Matematická logika (povídání k šesté. sérii)

Hlavním předmětem studia matematické logiky je obecný pohled na matematické teorie. Každá teorie má svůj jazyk a své axiomy. **Jazykem** se myslí seznam všech povolených symbolů (relačních, funkčních, konstant a operací), **axiomy** jsou nějaká tvrzení, která prohlásíme za pravdivá. Chceme-li něco v takové teorii dokázat, vycházíme z axiomů a logickým postupem se snažíme dobrat k dokazovanému tvrzení. Samozřejmě, budujeme-li takto rozsáhlejší teorii, můžeme vycházet i z dříve dokázaných tvrzení.

Uvedu zde příklad teorie uspořádání s nejmenším prvkem (TUSNP). Jazyk obsahuje relační symboly $\preccurlyeq$, $=$ a konstantu $\bot$. Axiomy této teorie jsou následující:

(1) $a \preccurlyeq a$
(2) $a \preccurlyeq b \ \&\ b \preccurlyeq a \ \Rightarrow\ a = b$
(3) $a \preccurlyeq b \ \&\ b \preccurlyeq c \ \Rightarrow\ a \preccurlyeq c$
(4) $\bot \preccurlyeq a$

Součástí každého jazyka jsou samozřejmě také názvy proměnných (x, y, atd.) a logické spojky (& značí „a“, $\vee$ značí „nebo“, $\neg$ značí negaci) a kvantifikátory. Pokud jsou v nějakém axiomu či tvrzení nekvantifikované proměnné, tvrzení platí pro všechny takové $x, y, \dots$ (např. axiom (1) $(\forall a)\ a \preccurlyeq a$, axiom (3) $(\forall a)\ (\forall b)\ (\forall c)\ \cdots$).

Mezi těmito axiomy chybí popis relace $=$ (resp. $\neq$). Tyto dva relační symboly se vyskytují v každé rozumné matematické teorii, a proto jejich přítomnost budeme vždy předpokládat s tím, že pro ně budou platit všechny vlastnosti, na které jsme intuitivně zvyklí. Formálně vzato, jazyk každé teorie bude obsahovat relační symboly $=, \neq$ a axiomy budou doplněny o následující:

(1) $x = x$
(2) $x = y \ \Rightarrow\ (\forall a)\ (a \sim x \Leftrightarrow a \sim y) \ \&\ (x \sim a \Leftrightarrow y \sim a)$ pro lib. relační symbol $\sim$
(3) $x = y \ \Rightarrow\ F(x) = F(y)$ pro libovolný funkční symbol F
(4) $x = y \ \Rightarrow\ (\forall a)\ (a * x = a * y) \ \&\ (x * a = y * a)$ pro libovolnou operaci $*$
(5) $x \neq y \iff \neg\, x = y$

Popis matematické teorie je vlastně soupisem vlastností, které by měl mít popisovaný objekt. Dá se dokázat, že pokud z axiomů nelze dokázat spor, pak existuje nějaká struktura, pro kterou jsou axiomy splněny. Nazývá se **model**. Modelem tedy myslíme neprázdnou množinu M, na které jsou definovány konstanty, funkce, operace a relace odpovídající symbolům jazyka tak, že pro ně platí axiomy. Je jasné, že modelů jedné teorie může být více a že se mohou navzájem dost lišit.

Zde je příklad dvou modelů TUSNP (modelem této teorie je libovolná uspořádaná množina s nejmenším prvkem).

I) Přirozená čísla. Nechť $M = \{0, 1, 2, \dots\}$, $\bot = 0$, $a \preccurlyeq b \Leftrightarrow a \leq b$. Je vidět, že axiomy jsou pro takto definované symboly splněny.

II) Systém podmnožin. Nechť X je nějaká množina a M je systém všech jejích podmnožin. Nechť $\bot = \emptyset$ a $a \preccurlyeq b \Leftrightarrow a \subseteq b$. Pak jsou splněny axiomy, neboť pro $A, B, C \subseteq X$

(1) $A \subseteq A$ zjevně.

