IB000 Úvod do informatiky — příklady na procvičení

Sada 9 — Řešení

Upozornění

Vzorová řešení dostáváte k dispozici, abyste mohli zkontrolovat správnost svých řešení. Můžete je použít i jako návody k řešení jednotlivých příkladů tak, že je budete číst po částech a budete se snažit další krok provést vždy sami. Příklady ztratí veškerý svůj smysl, pokud se je budete učit jako básničku. Snažte se nad nimi přemýšlet a vyřešit je sami, než se podíváte do vzorových řešení.

Téma

Induktivně definované množiny, jednoznačné induktivní definice, induktivně definované funkce z induktivně definovaných množin. Strukturální indukce.

Příklad 1.

Nechť $M \subseteq \mathbb{N}_0$ je induktivně definována takto:

- $0 \in M$
- jestliže $x \in M$, potom $x + 4 \in M$

a) Zapište formálně funkce induktivních pravidel této definice.
b) Platí $129 \in M$? Platí $65 \in M$?
c) Množinu M zapište explicitně, tj. ve tvaru $M = \{\ldots\}$.
d) Je tato definice jednoznačná? Svou odpověď zdůvodněte.

Řešení

a) Tato definice má jediné induktivní pravidlo, které je určeno funkcí $f : M \to M$, $f(x) = x + 4$ pro každé $x \in M$.
b) Platí $129 \notin M$ a $65 \notin M$. Protože induktivní pravidlo je rostoucí v tom smyslu, že větší číslo je prvkem množiny M na základě toho, že nějaké menší číslo je prvkem množiny M, stačí začít se základním prvkem množiny M a aplikovat induktivní pravidlo tak dlouho, dokud nedojdeme alespoň k číslu 129. Pokud číslo 129 odvodíme, potom $129 \in M$. Pokud odvodíme číslo větší než 129, aniž bychom předtím odvodili 129, potom $129 \notin M$. Pro číslo 129 by příslušná sekvence byla

$$0, 4, 8, 12, \ldots, 124, 128, 132$$

takže $129 \notin M$. Analogicky bychom argumentovali pro $65 \notin M$.
c) $M = \{4n \mid n \in \mathbb{N}_0\}$ Důkaz indukcí ponecháváme čtenáři. Jako návod poslouží analogické důkazy, které provedeme u dalších, složitějších příkladů. Důkaz správnosti explicitního vyjádření spočívá v důkazu rovnosti dvou množin. Musíme již tedy znát jak induktivní definici množiny, tak její explicitní vyjádření. Není jasné, jak jsme explicitní vyjádření určili.

Algoritmus neexistuje. S trochou zkušeností u těchto jednoduchých příkladů použijete metodu „podívám se a vidím“. Když se podíváte a nevidíte, zpravidla pomůže, když začnete s bázovými prvky a systematicky vypíšete nejsnáze odvoditelné prvky množiny, aniž byste vznikající výrazy zjednodušovali. V tomto příkladě by takovou posloupností bylo

$$\begin{aligned}0 &\in M\\ 0+4 &\in M\\ 0+4+4 &\in M\\ 0+4+4+4 &\in M\end{aligned}$$

Nyní už si můžete všimnout toho, že

$$\begin{aligned}0 &= 4\cdot 0\\ 0+4 &= 4\cdot 1\\ 0+4+4 &= 4\cdot 2\\ 0+4+4+4 &= 4\cdot 3\end{aligned}$$

a pokud si alespoň na intuitivní úrovni uvědomujete důkaz indukcí, který budete muset provést, dojdete k závěru, že budou postupně vznikat všechny násobky čísla 4. Jedná se vlastně o stejný mechanismus, jako je určování tranzitivního obalu relace.

d) Ano, tato definice je jednoznačná, protože množina má jediný bázový prvek a definice má jediné „rostoucí" induktivní pravidlo.

Příklad 2.

Nechť $M \subseteq \mathbb{N}_0$ je induktivně definována takto:

- $0 \in M$
- jestliže $x \in M$, potom $x+3 \in M$ a $x+5 \in M$
- jestliže $x, y \in M$, potom $xy \in M$

a) Zapište formálně funkce induktivních pravidel této definice.
b) Platí $127 \in M$? Platí $17 \in M$?
c) Množinu M zapište explicitně, tj. ve tvaru $M = \{\ldots\}$.
d) Je tato definice jednoznačná? Svou odpověď dokažte.
e) Rozhodněte, zda platí tvrzení

$$\exists m \in \mathbb{N}_0.\ \forall n \in \mathbb{N}_0.\ m \leq n \Rightarrow n \in M$$

a správnost svého rozhodnutí dokažte.

