdots \forall x_n \exists y\; x_1{\neq}y \wedge \cdots \wedge x_n{\neq}y$ a teorii $S_n = T \cup \{\varphi_1,\cdots,\varphi_n\}$. Podle předpokladu věty má každá S_n model. Podle věty o kompaktnosti má proto model i teorie $\bigcup_{i=1}^{\infty} S_n$. Tento model je nutně nekonečný a je i modelem teorie T. □

DIKÁTOVÁ LOGIKA. *Löwenheimova-Skolemova věta.*

a **80** (Löwenheimova-Skolemova). *Nechť T je teorie s jazykem L, která nekonečný model. Nechť κ je nekonečný kardinál takový, že $\kappa \geq |L|$. Pak á model mohutnosti κ.*

az. Nechť $\mathcal{M}$ je nekonečný model T. Jazyk L rozšíříme o systém $i < \kappa\}$ nových konstant a k T přidáme axiómy $\{c_i \neq c_j \mid i, j < \kappa\}$. ržíme tak teorii T'. Nechť K je konečná část T', a nechť $c_1, \cdots, c_n$ jsou hny nově přidané konstanty, které se vyskytují ve formulích teorie K ových konstant je jen konečně mnoho). Pokud tyto konstanty zujeme navzájem různými prvky nosiče $\mathcal{M}$, obdržíme model teorie K. dá konečná část T' je tedy splnitelná. Podle věty o kompaktnosti má model i teorie T'. Nosič tohoto model ale nutně obsahuje alespoň κ ájem různých individuí. □

VĚTA O NEÚPLNOSTI. *Úvod.*

- *Jazyk aritmetiky* je jazyk s rovností obsahující konstantu 0, unární funkční symbol S a dva binární funkční symboly $*$ a $+$.
- Význačnou realizací jazyka aritmetiky je $(\mathbb{N}_0, *, +)$, kde univerzem je soubor všech nezáporných celých čísel, 0 je realizováno jako nula, S jako funkce následníka, $*$ jako násobení, $+$ jako sčítání. (Relační predikáty jako $<, \leq$ lze snadno definovat.)
- Jedním ze základních kroků *Hilbertova programu* formalizace matematiky mělo být vytvoření *rekurzivní a úplné* teorie T jazyka aritmetiky.
- Slovem „úplné“ se myslí, že $T \vdash \varphi$ právě když $\varphi \in Th(\mathbb{N}_0, *, +)$ (Tj. formule dokazatelné v T jsou právě formule pravdivé v $(\mathbb{N}_0, *, +)$).
- Slovo „rekurzívní“ intuitivně znamená, že musí být „mechanicky ověřitelné“, zda daná posloupnost symbolů je či není důkazem v T (možných formalizací tohoto pojmu je více).
- Z Gödelových výsledků plyne, že taková teorie neexistuje.

A O NEÚPLNOSTI. *Turingův stroj.*

Alan Turing (1912–1954)

- Definoval pojem Turingova stroje a s jeho pomocí ukázal, že problém pravdivosti formulí prvního řádu je *nerozhodnutelný*.
- Považován za zakladatele informatiky (jako vědy).
- Turingův stroj je matematickým modelem „hloupého odvozovače“, který má k dispozici papír, tužku a gumu, a který si pamatuje konečně mnoho schémat axiómů.
- Význam Turingova stroje coby modelu reálných výpočetních zařízení se projevil až v druhé polovině 20. století.

VĚTA O NEÚPLNOSTI. *Turingův stroj (neformálně).*

Základní pojmy:

- Je-li Σ konečná *abeceda*, značí symbol Σ^* soubor všech konečných slov složených z prvků Σ (prázdné slovo značíme symbolem ε). Délku slova w značíme $len(w)$. Pro každé $1 \leq i \leq len(w)$ značí symbol $w(i)$ i-tý znak slova w (zleva). *Jazyk* nad abecedou Σ je podmnožina Σ^*.
- *Turingův stroj* je matematický model výpočetního zařízení, které je vybaveno konečně-stavovou *řídící jednotkou* („hlava odvozovače“), jednosměrně nekonečnou *pracovní páskou* („papír“), a čtecí/zápisovou hlavou („tužka/guma“).
- Na začátku výpočtu je na pásce zapsáno konečné *vstupní slovo*, hlava je na nejlevější pozici, a stavová jednotka je v počátečním stavu.
- Stroj na základě svého momentálního kontrolního stavu a symbolu pod čtecí hlavou provede „výpočetní krok“, tj. změní svůj kontrolní stav, nahradí symbol pod čtecí hlavou jiným symbolem, a posune čtecí hlavu vlevo nebo vpravo.