(2) $A \subseteq B \ \& \ B \subseteq A \ \Rightarrow \ A = B$ také platí.
(3) $A \subseteq B \ \& \ B \subseteq C \ \Rightarrow \ A \subseteq C$ je rovněž zřejmé.
(4) $\emptyset \subseteq A$ samozřejmě také.

Tento důkaz je dosti jednoduchý, vždy tomu tak zdaleka nebude.

V úlohách po vás zpravidla budeme chtít, abyste zjistili, zda dané tvrzení v dané teorii platí. Může se vám povést dokázat, že platí, nebo se vám může povést dokázat negaci (tzn. že neplatí), ale také se vám nemusí povést ani jedno. Ne vždy je chyba na vaší straně. Pokud jsou axiomy příliš slabé, tvrzení nejde ani dokázat, ani vyvrátit (říkáme, že je **nerozhodnutelné**). To může být také správná odpověď, ale musíte ji dokázat. Jedna z metod, pro vás asi nejlepší, je sestrojení dvou modelů dotyčné teorie, přičemž v jednom bude příslušné tvrzení pravdivé, kdežto v druhém nikoliv. Pokud takové modely sestrojíte, nemůžete samozřejmě z axiomů dotyčné tvrzení dokázat ani vyvrátit, neboť byste v jednom z těchto modelů dostali spor.

Příklad: Zjistěte, zda v TUSNP platí $(a \preccurlyeq b \ \vee \ b \preccurlyeq a)$.
Řešení: Toto tvrzení je (jak jinak) nerozhodnutelné. Vezměme model I. V něm je toto tvrzení realizováno jako $(\forall a \in M)\ (\forall b \in M)\ (a \leq b \ \vee \ b \leq a)$. To je ale zjevně pravda.

Teď si vezměme model II. Zde toto tvrzení znamená $(\forall A \subseteq X)\ (\forall B \subseteq X)\ (A \subseteq B \ \vee \ B \subseteq A)$. To rozhodně neplatí, pokud je množina X alespoň dvouprvková. Takže dotyčné tvrzení není možné z daných axiomů dokázat ani vyvrátit.

Pokud stále ještě příliš nerozumíte tomu, co se po vás chce, nezoufejte! Zde je to vše ve zkratce:

„Zjistěte, zda v této teorii platí “ znamená provedení jedné z těchto variant:

(1) Dokažte, že pokud platí axiomy, pak platí dokazované tvrzení.
(2) Dokažte, že pokud platí axiomy, pak platí negace dokazovaného tvrzení.
(3) Sestrojte model této teorie takový, že v něm platí dokazované tvrzení a sestrojte model této teorie takový, že v něm neplatí dokazované tvrzení.

„Sestrojte model“ znamená nalezení takové množiny a konstant, funkcí, operací a relací na ní, že platí axiomy.

Upozornění 1: Dokazujete-li nějaké tvrzení, nepovažujte za známé nic, než dané axiomy. Dokazujte pečlivě i zdánlivé triviality, uvidíte, že ne vždy je důkaz od pohledu jasných tvrzení jednoduchý.

Upozornění 2: Předchozí upozornění neplatí pro konstrukci modelů. Při ní se řiďte stejnými pokyny jako v každé jiné sérii.

6. série

Téma: Logika

Termín odeslání: 16. BŘEZNA 1998

1. ÚLOHA

Přidejme k teorii uspořádání s nejmenším prvkem operace $\triangle$ a $\triangledown$ a axiomy

(5) $a \triangle b = c \iff (a \preccurlyeq c \ \&\ b \preccurlyeq c \ \&\ (\forall d)\ ((a \preccurlyeq d \ \&\ b \preccurlyeq d) \ \Rightarrow\ c \preccurlyeq d))$

(6) $a \triangledown b = c \iff (c \preccurlyeq a \ \&\ c \preccurlyeq b \ \&\ (\forall d)\ ((d \preccurlyeq a \ \&\ d \preccurlyeq b) \ \Rightarrow\ d \preccurlyeq c))$

Zjistěte, zda v této teorii platí $a \triangledown (b \triangle a) = a \triangle (b \triangledown a)$.

2. ÚLOHA

Jazyk teorie: konstanta $\mho$, operace $\diamond$.