Řešení

a) Tato definice má ve skutečnosti tři induktivní pravidla, kterým odpovídají následující funkce:

$f_1 : M \to M$, $f_1(x) = x+3$ pro každé $x \in M$
$f_2 : M \to M$, $f_2(x) = x+5$ pro každé $x \in M$
$f_3 : M \times M \to M$, $f_3(x,y) = xy$ pro každá dvě $x, y \in M$

b) Pokud chceme ověřit, že nějaké $n \in \mathbb{N}$ patří do induktivně definované množiny M, musíme jej *odvodit*. Odvozením se rozumí taková posloupnost prvků M končící číslem n, že každý prvek posloupnosti je buď bázovým prvkem M, nebo vznikne z předchozích prvků posloupnosti a nějakého induktivního pravidla. Jedná se vlastně o podobný výpočet zdola nahoru, jako při výpočtu hodnoty formule pro danou valuaci.

Odvození ukážeme pro číslo 17.

$0 \in M$	(i)	bázový prvek M
$3 \in M$	(ii)	z (i) a funkce f_1
$6 \in M$	(iii)	z (ii) a funkce f_1
$9 \in M$	(iv)	z (iii) a funkce f_1
$12 \in M$	(v)	z (iv) a funkce f_1
$17 \in M$	(vi)	z (v) a funkce f_2

Tedy $17 \in M$. Podobně, jen delším odvození, bychom ověřili, že $127 \in M$. Opakovanou aplikací pravidla určeného funkcí f_1 bychom odvodili, že $117 \in M$, odkud bychom dvojnásobnou aplikací pravidla určeného funkcí f_2 dospěli k $127 \in M$.

c) Určení explicitního vyjádření množiny si můžete usnadnit, pokud se přesvědčíte, že nepracujete se „zbytečnými“ induktivními pravidly a bázovými prvky. Bázový prvek je „zbytečný“, pokud je možné jej odvodit pomocí induktivních pravidel z jiných bázových prvků. Induktivní pravidlo je zbytečné, pokud je možné jej nahradit posloupností jiných induktivních pravidel. Zbytečné bázové prvky a zbytečná induktivní pravidla je možné z našich úvah dočasně vynechat, aniž bychom změnili množinu, s jejíž definicí pracujeme.

Na rozdíl od bázových prvků může být explicitní vyjádření a důkaz toho, že induktivní pravidlo je zbytečné, poměrně komplikované. Často je lepší se spolehnout na intuitivní odhad a korektnost odhadu ověřit až při důkazu rovnosti množin. Připomeňme, že se jedná o „virtuální“ úpravy, které nám mají usnadnit nalezení explicitního vyjádření množiny. Důkazu korektnosti explicitního vyjádření se nevyhneme.

Je také důležité, abyste při postupném označování bázových prvků a induktivních pravidel jako „zbytečných“ neoznačili bázový prvek nebo induktivní pravidlo, které jste již dříve použili k označení jiného prvku nebo pravidla. Potom by se definovaná množina změnila.

V naší induktivní definici je zbytečné induktivní pravidlo, které je určeno funkcí f_3. Při vypisování nejsnáze odvoditelných prvků množiny M jej proto nebudeme uvažovat. Prvky jsme již upravili do tvaru, z nějž je dobře vidět jejich explicitní vyjádření. Systematicky prozkoumáváme všechny možnosti aplikací funkcí f_1 a f_2 podle celkového počtu jejich aplikací.

$$\begin{aligned}
0 &= 3 \cdot 0 + 5 \cdot 0 \in M \\
3 &= 3 \cdot 1 + 5 \cdot 0 \in M \\
5 &= 3 \cdot 0 + 5 \cdot 0 \in M \\
6 &= 3 \cdot 2 + 5 \cdot 0 \in M \\
8 &= 3 \cdot 1 + 5 \cdot 1 \in M \\
10 &= 3 \cdot 0 + 5 \cdot 2 \in M \\
9 &= 3 \cdot 3 + 5 \cdot 0 \in M \\
11 &= 3 \cdot 2 + 5 \cdot 1 \in M \\
13 &= 3 \cdot 1 + 5 \cdot 2 \in M \\
15 &= 3 \cdot 0 + 5 \cdot 3 \in M
\end{aligned}$$

Odtud již můžeme uhádnout, že $M = \{3k+5l \mid k, l \in \mathbb{N}_0\}$. Dokážeme, že je toto explicitní vyjádření množiny M správné.

Označme M_1 induktivně definovanou množinu a $M_2 = \{3k+5l \mid k,l \in \mathbb{N}_0\}$. Musíme dokázat rovnost množin $M_1 = M_2$.