TA O NEÚPLNOSTI. *Turingův stroj (neformálně).*

Výpočet se zastaví, pokud stroj dojde do konfigurace, jejíž kontrolní stav je *akceptující* nebo *zamítající*. Pro některá slova může stroj také nezastavit (cyklit).

Vstupní slovo je *akceptované*, jestliže stroj po konečně mnoha krocích dojde do akceptující konfigurace. Soubor všech vstupních slov, která stroj akceptuje, tvoří *jazyk akceptovaný daným strojem*.

VĚTA O NEÚPLNOSTI. *Turingův stroj (formálně).*

Definice 81. *Turingův stroj je devítice* $M = (Q, \Sigma, \Gamma, B, \bullet, \delta, q_0, \mathit{Acc}, \mathit{Rej})$, *kde*

- Q *je konečný soubor kontrolních stavů;*
- Σ *je konečná vstupní abeceda;*
- Γ *je konečná pásková abeceda (kde* $\Sigma \subseteq \Gamma$*);*
- $B \in \Gamma$ *je prázdný znak;*
- $\bullet \in \Gamma$ *je znak konce pásky;*
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$ *je přechodová funkce, kde pro každé* $p \in Q$ *platí* $\delta(p, \bullet) = (q, \bullet, R)$ *pro nějaké* $q \in Q$*;*
- $q_0 \in Q$ *je počáteční stav;*
- $\mathit{Acc} \subseteq Q$ *je množina akceptujících stavů;*
- $\mathit{Rej} \subseteq Q \setminus \mathit{Acc}$ *je množina zamítajících stavů.*

TA O NEÚPLNOSTI. *Turingův stroj (formálně).*

Nechť $\circ, \# \notin Q \cup \Gamma$, a nechť $\mathcal{C}(M) = (\Gamma \cup \{\#\}) \times (Q \cup \{\circ\})$. Prvky $\mathcal{C}(M)$ zapisujeme ve tvaru $[X, q]$.

Konfigurace stroje M je slovo $[X_1, p_1] \cdots [X_n, p_n]\,[\#, \circ] \in \mathcal{C}(M)^*$ takové, že $n \geq 1$, $X_1 = \bullet$, $X_i \neq \#$ pro každé $1 \leq i \leq n$, a existuje právě jedno $1 \leq j \leq n$, kde $p_j \in Q$. Slovo $X_1 \cdots X_n$ nazýváme *obsahem pásky* dané konfigurace, a stav p_j kontrolním stavem dané konfigurace.

Akceptující resp. *zamítající* konfigurace je konfigurace, jejíž kontrolní stav je akceptující resp. zamítající. *Koncová* konfigurace je konfigurace, která je akceptující nebo zamítající. Soubor všech konfigurací stroje M značíme $\mathit{Conf}(M)$.

Krok výpočtu je funkce $\mathit{step} : \mathit{Conf}(M) \to \mathit{Conf}(M)$, která je pro koncové konfigurace definována jako identita a pro nekoncové konfigurace takto:

- $\mathit{step}(\gamma\,[X, q]\,[Y, \circ]\,\rho) = \gamma\,[Z, \circ]\,[Y, r]\,\rho$ jestliže $\delta(q, Y) = (r, Z, R)$
- $\mathit{step}(\gamma\,[Y, \circ]\,[X, q]\,\rho) = \gamma[Z, \circ]\,[Y, r]\,\rho$ jestliže $\delta(q, Y) = (r, Z, L)$
- $\mathit{step}(\gamma\,[X, q]\,[\#, \circ]) = \gamma[Z, \circ]\,[B, r]\,[\#, \circ]$ jestliže $\delta(q, Y) = (r, Z, R)$