Axiomy:

(1) $a \diamond (b \diamond c) = (a \diamond b) \diamond c$

(2) $a \diamond \mho = \mho \diamond a = a$

Zjistěte, zda v této teorii platí

$((\forall a \neq \mho)\ (\exists b)\ (\exists c \neq b)\ a \diamond b = b \diamond a = a \diamond c = c \diamond a = \mho) \ \Rightarrow\ ((\forall x)\ (\forall y)\ x \diamond y = y \diamond x)$.

3. ÚLOHA

Jazyk teorie[1]: konstanta $\daleth$, funkční symbol $\beth$, operace $\oplus$.

Axiomy:

(1) $\beth(x) = \beth(y) \ \Rightarrow\ x = y$

(2) $x \oplus \daleth = x$

(3) $x \oplus \beth(y) = \beth(x \oplus y)$

(4) pro libovolné tvrzení $\varphi(x)$ platí $(\varphi(\daleth) \ \&\ (\forall x)\ (\varphi(x) \Rightarrow \varphi(\beth(x)))) \ \Rightarrow\ (\forall x)\ \varphi(x)$

Zjistěte, zda v této teorii platí

(a) $(\exists z)\ \beth(z) = \daleth$

(b) $(\forall x)\ (\forall y)\ x \oplus y = y \oplus x$

Návod: Povšimněte si, že modelem této teorie je např. $\mathbb{N} \cup \{0\}$ s obyčejným sčítáním, $\daleth = 0$, $\beth(x) = x + 1$. Axiom (4) říká, že můžete použít matematickou indukci.

4. ÚLOHA

Přidejme k teorii z minulého příkladu relační symbol $\propto$ a axiomy

(5) $\neg\ x \propto \daleth$

(6) $x \propto \beth(y) \iff (x \propto y \ \vee\ x = y)$

---

[1] Ty dva divné znaky jsou daleth a gimel, třetí a čtvrté písmeno hebrejské abecedy.

Zjistěte, zda v této teorii platí
(a) $(\exists z)\ \beth(z) = \daleth$
(b) $((\exists x)\ x \propto x\ \ \&\ \ (\forall y \neq \daleth)\ (\exists z)\ y = \beth(z)) \iff (\forall a)\ (\forall b)\ (a \propto b \Leftrightarrow (\exists c)\ b = a \oplus \beth(c))$

5. ÚLOHA
Jazyk teorie: operace $\heartsuit$.
Axiomy:

(1) $a \heartsuit (b \heartsuit c) = (a \heartsuit b) \heartsuit c$
(2) $(\forall a)\ (\forall b)\ (\exists c)\ a \heartsuit c = c \heartsuit a = b$
(3) $a \neq b\ \Rightarrow\ (c \heartsuit a \neq c \heartsuit b\ \ \&\ \ a \heartsuit c \neq b \heartsuit c)$

Zjistěte, zda v této teorii platí $((\exists a)\ (\forall b)\ a \heartsuit b = b)\ \ \&\ \ ((\forall a)\ (\exists b)\ (\forall c)\ (b \heartsuit a) \heartsuit c = c)$.

Řešení 6. série

1. úloha (Teorie svazů)
Přidejme k teorii uspořádání s nejmenším prvkem operace $\triangle$ a $\triangledown$ a axiomy

(5) $a \triangle b = c \iff (a \preccurlyeq c \ \& \ b \preccurlyeq c \ \& \ (\forall d)\ ((a \preccurlyeq d \ \& \ b \preccurlyeq d) \ \Rightarrow \ c \preccurlyeq d))$
(6) $a \triangledown b = c \iff (c \preccurlyeq a \ \& \ c \preccurlyeq b \ \& \ (\forall d)\ ((d \preccurlyeq a \ \& \ d \preccurlyeq b) \ \Rightarrow \ d \preccurlyeq c))$

Zjistěte, zda v této teorii platí $a \triangledown (b \triangle a) = a \triangle (b \triangledown a)$.

(V následujícím řešení je drobná chybička. Zkus ji odhalit sám a pokud se Ti to nepovede, podívej se na poznámky opravovatele.) Tvrzení platí. Stačí si uvědomit, že obě strany rovnosti se rovnají a.