Nejprve dokažme, že $M_1 \subseteq M_2$. Důkaz můžeme vést strukturální indukci, protože dokazujeme tvrzení $\forall x \in M_1.\ x \in M_2$.

Základní krok: x je bázový prvek M_1. Tedy $x = 0 = 3 \cdot 0 + 5 \cdot 0 \in M_2$.

Indukční krok: pravidlo určené funkcí f_1. Nechť pro $x \in M_1$ platí $x \in M_2$ (toto je indukční předpoklad). Musíme dokázat, že $f_1(x) = x+3 \in M_2$. Z indukčního předpokladu víme, že $x \in M_2$, tedy $x = 3k+5l$ pro nějaká $k,l \in \mathbb{N}_0$. Potom $x+3 = 3(k+1)+5l \in M_2$, což jsme měli dokázat.

Indukční krok: pravidlo určené funkcí f_2. Nechť pro $x \in M_1$ platí $x \in M_2$ (toto je indukční předpoklad). Musíme dokázat, že $f_2(x) = x+5 \in M_2$. Z indukčního předpokladu víme, že $x \in M_2$, tedy $x = 3k+5l$ pro nějaká $k,l \in \mathbb{N}_0$. Potom $x+5 = 3k+5(l+1) \in M_2$, což jsme měli dokázat.

Indukční krok: pravidlo určené funkcí f_3. Nechť pro $x,y \in M_1$ platí $x \in M_2$ a $y \in M_2$ (toto je indukční předpoklad). Musíme dokázat, že $f_3(x,y) = xy \in M_2$. Z indukčního předpokladu víme, že $x \in M_2$, tedy $x = 3k_1+5l_1$ pro nějaká $k_1,l_1 \in \mathbb{N}_0$. Dále z indukčního předpokladu víme, že $y \in M_2$, tedy $y = 3k_2 + 5l_2$ pro nějaká $k_2,l_2 \in \mathbb{N}_0$. Potom $xy = (3k_1 + 5l_1)(3k_2 + 5l_2) = 3(3k_1k_2 + 5k_1l_2 + 5k_2l_1) + 5(5l_1l_2) \in M_2$, což jsme měli dokázat.

Nyní dokažme, že $M_2 \subseteq M_1$. Intuitivně je tvrzení zřejmé: nechť $3k + 5l \in M_2$ pro nějaká $k,l \in \mathbb{N}_0$. Potom $3k + 5l \in M_1$, protože jej získáme k-násobnou aplikací funkce f_1 a l-násobnou aplikací funkce f_2 na bázový prvek $0 \in M_1$. My však budeme pečliví a uvedeme formální důkaz.

Dokazujeme tvrzení $\forall k \in \mathbb{N}_0.\ \forall l \in \mathbb{N}_0.\ 3k + 5l \in M_1$. Důkaz povedeme indukcí vzhledem k $n = k + l$.

Základní krok: $n = 0$. Potom $k = l = 0$ a $3k + 5l = 0 \in M_1$, protože 0 je bázový prvek M_1.

Indukční krok: $k + l = n + 1$. Rozlišíme dvě možnosti.

Pokud $k > 0$, potom $(k-1) + l = n$ a z indukčního předpokladu víme, že $3(k-1) + 5l \in M_1$. Aplikací pravidla určeného funkcí f_1 na $3(k-1) + 5l$ dostáváme $3(k-1) + 5l + 3 = 3k + 5l \in M_1$, což jsme měli dokázat.

Pokud $l > 0$, potom $k + (l-1) = n$ a z indukčního předpokladu víme, že $3k + 5(l-1) \in M_1$. Aplikací pravidla určeného funkcí f_2 na $3k + 5(l-1)$ dostáváme $3k + 5(l-1) + 5 = 3k + 5l \in M_1$, což jsme měli dokázat.

d) Definice jednoznačná není. Jako protipříklad uvedeme jiné odvození $17 \in M$, než které jsme uvedli výše.

$0 \in M$	(i)	bázový prvek M
$3 \in M$	(ii)	z (i) a funkce f_1
$8 \in M$	(iii)	z (ii) a funkce f_2
$11 \in M$	(iv)	z (iii) a funkce f_1
$14 \in M$	(v)	z (iv) a funkce f_1
$17 \in M$	(vi)	z (v) a funkce f_1

e) Přirozeným jazykem řečeno se zajímáme o to, zda od nějakého přirozeného čísla jsou všechna větší přirozená čísla prvkem množiny M. Pokud tvrzení platí, nejsnazší způsob, jak jej dokázat, může spočívat v nalezení onoho čísla m a důkazu, že $\forall n \in \mathbb{N}_0.\ m \leq \leq n \Rightarrow n \in M$ pro naše konkrétní m. Pokud tvrzení neplatí, nejsnazší způsob, jak jej dokázat, může spočívat ve stanovení předpisu, který ke každému přirozenému číslu m stanoví větší přirozené číslo n, které není prvkem M.