VĚTA O NEÚPLNOSTI. *Turingův stroj (formálně).*

- Nechť $w = a_1 \cdots a_n$ je slovo nad abecedou Σ (w může být i prázdné). *Iniciální konfigurace* pro w je konfigurace $\alpha(w) = [\bullet, q_0][a_1, \circ] \cdots [a_n, \circ]\,[\#, \circ]$. Slovo w je *akceptované* strojem M, jestliže existuje $k \in \mathbb{N}$ takové, že $\mathit{step}^k(\alpha(w))$ je akceptující konfigurace. *Jazyk* akceptovaný strojem M, označovaný $L(M)$, je soubor všech $w \in \Sigma^*$, které jsou akceptované strojem M.
- Nechť $([X_1, p_1], [X_2, p_2], [Y_1, q_1], [Y_2, q_2])$ je čtveřice symbolů z $\mathcal{C}(M)$. Tato čtveřice je *kompatibilní*, jestliže existuje nekoncová konfigurace $\alpha \in \mathit{Conf}(M)$ a vhodné $1 \leq i < \mathit{len}(\alpha)$ takové, že $\alpha(i) = [X_1, p_1]$, $\alpha(i{+}1) = [X_2, p_2]$ a dále $\beta(i) = [Y_1, q_1]$, $\beta(i{+}1) = [Y_2, q_2]$ kde $\beta = \mathit{step}(\alpha)$. Soubor všech kompatibilních čtveřic stroje M označme $\mathit{Comp}(M)$. Soubor $\mathit{Comp}(M)$ lze snadno „vypočítat“ na základě toho, jak vypadá přechodová funkce δ.
- Nechť $\alpha \in \mathit{Conf}(M)$ je konfigurace a nechť $\beta \in \mathcal{C}(M)^*$ je slovo stejné délky, jako má α. Pak $\beta = \mathit{step}(\alpha)$ právě když pro každé $1 \leq i < \mathit{len}(\alpha)$ platí, že $(\alpha(i), \alpha(i{+}1), \beta(i), \beta(i{+}1)) \in \mathit{Comp}(M)$.

A O NEÚPLNOSTI. *Vlastnosti jazyků.*

zavedeme několik pojmů, které se týkají jazyků.

Jazyk $L \subseteq \Sigma^*$ je *rekurzivně vyčíslitelný*, jestliže $L = L(M)$ pro nějaký Turingův troj M. Jazyk $L \subseteq \Sigma^*$ je *rekurzivní*, jestliže $L = L(M)$ pro nějaký Turingův stroj M, který zastaví pro *každé* vstupní slovo. Jednoduché pozorování je, že jazyk $\subseteq \Sigma^*$ je rekurzivní právě když L i $\overline{L}$ jsou rekurzivně vyčíslitelné (kde $\overline{L} = \Sigma^* \setminus L$).

Předpokládejme, že kontrolní stavy a symboly páskové abecedy *každého* uringova stroje jsou prvky nějaké fixní spočetné množiny (to lze bez újmy na obecnosti). Pak *každý* Turingův stroj M lze jednoznačně zapsat jako slovo $ode(M) \in \{0,1\}^*$. Podobně každé vstupní slovo w stroje M lze jednoznačně apsat jako slovo $code(w) \in \{0,1\}^*$. Navíc lze předpokládat, že *každé* $v \in \{0,1\}^*$ e kódem nějakého stroje M_v a nějakého vstupního slova w_v stroje M_v.

Jvedené kódování umožňuje zkonstruovat *univerzální* Turingův stroj U se rstupní abecedou $\{0,1,\#\}$ takový, že pro každé slovo tvaru $u\#v$, kde $u, v \in \{0,1\}^*$, latí, že U akceptuje $u\#v$ právě když stroj M_u akceptuje slovo w_v.

Jvažme jazyk $Accept = \{u\#v \mid M_u \text{ akceptuje } w_v\}$. Podle předchozího bodu je *ccept* rekurzivně vyčíslitelný. Ukážeme, že *Accept není rekurzivní*. Podle ednoho z předchozích bodů pak jazyk $\overline{Accept}$ *není rekurzivně vyčíslitelný*.

VĚTA O NEÚPLNOSTI. *Jazyk Accept.*

Věta 82. *Jazyk Accept není rekurzivní.*

Důkaz. Předpokládejme, že existuje Turingův stroj M, který zastaví pro každé vstupní slovo a $L(M) = Accept$. Buď M' stroj se vstupní abecedou $\{0,1\}$, který funguje následovně:

- M' pro dané vstupní slovo u nejprve „vyrobí“ na pásce slovo $u\#u$.
- Pak M' přesune čtecí hlavu úplně vlevo a dále se začne chovat jako stroj M s tím rozdílem, že se zamění akceptující a zamítající stavy.
- Výsledkem je, že $u \in L(M')$ právě když $u\#u \notin L(M)$

Nechť $v = code(M')$. Platí $w_v \in L(M')$?

- Ano. Pak $v\#v \notin L(M)$, tj. $M_v = M'$ neakceptuje w_v, spor.
- Ne. Pak $v\#v \in L(M)$, tj. $M_v = M'$ akceptuje w_v, spor.

Z předpokladu existence stroje M se nám podařilo odvodit spor. Stroj M tedy *neexistuje*. □

A O NEÚPLNOSTI. *Peanova aritmetika.*

ním z pokusů o vytvoření rekurzivní a úplné teorie aritmetiky byl edující systém nazývaný *Peanova aritmetika* (seznam Peanových mů bývá v literatuře uváděn v různých podobách):

$\forall x\ S(x) \neq 0$

$\forall x \forall y\ S(x){=}S(y) \to x{=}y$

$\forall x\ x{+}0 = x$

$\forall x \forall y\ x{+}S(y) = S(x{+}y)$

$\forall x\ x{*}0 = 0$

$\forall x \forall y\ x{*}S(y) = (x{*}y) + x$

$\varphi(0) \wedge \forall x\,(\varphi(x) \to \varphi(S(x)))) \to \forall x\,\varphi(x)$, kde φ je formule s jednou volnou roměnnou x.