Nejprve levá strana. Označme $c = b \triangle a$ a $x = a \triangledown c$. Podle axiomu (5) platí $a \propto c$. Chceme dokázat, že $x = a$. Musíme tedy ověřit podmínky z axiomu (6). Vidíme, že $a \propto a$ platí z axiomu (1), $a \propto c$ z axiomu (5) a tvrzení $(\forall y)\ ((y \propto a \ \& \ y \propto c) \ \Rightarrow \ y \propto a)$ je splněno zřejmě. Pro pravou stranu bychom postupovali zcela analogicky — pouze s prohozenými nerovnostmi a znaménky $\triangledown$ a $\triangle$.

Poznámky opravovatele: Drtivá většina řešitelů (autora úlohy nevyjímaje) řešila (víceméně správně) úlohu
operace $\triangle$ a $\triangledown$ jsou definovány $\implies$ $a \triangle (a \triangledown b) = a \triangledown (a \triangle b)$.
Tato úloha nemá se zadanou moc společného, přesto za správné řešení dostali 3 body.

Problém je v tom, že operace nemusí být definovány. Jedná se o podobný problém, jako když se ptáme, zda platí $1 : (1 : a) = a$ — platí to vždy, když je levá strana definována, tj. když $a \neq 0$.

Správné řešení mělo vypadat asi takto:

Nejprve najdu model, kde jsou $\triangle$ a $\triangledown$ definovány a rovnost platí. Příkladem takového modelu jsou třeba přirozená čísla s normálním uspořádáním, kde $a \triangle b = \max(a, b)$ a $a \triangledown b = \min(a, b)$.

Dále najdu model, kde tvrzení neplatí. Nejjednoduším takovým modelem je dvouprvková množina $\{x, y\}$, kde x a y jsou neporovnatelné. Rozmyslete si, že $x \triangle y$ ani $x \triangledown y$ není definováno, jinak by neplatily axiomy.

Našli jsme model, v němž tvrzení platí, i model, v němž tvrzení neplatí, tudíž tvrzení je nerozhodnutelné.

2. úloha (Teorie monoidů)
Jazyk teorie: konstanta $\mho$, operace $\diamond$.

Axiomy:

(1) $a \diamond (b \diamond c) = (a \diamond b) \diamond c$
(2) $a \diamond \mho = \mho \diamond a = a$

Zjistěte, zda v této teorii platí
$((\forall a \neq \mathfrak{V})\ (\exists b)\ (\exists c \neq b)\ a \diamond b = b \diamond a = a \diamond c = c \diamond a = \mathfrak{V}) \ \Rightarrow\ ((\forall x)\ (\forall y)\ x \diamond y = y \diamond x)$.

Tvrzení platí.

Pokud je ve výrazu $A \Rightarrow B$ tvrzení A nepravdivé, pak tento výraz je pravdivý, ať už B platí nebo ne (viz tabulka pravdivostních hodnot pro $\Rightarrow$). V našem případě lze dokázat, že předpoklad neplatí.

Sporem. Víme, že pro libovolné $a \neq \mathfrak{V}$ existují $b \neq c$ takové, že $b \heartsuit a = \mathfrak{V}$ a $a \heartsuit c = \mathfrak{V}$. Podle axiomu (1) platí $(b \heartsuit a) \heartsuit c = b \heartsuit (a \heartsuit c)$. Potom ale platí $\mathfrak{V} \heartsuit c = b \heartsuit \mathfrak{V}$, což podle axiomu (2) dává $b = c$, což je spor.

3. úloha (P–aritmetika)
Jazyk teorie[2]: konstanta $\daleth$, funkční symbol $\beth$, operace $\oplus$.

Axiomy:

(1) $\beth(x) = \beth(y) \ \Rightarrow\ x = y$
(2) $x \oplus \daleth = x$
(3) $x \oplus \beth(y) = \beth(x \oplus y)$
(4) pro libovolné tvrzení $\varphi(x)$ platí $(\varphi(\daleth)\ \&\ (\forall x)\ (\varphi(x) \Rightarrow \varphi(\beth(x)))) \ \Rightarrow\ (\forall x)\ \varphi(x)$

Zjistěte, zda v této teorii platí
(a) $(\exists z)\ \beth(z) = \daleth$
(b) $(\forall x)\ (\forall y)\ x \oplus y = y \oplus x$

Návod: Povšimněte si, že modelem této teorie je např. $\mathbb{N} \cup \{0\}$ s obyčejným sčítáním, $\daleth = 0$, $\beth(x) = x + 1$. Axiom (4) říká, že můžete použít matematickou indukci.