Tvrzení platí. Dokážeme, že každé přirozené číslo větší než nějaké určité přirozené číslo můžeme vyjádřit ve tvaru $3k + 5l$, kde $k, l \in \mathbb{N}_0$. Nejprve ukážeme, jak ve tvaru $3k + 5l$ vyjádřit čísla od 20 do 24 včetně.

$$\begin{aligned}
20 &= 3 \cdot 0 + 5 \cdot 4 \\
21 &= 3 \cdot 7 + 5 \cdot 0 \\
22 &= 3 \cdot 4 + 5 \cdot 2 \\
23 &= 3 \cdot 1 + 5 \cdot 4 \\
24 &= 3 \cdot 8 + 5 \cdot 0
\end{aligned}$$

Nechť $n \in \mathbb{N}_0$, $n \geq 20$. Nechť $n = 5q + r$, kde $q, r \in \mathbb{N}_0$, $0 \leq r < 5$. (Tj. r je zbytek z n po dělení číslem 5.) Protože $n \geq 20$, platí $q \geq 4$. Potom $n = 5(q - 4) + (20 + r)$, kde $20 \leq 20 + r \leq 24$, takže platí $20 + r = 3k + 5l$, kde k a l je určeno výše uvedenou tabulkou. Celkem dostáváme $n = 5(q - 4) + 3k + 5l = 3k + 5(l + q - 4) \in M$.

Tvrzení tedy platí, protože jsme dokázali, že za m můžeme položit například číslo 20.

Příklad 3.

Uvažujme induktivně definovanou množinu $M \subseteq \mathbb{N}_0$

- $0 \in M$, $1 \in M$
- jestliže $x \in M$, potom $2x \in M$

Tato induktivní definice je zřejmě jednoznačná, takže funkce $f : M \to \mathbb{N}_0$ je korektně určena následující induktivní definicí

- $f(0) = \perp$, $f(1) = 0$
- $f(2x) = f(x) + 1$

a) Ukažte všechny kroky výpočtu hodnoty $f(256)$ podle této induktivní definice.
b) Ukažte všechny kroky výpočtu hodnoty $f(192)$ podle této induktivní definice.
c) Množinu M zapište explicitně.
d) S využitím explicitního vyjádření prvků množiny M zapište explicitně i funkci f, tj. pro každé $n \in M$ stanovte hodnotu $f(n)$.

Řešení

a) Hodnota $f(m)$ je definována induktivně v závislosti na struktuře prvku $m \in M$. Jedná se tedy o analogii funkcí $\mathcal{F}$ a $\mathcal{G}$ pro normalizaci formulí výrokové a predikátové logiky. Výpočet proto bude také analogický. Rozdíl je pouze v tom, že u formulí byla struktura zřejmá z jejich zápisu. U čísel budeme muset jejich strukturu hledat. Jednoznačnost induktivní definice množiny M zajišťuje že bude vždy existovat právě jedna možnost, jak číslo rozložit na strukturálně jednodušší čísla.

$$\begin{aligned}
&f(256) = f(2 \cdot 128) \\
&= f(128) + 1 = f(2 \cdot 64) \\
&= (f(64) + 1) + 1 = (f(2 \cdot 32) + 1) + 1 \\
&= ((f(32) + 1) + 1) + 1 = ((f(2 \cdot 16) + 1) + 1) + 1
\end{aligned}$$

$$
\begin{aligned}
&= (((f(16) + 1) + 1) + 1) + 1 = (((f(2 \cdot 8) + 1) + 1) + 1) + 1 \\
&= ((((f(8) + 1) + 1) + 1) + 1) + 1 = ((((f(2 \cdot 4) + 1) + 1) + 1) + 1) + 1 \\
&= (((((f(4) + 1) + 1) + 1) + 1) + 1) + 1 \\
&= (((((f(2 \cdot 2) + 1) + 1) + 1) + 1) + 1) + 1 \\
&= ((((((f(2) + 1) + 1) + 1) + 1) + 1) + 1) + 1 \\
&= ((((((f(2 \cdot 1) + 1) + 1) + 1) + 1) + 1) + 1) + 1 \\
&= (((((((f(1) + 1) + 1) + 1) + 1) + 1) + 1) + 1) + 1 \\
&= (((((((0 + 1) + 1) + 1) + 1) + 1) + 1) + 1) + 1 \\
&= 8
\end{aligned}
$$

b) Zadání v tomto případě samozřejmě nemá smysl, protože $192 \notin M$ a funkce f pro něj není definována. Pokud byste se pokusili o výpočet, dostali byste