VĚTA O NEÚPLNOSTI. *Peanova aritmetika.*

Každou formuli jazyka aritmetiky je možné zapsat jako slovo nad abecedou $\{v, +, *, 0, S, (,), \forall, \to, \neg, =, \#\}$. Různé proměnné zapisujeme jako řetězce složené z v různé délky (např. místo x, y, z můžeme psát v, vv, vvv apod.). Podobně můžeme i každou *konečnou* posloupnost formulí zapsat jako slovo nad uvedenou abecedou, kde symbol $\#$ použijeme pro oddělení jednotlivých formulí.

Definice 83. *Teorie T jazyka aritmetiky je rekurzivní, jestliže jazyk tvořený zápisy všech důkazů v T je rekurzivní.*

Lze snadno (i když technicky) dokázat, že např. Peanovy axiómy tvoří rekurzivní teorii. Definici rekurzivity teorie lze samozřejmě rozšířit i na teorie nad jinými jazyky. Rekurzivní teorie odpovídají (na intuitivní úrovni) právě teoriím, které umožňují „mechanické odvozování“. Triviální pozorování o rekurzivních teoriích podává následující věta.

Věta 84. *Nechť T je rekurzivní teorie jazyka aritmetiky. Pak jazyk tvořený všemi formulemi dokazatelnými v T je rekurzivně vyčíslitelný.*

A O NEÚPLNOSTI. *Jazyk Valid.*

ť *Valid* je jazyk nad abecedou $\{v,+,*,0,S,(,),\forall,\to,\neg,=\}$ obsahující zápisy všech
ulí teorie $Th(\mathbb{N}_0,*,+)$. Naším cílem je dokázat, že *Valid* *není* rekurzivně
litelný jazyk.

85. *Jazyk Valid není rekurzivně vyčíslitelný.*

z. Ukážeme, že existuje Turingův stroj M, který pro každé vstupní slovo v nad
edou $\{0,1,\#\}$ zastaví v konfiguraci, kdy je na pásce zápsáno slovo w nad
edou $\{v,+,*,0,S,(,),\forall,\to,\neg,=\}$ takové, že $v \in \overline{Accept}$ právě když $w \in Valid$.
d by tedy jazyk *Valid* byl akceptovaný nějakým strojem M', stačilo by „napojit
e M a M' za sebe“ a dostali bychom stroj akceptující jazyk $\overline{Accept}$, což je spor.

VĚTA O NEÚPLNOSTI. *Jazyk Valid.*

Stroj M nejprve „prověří“ vstupní slovo: pokud není tvaru $u\#v$, M smaže vstupní pásku a zapíše na ní (nějakou) pravdivou formuli. Jinak M „nalezne“ prvočíslo p, takové, že $p > |C(M_u)|$. Pozorování:

- Jestliže zapisujeme čísla v soustavě o základu p, potřebujeme p „číslic“ $[0],\cdots,[p-1]$. Každému symbolu z $C(M_u)$ lze tedy přiřadit jedinečnou „číslici“. Dále nebudeme rozlišovat mezi symboly souboru $C(M_u)$ a jim přiřazenými číslicemi.
- Každé konfiguraci stroje M_u pak odpovídá číslo v soustavě o základu p. Zápis tohoto čísla získáme tak, že symboly konfigurace zapíšeme v opačném pořadí. Např. konfiguraci $[\bullet,\circ]\,[X,\circ]\,[Y,q]\,[Z,\circ]\,[B,\circ]\,[C,\circ]\,[C,\circ]\,[\#,\circ]$ zapíšeme jako číslo
$$[\#,\circ]\,[C,\circ]\,[C,\circ]\,[B,\circ]\,[Z,\circ]\,[Y,q]\,[X,\circ]\,[\bullet,\circ]$$
- M_u akceptuje slovo w_v právě když existuje *konečná* posloupnost konfigurací $\alpha_0,\alpha_1,\cdots,\alpha_n$ s následujícími vlastnostmi:
  - → α_0 je počáteční konfigurace pro slovo w_v.
  - → $\alpha_{i+1} = step(\alpha_i)$ pro každé $0 \le i < n$
  - → α_n je akceptující.