(a) Toto tvrzení je nerozhodnutelné.
I) Vezměme model $\mathbb{N} \cup \{0\}$ zmíněný v návodu, $x \oplus y = x + y$, $\daleth = 0$, $\beth(x) = x + 1$. Axiomy jsou splněny (ověřte!). Přepišme tedy výraz $(\exists z)\ \beth(z) = \daleth$ jako $(\exists n \in \{0, 1, \dots\})\ n + 1 = 0$. Jenže $n + 1 = 0 \Leftrightarrow n = -1$, ale -1 do $\mathbb{N} \cup \{0\}$ nepatří, čímž máme spor.
II) Vezměme si následující model (nazývaný $\mathbb{Z}_p, p > 1$). Za množinu M zvolme $\{0, \dots, p-1\} \subset \mathbb{N}$ a definujme symboly

$$\daleth = 0, \quad x \oplus y = (x + y) \bmod p, \quad \beth(x) = (x + 1) \bmod p,$$

kde $a \bmod b$ značí zbytek a po dělení b. Nyní ověřme, že platí axiomy. Pokud $(x+1) \bmod p = (y+1) \bmod p$, pak $x \bmod p = y \bmod p$, a protože $x, y \in \{0, \dots, p-1\}$, tak zbytek po dělení p je stejný, jako původní číslo, takže $x = y$. Druhý axiom tvrdí $(x+0) \bmod p = x$, což je pravda, neboť (jako minule) $(x + 0) = x = x \bmod p$. Třetí axiom je $(x + ((y + 1) \bmod p)) \bmod p = ((x + y) \bmod p + 1) \bmod p$, což není nic jiného, než $(x + y) \bmod p = (x + y) \bmod p$. Indukce: pokud platí $\varphi(0)$ a $\varphi(n) \ \Rightarrow\ \varphi((n+1) \bmod p)$, pak dostáváme postupným užíváním druhého pravidla pro $n = 0, \dots, p-2$ platnost $\varphi(1)$, $\dots$, $\varphi(p-1)$, tj. $\varphi(x)$ pro libovolné x.

[2] Ty dva divné znaky jsou daleth a gimel, třetí a čtvrté písmeno hebrejské abecedy.

V tomto modelu (dokonce pro každé p jiném) na rozdíl od I) zadané tvrzení platí. Pro $z = p - 1$ máme $\beth(z) = ((p-1)+1) \bmod p = p \bmod p = 0$.

(b) Toto tvrzení platí.

Lemma 1. $\daleth \oplus x = x$ *(tento výraz označme jako $\varphi(x)$).*

Použijeme axiom (4) – matematickou indukci:
A) $\varphi(\daleth)$ je $\daleth \oplus \daleth = \daleth$, což platí podle axiomu (2).
B) Platí $\varphi(x)$ (indukční předpoklad), chceme dokázat platnost $\varphi(\beth(x))$, tj. $\daleth \oplus \beth(x) = \beth(x)$. Pišme $\daleth \oplus \beth(x) = \beth(\daleth \oplus x) = \beth(x)$ – první rovnost podle axiomu (3), druhá je indukční předpoklad (i.p.).

Lemma 2. $\beth(y) \oplus x = \beth(y \oplus x)$ *(tento výraz označme jako $\varphi(x)$).*

Použijeme axiom (4) (stejně jako minule):
A) $\beth(y) \oplus \daleth = \beth(y) = \beth(y \oplus \daleth)$ podle axiomu (2).
B) $\beth(y) \oplus \beth(x) = \beth(\beth(y) \oplus x) = \beth(\beth(y \oplus x)) = \beth(y \oplus \beth(x))$ – postupně použijeme axiom (3), i.p., axiom (3).