$$
\begin{aligned}
&f(192) = f(2 \cdot 96) \\
&= f(96) + 1 = f(2 \cdot 48) + 1 \\
&= (f(48) + 1) + 1 = (f(2 \cdot 24) + 1) + 1 \\
&= ((f(24) + 1) + 1) + 1 = ((f(2 \cdot 12) + 1) + 1) + 1 \\
&= (((f(12) + 1) + 1) + 1) + 1 = (((f(2 \cdot 6) + 1) + 1) + 1) + 1 \\
&= ((((f(6) + 1) + 1) + 1) + 1) + 1 = ((((f(2 \cdot 3) + 1) + 1) + 1) + 1) + 1 \\
&= ((((f(3) + 1) + 1) + 1) + 1) + 1
\end{aligned}
$$

Není jasné, jak pokračovat s výpočtem $f(3)$, protože číslo 3 není ani bázový prvek M, ani jej není možné rozložit na strukturálně jednodušší prvky M.

c) Opět vypíšeme několik prvních prvků množiny M.

$$
\begin{aligned}
0 &\in M \\
1 = 2^0 &\in M \\
2 \cdot 1 = 2^1 &\in M \\
2 \cdot 2 \cdot 1 = 2^2 &\in M \\
2 \cdot 2 \cdot 2 \cdot 1 = 2^3 &\in M \\
2 \cdot 2 \cdot 2 \cdot 2 \cdot 1 = 2^4 &\in M
\end{aligned}
$$

Je vidět, že kromě čísla 0 budou všechny prvky množiny M tvaru 2^i pro nějaké přirozené číslo i. Platí tedy $M = \{0\} \cup \{2^i \mid i \in \mathbb{N}_0\}$. Důkaz ponecháváme čtenáři.

d) Indukcí vzhledem k i by bylo snadné dokázat, že $f(2^i) = i$ platí pro všechna $i \in \mathbb{N}_0$. Pokud to spojíme s tím, že hodnota $f(0)$ není definována, můžeme hodnotu $f(n)$ pro libovolné $n \in M$ explicitně zapsat takto:

$$
f(n) = \begin{cases} \perp & \text{pokud } n = 0 \\ i & \text{pokud } n = 2^i \text{ pro nějaké } i \in \mathbb{N}_0 \end{cases}
$$

Musíme upozornit na to, že jsme se zde dopustili malé nepřesnosti. Vzhledem k tomu, že jsme f definovali jako parciální funkci, aby odpovídala logaritmu na přirozených číslech s nulou, nestačí ke korektnosti její induktivní definice, aby byla induktivní definice množiny M jednoznačná. Využili jsme i toho, že z bázového prvku 0 nelze odvodit žádný jiný prvek M. Jinak bychom museli říct, co znamená například $\perp + 1$.

Příklad 4.

Množinu $\mathbb{N}_0 \subseteq \mathbb{N}_0$ definujme následující induktivní definicí:

- $0 \in \mathbb{N}_0$
- jestliže $n \in \mathbb{N}_0$, potom $n + 1 \in \mathbb{N}_0$

Induktivně definujte funkce

a) $f : \mathbb{N}_0 \to \mathbb{N}_0$, $f(n) = n + 3$

b) $f : \mathbb{N}_0 \to \mathbb{N}_0$, $f(n) = n^2 + 3n + 1$

c) $f : \mathbb{N}_0 \to \mathbb{N}_0$, $f(n) = 2^{n+1} - 1$

d) $f : \mathbb{N}_0 \to \{\text{sudé}, \text{liché}\}$

$$f(n) = \begin{cases} \text{sudé} & \text{pokud } n \text{ je sudé} \\ \text{liché} & \text{jinak} \end{cases}$$

Řešení

Nechť je úkolem explicitně zadanou funkci $f : A \to B$ definovat induktivně, pokud je množina A zadána jednoznačnou induktivní definicí. Pro základní krok definice f stačí podle explicitního zadání f vypočítat její hodnotu pro bázové prvky z induktivní definice A. Nechť je induktivní pravidlo definice A určeno funkcí $g : A^n \to A$. Induktivní pravidlo definice f odpovídající tomuto pravidlu definice A můžeme určit tak, že pomocí explicitního zadání funkce f se pokusíme upravit $f(g(x_1, \ldots, x_n))$ na $h(f(x_1), \ldots, f(x_n))$. Hodnotu $f(g(x_1, \ldots, x_n))$ tedy vyjádříme v závislosti na hodnotách funkce f aplikované na strukturálně jednodušší prvky A. To může být velmi obtížné, nebo to nemusí být vůbec možné.