A O NEÚPLNOSTI. *Jazyk Valid.*

Bez újmy na obecnosti můžeme předpokládat, že zápisy konfigurací
$\alpha_0,\alpha_1,\cdots,\alpha_n$ mají *stejnou délku*. (Zápisy „krátkých“ konfigurací lze „doplnit“
zprava symboly $[B,\circ]$, zapsanými těsně před symbol $[\#,\circ]$.)

Posloupnost konfigurací $\alpha_0,\alpha_1,\cdots,\alpha_n$ lze tedy opět zapsat jako číslo v soustavě
o základu p. Zápis tohoto čísla vypadá takto: $[\alpha_n]\,[\alpha_{n-1}]\cdots[\alpha_0]$, kde $[\alpha_i]$ je zápis
konfigurace α_i tak, jak bylo popsáno výše.

Sestrojíme formuli $ACOMP(y)$, která říká, že y reprezentuje akceptující výpočet
stroje M_u na slově w_v. Tj. $ACOMP(y/k)$ platí právě když zápis čísla k v p-ární
soustavě je zápisem akceptující výpočetní posloupnosti stroje M_u na slově w_v.

Konstrukce $ACOMP(y)$ je „algoritmická“, tj. realizovatelná strojem M. Ten tuto
formuli „vypočte“, na pásku zapíše formuli $\neg\exists y\, ACOMP(y)$ a přejde do
akceptujícího stavu.

VĚTA O NEÚPLNOSTI. *Jazyk Valid.*

- Formuli $ACOMP(y)$ setrojíme postupně takto:
  - → „Číslo y je mocninou p.“ (Zde p je prvočíslo vypočtené výše.)
$$POWER_p(y) \equiv \forall z((DIV(z,y) \wedge PRIME(z)) \to z{=}p)$$
  - → „V p-árním zápisu v se na $\log_p(y)$-tém místě zprava vyskytuje symbol $[b]$“. (Předpokládáme, že y je mocnina p)
$$DIGIT(v,y,b) \equiv \exists u\, \exists a\, (v{=}a{+}by{+}upy \ \wedge\ a{<}y \ \wedge\ b{<}p)$$
  - → „V p-árním zápisu v tvoří dvojice po sobě jdoucích symbolů od pozice $\log_p(y)$ zprava následovaná dvojicí po sobě jdoucích symbolů od pozice $\log_p(z)$ zprava kompatibilní čtveřici.“ (Předpokládáme, že y i z jsou mocniny p.)
$$MATCH(v,y,z) \quad \equiv \bigvee_{([a],[b],[c],[d])\in Comp(M_u)} DIGIT(v,y,a) \wedge DIGIT(v,yp,b) \wedge\ DIGIT(v,z,c) \wedge DIGIT(v,zp,d)$$
  - → „V p-árním zápisu v se prvních $\log_p(d)$ znaků shoduje se zápisem výpočtu stroje M_u na slově w_v, kde délka zápisu konfigurací je $\log_p(c)$. (Předpokládáme, že d i c jsou mocniny p.)“
$$MOVE(v,c,d) \equiv \forall y\, ((POWER_p(y) \ \wedge\ ypc{<}d) \to MATCH(v,y,yc))$$

A O NEÚPLNOSTI. *Jazyk Valid.*

- „V p-árním zápisu v je jako první (zprava) zapsána konfigurace

$$[\bullet, q_0]\,[a_1,\circ]\cdots[a_n,\circ]\,[B,\circ]\cdots[B,\circ]\,[\#,\circ]$$

kde $w_v = a_1 \cdots a_n$ a délka této kofigurace je $\log_p(c) - 1$.“ (Předpokládáme, že c je mocnina p.)

$$\begin{aligned} \mathit{START}(v,c) \quad\equiv\quad & p^{n+1} < c \ \wedge\ \mathit{DIGIT}(v,1,[\bullet,q_0]) \ \wedge \\ & \bigwedge_{i=1}^{n} \mathit{DIGIT}(v,p^i,[a_i,\circ]) \ \wedge \\ & \exists k\,(c = pk \ \wedge\ \mathit{DIGIT}(v,k,[\#,\circ]) \ \wedge \\ & \quad \forall y\,((\mathit{POWER}_p(y) \ \wedge\ p^{n+1}{<}y{<}c) \rightarrow \mathit{DIGIT}(v,y,[B,\circ])) \end{aligned}$$

- „V p-árním zápisu v se vyskytuje symbol s akceptujícím kontrolním stavem.“ (Předpokládáme, že d je mocnina p.) Nechť H je soubor všech p-árních číslic tvaru $[X,q]$, kde $X \in \Gamma$ a q je akceptující kontrolní stav stroje M_u.