Vlastní tvrzení $y \oplus x = x \oplus y$ dokážeme také z axiomu (4):
A) $y \oplus \daleth = y = \daleth \oplus y$ podle axiomu (2) a Lemmatu 1.
B) $y \oplus \beth(x) = \beth(y \oplus x) = \beth(x \oplus y) = \beth(x) \oplus y$ – postupně podle axiomu (3), i.p. a Lemmatu 2.
Čímž dokázáno jest.

Poznámky opravovatele: Nelíbily se mi dvě věci. Za prvé mnoho řešitelů nalezlo nějakou množinu a nějaké operace na ní, ale vůbec neověřovali, že nalezli model teorie, tj. že platí axiomy. Ověření axiomů sice nebylo těžké, ale i v takovém případě je třeba se alespoň zmínit o tom, že axiomy platí, a eventuálně vynechat důkaz s poukazem na jeho trivialitu.

Za druhé — důkaz části (b) prováděla většina řešitelů matematickou indukcí (stejně jako autorské řešení). Někteří však vynechali „kostru“ důkazu, v jejich řešení chybělo něco takovéhoto: „Dokazujeme $\varphi(x)$ indukcí. ... takže $\varphi(0)$ platí. Pokud platí $\varphi(x)$, ... , a tedy platí i $\varphi(\beth(x))$. Podle axiomu 4 platí tedy $(\forall x)\varphi(x)$.“ a byly tam jen kroky zde nahrazené .... Pokud by důkaz obsahoval jen jednu indukci, nevadilo by to tolik. Když jsou ale ty indukce tři, navíc do sebe vnořené, tak čtenář, který ten důkaz dopředu nezná, netuší, co se vlastně děje, kdy která indukce začíná a končí, ani co se tou indukcí dokazuje.

Další poznámky se týkají i čtvrté úlohy. V několika řešeních se vyskytla následující úvaha:
Označíme $\beth^0(\daleth) = \daleth$ a $\beth^n(\daleth) = \beth(\beth^{n-1}(\daleth))$, tj. $\beth^n(\daleth)$ představuje n-té přirozené číslo. Budeme dokazovat indukcí následující tvrzení $(*)$: $(\forall x)(\exists n \in \mathbb{N})\ x = \beth^n(\daleth)$. To se nám samozřejmě povede (zkuste si to sami!). V čem je problém? V obvyklé formulaci axiomu 4 (indukce) je $\varphi(x)$ formule příslušné teorie. Tou však $(\exists n \in \mathbb{N})\ x = \beth^n(\daleth)$ není, obsahuje totiž existenční kvantifikátor na výběr prvku z množiny $\mathbb{N}$. V zadané teorii však není definována ani množina $\mathbb{N}$, ani symbol $\in$! Bohužel v zadání bylo místo „libovolná formule teorie“ uvedeno „libovolné tvrzení“, takže tento způsob řešení byl správný.

Při obvyklé formulaci axiomu 4 však tvrzení $(*)$ neplatí, mohou existovat „čísla“, která prostým opakováním funkce následníka nedostaneme!

Abych dodal svým slovům váhu (a vás trochu poučil), předvedu zde model dané teorie (při správné formulaci axiomu 4), ve kterém budou existovat čísla nedosažitelná cyklickým voláním funkce $\beth$ na konstantu $\daleth$ (tj. budou existovat „nekonečně velká čísla“ — čísla větší než jakékoliv přirozené číslo).

Část matematiky, která se zabývá podobnými otázkami, se nazývá teorie modelů. Budu zde dosti zjednodušovat, neboť moje konstrukce využívá trochu pokročilejších partií této vědy.

Další dva odstavce budou trošičku náročnější na představu. Neděs se, prosím, uvedené konstrukce. Pokud Ti bude připadat příliš těžká, zkus přejít rovnou k poslednímu odstavci tohoto textu, tam je v jádru řečeno, k čemu směřujeme.