Induktivní definice množiny $\mathbb{N}_0$ obsahuje jediný bázový prvek a jediné induktivní pravidlo. Podle výše uvedeného postupu tedy vždy nejprve provedeme dva výpočty (pro bázový a induktivní krok definice f) a potom zapíšeme induktivní definici funkce f.

a) Výpočty:

$$\begin{aligned} f(0) &= 0 + 3 = 3 \\ f(n+1) &= (n+1) + 3 = (n+3) + 1 = f(n) + 1 \end{aligned}$$

Induktivní definice f:

- $f(0) = 3$
- $f(n+1) = f(n) + 1$

b) Výpočty:

$$\begin{aligned} f(0) &= 0^2 + 3 \cdot 0 + 1 = 1 \\ f(n+1) &= (n+1)^2 + 3(n+1) + 1 = n^2 + 3n + 1 + 2n + 4 = f(n) + 2n + 4 \end{aligned}$$

Induktivní definice f:

- $f(0) = 1$
- $f(n+1) = f(n) + 2n + 4$

Použití n v induktivním kroku definice f je možné, protože se jedná o funkci, jejíž definiční obor je totožný s oborem hodnot. U obecné funkce $f : A \to B$ by to samozřejmě možné nebylo.

c) Výpočty:

$$f(0) = 2^{0+1} - 1 = 1$$
$$f(n+1) = 2^{(n+1)+1} - 1 = 2 \cdot 2^{n+1} - 1 = 2(2^{n+1} - 1) + 1 = 2f(n) + 1$$

Induktivní definice f:

- $f(0) = 1$
- $f(n+1) = 2 \cdot f(n) + 1$

d) Zde si výpočty odpustíme. Nula je jistě sudé číslo. Pokud k sudému číslu přičteme jedničku, získáme číslo liché. Pokud naopak přičteme jedničku k lichému číslu, získáme číslo sudé.

Induktivní definice f:

- $f(0) = \text{sudé}$
- $f(n+1) = \begin{cases} \text{sudé} & \text{pokud } f(n) = \text{liché} \\ \text{liché} & \text{jinak} \end{cases}$

Příklad 5.

Mějme množinu (abecedu) $\Sigma = \{a\}$. Konečným posloupnostem prvků (znaků) Σ budeme pro stručnost říkat slova nad abecedou Σ. Prázdnou posloupnost (prázdné slovo, slovo délky 0) budeme značit ε. Uvědomte si, že ε je metasymbol, zejména $\varepsilon \notin \Sigma$. Množinu $\Sigma^* \subseteq \Sigma^*$ všech slov nad abecedou Σ definujme induktivně takto:

- $\varepsilon \in \Sigma^*$
- jestliže $w \in \Sigma^*$, potom $wa \in \Sigma^*$.

Tato definice je jednoznačná. Všimněte si podobnosti této definice s induktivní definicí množiny přirozených čísel. Induktivně definujme funkci $l : \Sigma^* \to \mathbb{N}_0$, která bude počítat délku slova nad abecedou Σ.

- $l(\varepsilon) = 0$
- $l(wa) = l(w) + 1$

Uvažujme funkci $S : \Sigma^* \to \Sigma^*$ definovanou induktivně takto:

- $S(\varepsilon) = a$
- $S(wa) = S(w).aaa$

Nechť $w \in \Sigma^*$. Pomocí funkce l charakterizujte, co počítá funkce S, tj. stanovte, co musí splňovat $u, v \in \Sigma^*$, aby platilo $S(u) = v$ a své tvrzení dokažte (strukturální indukcí).

Příklad 6.

Nechť Σ je konečná množina symbolů.

a) Podejte jednoznačnou induktivní definici množiny Σ^* všech konečných posloupností symbolů z množiny Σ.

b) Nechť $w_1, w_2 \in \Sigma^*$. Definujte induktivně množinu všech slov nad abecedou Σ, která obsahují podslovo w_1 nebo w_2. Strukturální indukcí dokažte, že je definice správně.

c) S využitím jednoznačné induktivní definice množiny Σ^* z předchozí části tohoto příkladu pro každé $a \in \Sigma$ induktivně definujte funkci $\#_a : \Sigma^* \to \mathbb{N}_0$, která pro každé slovo $w \in \Sigma^*$ vrátí počet symbolů a ve slově w. Strukturální indukcí dokažte, že je funkce definována správně.

Příklad 7.