$$\mathit{ACC}(v,d) \equiv \exists y\,(\mathit{POWER}_p(y) \ \wedge\ y{<}d \ \wedge \bigvee_{[a]\in H} \mathit{DIGIT}(v,y,a))$$

VĚTA O NEÚPLNOSTI. *Jazyk Valid.*

- „p-ární zápis v je zápisem akceptujícího výpočtu stroje M_u na slově w_v.“

$$\begin{aligned} \mathit{ACOMP}(v) \quad\equiv\quad & \exists c\,\exists d\,(\mathit{POWER}_p(c) \ \wedge\ \mathit{POWER}_p(c) \ \wedge\ c{<}d \ \wedge\ v{<}d \\ & \wedge\ \mathit{START}(v,c) \ \wedge\ \mathit{MOVE}(v,c,d) \ \wedge\ \mathit{ACC}(v,d)) \end{aligned}$$

- Výše uvedená konstrukce závisí jen na „jednoduchých“ parametrech stroje M_u (prvočíslo p, soubor $\mathit{Comp}(M_u)$, apod.) a stroj M je dokáže snadno „zjistit“ z kódu stroje M_u.

☐

A O NEÚPLNOSTI. *Gödelův důkaz.*

álním důsledkem *věty 84* a *věty 85* je následující:

86 (o neúplnosti). *Neexistuje žádná rekurzivní teorie jazyka*
netiky, ve které jsou dokazatelné právě všechny formule pravdivé
alizaci $(\mathbb{N}_0,+,*)$. Speciálně pro každou korektní teorii T (tj. takovou teorii,
á umožnuje dokázat pouze formule pravdivé v $(\mathbb{N}_0,+,*)$, nutně existuje
ule platná v $(\mathbb{N}_0,+,*)$), která není v T dokazatelná.

86 bývá v literatuře také označována jako *první věta o neúplnosti*.
odní Gödelova formulace této věty (a zejména její důkaz) vypadá
sně. Klíčové obraty v Gödelově konstrukci si nyní naznačíme. V této
i se slovem „formule“ myslí *formule jazyka aritmetiky*.

VĚTA O NEÚPLNOSTI. *Gödelův důkaz.*

Nechť PA značí teorii Peanovy aritmetiky, a nechť $\mathcal{N}$ značí realizaci $(\mathbb{N}_0,+,*)$ jazyka aritmetiky. Formule jsou konečná slova nad abecedou $\{v,+,*,0,S,(,),\forall,\rightarrow,\neg,=\}$ a lze je tedy kódovat *čísly* stejným způsobem jako konfigurace Turingových strojů. Pro každou formuli φ označíme symbolem $\lceil\varphi\rceil$ číslo, které je jejím kódem.

Lema 87 (Gödelovo lema o pevném bodě). *Pro každou formuli $\psi(x)$ existuje uzavřená formule τ taková, že $\mathit{PA} \vdash \tau \leftrightarrow \psi(\lceil\tau\rceil)$. (Formule τ říká „ψ platí pro můj kód“.)*

Důkaz. (osnova) Pro libovolnou fixní proměnnou x_0 lze sestrojit formuli $\mathit{SUBST}(x,y,z)$, která říká následující:

- „Číslo z je kódem formule, kterou získáme substitucí proměnné x_0 za konstantu s hodnotou x ve formuli s kódem y.“

Např. $\mathit{SUBST}(5,\lceil\varphi(x_0)\rceil,413)$ je pravdivá právě když $\lceil\varphi(5)\rceil = 413$. Konstrukce formule $\mathit{SUBST}(x,y,z)$ je technická; lze použít podobný přístup jako při konstrukci formule ACOMP v důkazu *věty 85*.

A O NEÚPLNOSTI. *Gödelův důkaz.*

definujeme

$$\sigma(x) \;\equiv\; \forall y\,(\mathit{SUBST}(x,x,y) \to \psi(y))$$

$$\tau \;\equiv\; \sigma(\ulcorner\sigma(x_0)\urcorner)$$

me, že τ má požadovanou vlastnost:

$$\tau \;\equiv\; \sigma(\ulcorner\sigma(x_0)\urcorner) \;\equiv\; \forall y\,(\mathit{SUBST}(\ulcorner\sigma(x_0)\urcorner,\ulcorner\sigma(x_0)\urcorner,y) \to \psi(y))$$

$\mathcal{N} \models \forall y\,(\mathit{SUBST}(\ulcorner\sigma(x_0)\urcorner,\ulcorner\sigma(x_0)\urcorner,y) \to \psi(y))$ právě když
$\mathcal{N} \models \forall y\,(y = \ulcorner\sigma(\ulcorner\sigma(x_0)\urcorner)\urcorner \to \psi(y))$

$$\forall y\,(y = \ulcorner\sigma(\ulcorner\sigma(x_0)\urcorner)\urcorner \to \psi(y)) \;\equiv\; \forall y\,(y = \ulcorner\tau\urcorner \to \psi(y))$$