Nechť $\Sigma = \{a, b, c\}$. Uvažujme množinu $M \subseteq \Sigma^*$ danou následující induktivní definicí

- $ba, bc, cb, ab \in M$
- jestliže $x, y \in M$ a $x = au$ a $y = va$ pro nějaká $u, v \in \Sigma^*$, potom $xy \in M$
- jestliže $x, y \in M$ a $x = ub$ a $y = bv$ pro nějaká $u, v \in \Sigma^*$, potom $xy \in M$

a) Rozhodněte, zda $abbacbba \in M$, $cbbccbba \in M$, $abbccbba \in M$, $abbabccbabba \in M$. Svá tvrzení zdůvodněte.

b) Reverzí slova $w \in \Sigma^*$, $w = a_1 \dots a_n$, kde $a_i \in \Sigma$ pro každé $i = 1, \dots, n$, rozumíme slovo $w^R = a_n \dots a_1$. Například reverzí slova *abbc* je slovo *cbba*.
Strukturální indukcí dokažte, že pro každé $w \in M$ platí $w^R \in M$, tj. že množina M je uzavřená na reverzi slov.

Řešení

Pro stručnost budeme induktivní pravidla označovat jako pravidlo 1 a pravidlo 2 podle pořadí, v němž jsou uvedena.

a) Platí $cbbccbba \notin M$. Slovo mohlo vzniknout pouze použitím pravidla 2 a to dvěma způsoby: *cb.bccbba* nebo *cbbccb.ba*. Slovo *bccbba*, resp. *cbbccb* mohlo opět vzniknout pouze použitím pravidla 2 a to jediným způsobem: *bccb.ba*, resp. *cb.bccb*. Ovšem $bccb \notin M$, takže neexistuje odvození slova *cbbccbba*.

Platí $abbabccbabba \notin M$. Zde je rozbor možností příliš pracný, než abychom jej zde uváděli. Alternativně lze využít skutečnosti, že obě pravidla slova striktně prodlužují. Je tedy snadné systematicky odvodit všechna slova délky 12 a přesvědčit se, že mezi nimi slovo *abbabccbabba* není.

Platí $abbacbba, abbccbba \in M$. Odvození obou slov provedeme zároveň.

ab	$\in M$	(i)	bázový prvek M
ba	$\in M$	(ii)	bázový prvek M
bc	$\in M$	(iii)	bázový prvek M
cb	$\in M$	(iv)	bázový prvek M
$abba$	$\in M$	(v)	z (i), (ii) a pravidla 1
$abbc$	$\in M$	(vi)	z (i), (iii) a pravidla 2
$cbba$	$\in M$	(vii)	z (iv), (ii) a pravidla 2
$abbacbba$	$\in M$	(viii)	z (v), (vii) a pravidla 1
$abbccbba$	$\in M$	(ix)	z (vi), (vii) a pravidla 1

b) *Základní krok: ab.* Platí $(ab)^R = ba$, což je bázový prvek a tedy $(ab)^R \in M$.
Základní krok: ba. Platí $(ba)^R = ab$, což je bázový prvek a tedy $(ba)^R \in M$.
Základní krok: bc. Platí $(bc)^R = cb$, což je bázový prvek a tedy $(bc)^R \in M$.
Základní krok: cb. Platí $(cb)^R = bc$, což je bázový prvek a tedy $(cb)^R \in M$.
Indukční krok: pravidlo 1. Nechť $x, y \in M$, $x = au$ a $y = va$ pro nějaká $u, v \in \Sigma^*$. Z indukčního předpokladu plyne, že také $x^R = u^R.a \in M$ a $y^R = a.v^R \in M$. Proto

$$(xy)^R = (auva)^R = (a.v^R).(u^R.a) \in M$$

Indukční krok: pravidlo 2. Nechť $x, y \in M$, $x = ub$ a $y = bv$ pro nějaká $u, v \in \Sigma^*$. Z indukčního předpokladu plyne, že také $x^R = b.u^R \in M$ a $y^R = v^R.b \in M$. Proto

$$(xy)^R = (ubbv)^R = (v^R.b).(b.u^R) \in M$$

Příklad 8.

Nechť M je množina. Nechť $X, Y \subseteq M$ jsou induktivně definované množiny se společnou množinou $B \subseteq M$ bázových prvků, přičemž $f_1, \ldots, f_m$ jsou funkce induktivních pravidel z definice X a $g_1, \ldots, g_n$ jsou funkce induktivních pravidel z definice Y.
Nechť má induktivně definovaná množina $Z_1 \subseteq M$ množinu bázových prvků X a funkce induktivních pravidel $g_1, \ldots, g_n$.
Nechť má induktivně definovaná množina $Z_2 \subseteq M$ množinu bázových prvků Y a funkce induktivních pravidel $f_1, \ldots, f_m$.
Rozhodněte, zda platí $Z_1 = Z_2$ a své tvrzení dokažte.

Příklad 9.

Nechť M je množina. Nechť $X, Y \subseteq M$ jsou *jednoznačně* induktivně definované množiny. Nechť $B_X \subseteq M$ je množina bázových prvků definice X a nechť $B_Y \subseteq M$ je množina bázových prvků definice Y. Nechť definice X a Y mají společné funkce induktivních pravidel $f_1, \ldots, f_n$.
Nechť má induktivně definovaná množina $S \subseteq M$ množinu bázových prvků $B_X \cap B_Y$ a funkce induktivních pravidel $f_1, \ldots, f_n$.
Nechť má induktivně definovaná množina $T \subseteq M$ množinu bázových prvků $B_X \cup B_Y$ a funkce induktivních pravidel $f_1, \ldots, f_n$.

a) Rozhodněte, zda je množina S definována jednoznačně. Své tvrzení dokažte.
b) Rozhodněte, zda je množina T definována jednoznačně. Své tvrzení dokažte.
c) Rozhodněte, zda platí $S = X \cap Y$ a své tvrzení dokažte. Co můžeme na základě tohoto výsledku říct o případě, v němž bychom nepožadovali, aby definice množin X a Y byly jednoznačné?
d) Rozhodněte, zda platí $T = X \cup Y$ a své tvrzení dokažte. Co můžeme na základě tohoto výsledku říct o případě, v němž bychom nepožadovali, aby definice množin X a Y byly jednoznačné?

Příklad 10.

V závěrečném příkladě této sady se seznámíte s obecnějším pojetím induktivních definic, kdy je navzájem provázána definice více množin, resp. funkcí. U funkcí jste se s tím už v omezené míře setkali. Definice funkcí $\mathcal{F}$ a $\mathcal{G}$, které převádějí logické formule do normálního tvaru, jsou také provázány, ale obě funkce mají stejný definiční obor.
Nechť jsou množiny $A, B, C \subseteq \{\mathtt{0}, \mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}, \mathtt{5}, \mathtt{6}, \mathtt{7}, \mathtt{8}, \mathtt{9}, \mathtt{(}, \mathtt{)}, \mathtt{*}, \mathtt{+}\}^*$ definovány induktivně takto (všimněte si typografického vyznačení, že se jedná o symboly, z nichž budeme vytvářet slova, nikoliv o čísla a operace s nimi):

- $\{\mathtt{0}, \mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}, \mathtt{5}, \mathtt{6}, \mathtt{7}, \mathtt{8}, \mathtt{9}\} \subseteq A$
- jestliže $t \in C$, potom $\mathtt{(}t\mathtt{)} \in A$
- $A \subseteq B$
- jestliže $x \in B$ a $y \in A$, potom $x\mathtt{*}y \in B$

- $B \subseteq C$
- jestliže $x \in B$ a $y \in C$, potom x+$y \in C$

Nechť $X = \{\texttt{0}, \texttt{1}, \texttt{2}, \texttt{3}, \texttt{4}, \texttt{5}, \texttt{6}, \texttt{7}, \texttt{8}, \texttt{9}, \texttt{T}, \texttt{P}\}$. Nechť $u, v \in X^*$. Zřetězení slov u a v budeme značit $u \,.\, v$, pokud by zápis uv vedl k nejasnostem. Uvažme funkce $M_A : A \to X^*$, $M_B : B \to X^*$ a $M_C : C \to X^*$ definované induktivně takto:

- $M_A(k) = k$ pro $k \in \{\texttt{0}, \texttt{1}, \texttt{2}, \texttt{3}, \texttt{4}, \texttt{5}, \texttt{6}, \texttt{7}, \texttt{8}, \texttt{9}\}$
- $M_A(\texttt{(}t\texttt{)}) = M_C(t)$
- $M_B(t) = M_A(t)$ pro $t \in A$
- $M_B(x\texttt{*}y) = M_B(x) \,.\, M_A(y) \,.\, \texttt{T}$
- $M_C(t) = M_B(t)$ pro $t \in B$
- $M_C(x\texttt{+}y) = M_B(x) \,.\, M(C) \,.\, \texttt{P}$

a) Rozhodněte, zda platí `8+9` $\in C$, `(8+9)` $\in C$, `4+15+0` $\in C$, `3+2` $\in A$, `(3+2+4*7)` $\in A$, `3*(2+2)` $\in B$, `3*2+2` $\in B$, `(3*2)+2` $\in B$, `3*2+2` $\in C$.
b) Ukažte všechny kroky výpočtu $M_C($`1+2+3+4*5*6*7*8`$)$.
c) Ukažte všechny kroky výpočtu $M_C($`1*(2+3*4+5*6)*7+8*9`$)$.
d) Umíte říct, co je množina C a co počítá funkce M_C?