$\mathcal{N} \models \forall y\,(y = \ulcorner\tau\urcorner \to \psi(y))$ právě když $\mathcal{N} \models \psi(\ulcorner\tau\urcorner)$

chozí argument se opírá o *sémantickou* ekvivalenci jistých formulí; ekvivalence
o formulí je ale ve skutečnosti *dokazatelná v PA*. Např.

$$PA \vdash (\forall y\,(y = \ulcorner\tau\urcorner \to \psi(y))) \leftrightarrow \psi(\ulcorner\tau\urcorner)$$

e třeba v posledním bodu. Proto $PA \vdash \tau \leftrightarrow \psi(\ulcorner\tau\urcorner)$. □

VĚTA O NEÚPLNOSTI. *Gödelův důkaz.*

Věta 88 (1. věta o neúplnosti, Gödelova). *Lze sestrojit uzavřenou formuli ρ, která je pravdivá v $\mathcal{N}$, ale není dokazatelná v PA.*

Důkaz. (osnova) Ukáže se, že i důkazy (tj. konečné posloupnosti formulí) je možné kódovat čísly, a že existuje formule $\mathit{PROOF}(x,y)$, která říká, že x je kódem důkazu (v PA) pro formuli s kódem y. Dokazatelnost v PA lze pak zapsat formulí

- $\mathit{PROVABLE}(y) \;\equiv\; \exists x\, \mathit{PROOF}(x,y)$

Pak pro každou uzavřenou formuli φ platí

- $PA \vdash \varphi$ právě když $\mathcal{N} \models \mathit{PROVABLE}(\ulcorner\varphi\urcorner)$

Dále lze ukázat

- $PA \vdash \varphi$ právě když $PA \vdash \mathit{PROVABLE}(\ulcorner\varphi\urcorner)$

Směr „$\Leftarrow$“ plyne ihned z korektnosti PA (indukcí se snadno ukáže, že jestliže $PA \vdash \varphi$, pak $\mathcal{N} \models \varphi$). Opačný směr je výrazně pracnější.

Nyní stačí aplikovat *lema 87* na formuli $\neg\mathit{PROVABLE}(x)$. Dostaneme tak sentenci ρ takovou, že platí

- $PA \vdash \rho \leftrightarrow \neg\mathit{PROVABLE}(\ulcorner\rho\urcorner)$

A O NEÚPLNOSTI. *Gödelův důkaz.*

ule ρ tedy říká *„já nejsem dokazatelná“*, přičemž toto tvrzení je v PA
zatelné. Z korektnosti PA dostáváme, že

$$\mathcal{N} \models \rho \leftrightarrow \neg\mathit{PROVABLE}(\ulcorner\rho\urcorner)$$

ale musí platit $\mathcal{N} \models \rho$; kdyby totiž $\mathcal{N} \models \neg\rho$, dostaneme $\mathcal{N} \models \mathit{PROVABLE}(\ulcorner\rho\urcorner)$,
$PA \vdash \rho$ a tedy $\mathcal{N} \models \rho$, spor.

ož $\mathcal{N} \models \rho$, platí $\mathcal{N} \models \neg\mathit{PROVABLE}(\ulcorner\rho\urcorner)$, tedy $\mathcal{N} \not\models \mathit{PROVABLE}(\ulcorner\rho\urcorner)$, proto $PA \nvdash \rho$.

ule ρ je tedy pravdivá v $\mathcal{N}$, ale není dokazatelná v PA. □

VĚTA O NEÚPLNOSTI. *Kódování tvrzení o PA v PA.*

Pozorování:

- Důkaz *věty 88* se opírá o možnost vyjádřit jistá *matatvrzení* o formulích aritmetiky a teorii PA jako formule aritmetiky. Typicky lze takto vyjádřit tvrzení, která se týkají *dokazatelnosti*.
  - Metatvrzení „$PA \vdash \varphi$“ lze vyjádřit formulí $\mathit{PROVABLE}(\ulcorner\varphi\urcorner)$. Dokonce platí $PA \vdash \varphi$ právě když $PA \vdash \mathit{PROVABLE}(\ulcorner\varphi\urcorner)$.
  - I metatvrzení „$PA \vdash \varphi$ právě když $PA \vdash \mathit{PROVABLE}(\ulcorner\varphi\urcorner)$“ lze vyjádřit v PA pomocí formule

    $$\mathit{PROVABLE}(\ulcorner\varphi\urcorner) \leftrightarrow \mathit{PROVABLE}(\ulcorner\mathit{PROVABLE}(\ulcorner\varphi\urcorner)\urcorner)$$

    I tato formule je v PA dokazatelná.
  - *Bezespornost* teorie PA lze vyjádřit formulí $\mathit{CONSIS} \equiv \neg\mathit{PROVABLE}(\ulcorner\xi \wedge \neg\xi\urcorner)$, kde ξ je (nějaká) formule.

A O NEÚPLNOSTI. *Kódování tvrzení o PA v PA.*

Jsou ale i metatvrzení o formulích aritmetiky, která jako formule aritmetiky výjádřit *nelze*. Typicky se jedná o tvrzení týkající se *pravdivosti*.

→ Tvrzení „$\mathcal{N} \models \varphi$“ jako formuli aritmetiky vyjádřit nelze: Předpokládejme naopak, že existuje formule $\mathit{TRUE}(x)$ taková, že $\mathcal{N} \models \varphi$ právě když $\mathcal{N} \models \mathit{TRUE}(\lceil\varphi\rceil)$. Pak podle *lematu 87* existuje sentence τ taková, že $\mathcal{N} \models \tau$ právě když $\mathcal{N} \models \neg\mathit{TRUE}(\lceil\tau\rceil)$. Ovšem podle výše uvedeného platí $\mathcal{N} \models \tau$ právě když $\mathcal{N} \models \mathit{TRUE}(\lceil\tau\rceil)$, což je spor.

VĚTA O NEÚPLNOSTI. *Druhá věta o neúplnosti.*

Úvahy o vyjádřitelnosti některých vlastností teorie PA formulemi aritmetiky hrají klíčovou roli v důkazu následujícího tvrzení:

Věta 89 (2. věta o neúplnosti, Gödelova)**.** *Je-li PA bezesporná, pak CONSIS není v PA dokazatelná. (Jinými slovy: v „dostatečně silné“ teorii lze dokázat její vlastní bezespornost jen v případě, že je tato teorie sporná.)*

Důkaz. (osnova) Nechť ρ je formule zkonstruovaná v důkazu *věty 88* (která o sobě říká, že je nedokazatelná). Uvažme následující metatvrzení:

→ „Jestliže $\mathit{PA} \vdash \rho$, pak platí $\mathit{PA} \vdash \mathit{PROVABLE}(\lceil\rho\rceil)$ a současně $\mathit{PA} \vdash \neg\mathit{PROVABLE}(\lceil\rho\rceil)$“

Toto tvrzení je nejen pravdivé, ale lze ho vyjádřit formulí aritmetiky, která je navíc *dokazatelná* v PA:

→ $\mathit{PA} \vdash \mathit{PROVABLE}(\lceil\rho\rceil) \rightarrow (\mathit{PROVABLE}(\lceil\mathit{PROVABLE}(\lceil\rho\rceil)\rceil) \wedge \mathit{PROVABLE}(\lceil\neg\mathit{PROVABLE}(\lceil\rho\rceil)\rceil))$

Proto platí také $\mathit{PA} \vdash \mathit{PROVABLE}(\lceil\rho\rceil) \rightarrow \neg\mathit{CONSIS}$.

A O NEÚPLNOSTI. *Druhá věta o neúplnosti.*

ěnou uvedeného tvrzení dostáváme

$\mathit{A} \vdash \mathit{CONSIS} \rightarrow \neg\mathit{PROVABLE}(\lceil\rho\rceil)$

y $\mathit{PA} \vdash \mathit{CONSIS}$, platilo by také $\mathit{PA} \vdash \neg\mathit{PROVABLE}(\lceil\rho\rceil)$ (aplikací MP). Už dříve ale ukázali (viz důkaz *věty 88*), že

$\mathit{A} \vdash \rho \leftrightarrow \neg\mathit{PROVABLE}(\lceil\rho\rceil)$

aplikací MP tedy dostáváme $\mathit{PA} \vdash \rho$. Výše jsme ale ukázali, že předpoklad ρ implikuje, že PA je sporná. Celkem tedy dostáváme, že předpoklad CONSIS implikuje, že PA je sporná. □

tuitivní úrovni: druhá věta o neúplnosti říká, že bezespornost „dostatečně“ teorie (např. teorie množin) *nelze v této teorii dokázat*. Jediná možnost je ít *metaargumenty*, tj. zdůvodnit bezespornost dané teorie pomocí teorie „vyšší“. ezespornost této vyšší teorie není ovšem možno prokázat v ní samé. Na nějaké ni nám prostě nezbývá, než v bezespornost *uvěřit*, resp. ji *předpokládat*. lovy výsledky o neúplnosti mají tedy i svůj *epistemologický* význam.