Označme A množinu všech posloupností přirozených čísel. Na ní definujme $\daleth_A = (0, 0, \dots)$ a operace $\oplus_A, \beth_A$ po složkách.[3]

Nechť $\mathfrak{U}$ je soubor všech „velikých“ podmnožin $\mathbb{N}$. Konkrétněji, ať $\mathfrak{F} = \{A \subseteq \mathbb{N} : \mathbb{N} \setminus A$ je konečná $\}$ a $\mathfrak{U}$ ať je nějaká nadmnožina množiny $\mathfrak{F}$ splňující

(1) $A \subseteq \mathbb{N} \;\Rightarrow\; A \in \mathfrak{U}$ nebo $\mathbb{N} \setminus A \in \mathfrak{U}$
(2) $A, B \in \mathfrak{U} \;\Rightarrow\; A \cap B \in \mathfrak{U}$ (to znamená průnik velikých množin je veliký)
(3) $A \in \mathfrak{U}$, $A \subset B \;\Rightarrow\; B \in \mathfrak{U}$ (nadmnožina veliké množiny je veliká)

Taková množina $\mathfrak{U}$ skutečně existuje, to však zde nebudeme dokazovat. Dále definujme na množině A ekvivalenci $\sim$ přepisem

$$(a_i) \sim (b_i) \Longleftrightarrow \{i : a_i = b_i\} \in \mathfrak{U},$$

tj. posloupnosti (a_i) a (b_i) se shodují na „veliké“ podmnožině indexů. Přichází stěžejní krok.

Označme $[(a_i)]$ množinu všech posloupností, které jsou ekvivalentní s (a_i), tj. $[(a_i)] = \{(b_i) : (a_i) \sim (b_i)\}$. Označme B množinu všech $[(a_i)]$. Na této množině definujme operace následujícím způsobem: $\daleth_B = [\daleth_A]$, $\beth_B([(a_i)]) = [\beth_A((a_i))]$, $[(a_i)] \oplus_B [(b_i)] = [(a_i) \oplus_A (b_i)]$. Nebudu dokazovat (je to obtížné), že operace a funkce jsou definovány korektně a že takto sestrojená struktura je skutečně modelem naší teorie. Avšak předvedu to, co bylo cílem naší konstrukce.

V předcházejích dvou odstavcích jsme nadefinovali jistou množinu posloupností, z nichž některé jsme prohlásili za stejné a dostali model B. Na něm je důležité (kromě toho, že je modelem naší teorie) hlavně následující skutečnost. V modelu B platí: $\daleth = [(0, 0, 0, \dots)]$, $\beth(\daleth) = [(1, 1, 1, \dots)]$, $\beth(\beth(\daleth)) = [(2, 2, 2, \dots)]$, $\dots$ Je vidět,[4] že „normální přirozená čísla“ mají zde tvar $\beth^n(\daleth) = [(n, n, n, \dots)]$. Vezměme však „nestandardní číslo“ $[(0, 1, 2, \dots)]$. Tato

[3] Souslovím definovat operace po složkách míníme například pro sčítání, že součet dvou posloupností $(a_1, a_2, \dots)$, $(b_1, b_2, \dots)$ je roven posloupnosti $(a_1+b_1, a_2+b_2, \dots)$, tj. uvedenou operaci provádíme v každé složce zvlášť.

[4] Pokud jsi přeskočil konstrukci modelu B, tak to vem prosím za fakt.

posloupnost není shodná s žádnou $(n, n, n, \dots)$ na nekonečně mnoha indexech a proto nemůže být toto „číslo“ rovno žádnému $\beth^n(\daleth)$, což jsme chtěli ukázat.

Pokud analogickým způsobem dodefinujeme i relaci $\propto$ na A a B, je možno dokázat, že uvedené „nestandardní číslo“ je také větší než všechna „standardní“ — zkuste si to sami. Odtud pramení formulace „nekonečně velká čísla“.

4. úloha (P–aritmetika s nerovností)
Přidejme k teorii z minulého příkladu relační symbol $\propto$ a axiomy

(5) $\neg\ x \propto \daleth$
(6) $x \propto \beth(y) \iff (x \propto y\ \vee\ x = y)$

Zjistěte, zda v této teorii platí
(a) $(\exists z)\ \beth(z) = \daleth$
(b) $((\exists x)\ x \propto x\ \ \&\ \ (\forall y \neq \daleth)\ (\exists z)\ y = \beth(z)) \iff (\forall a)\ (\forall b)\ (a \propto b \Leftrightarrow (\exists c)\ b = a \oplus \beth(c))$

(a) Tvrzení neplatí.

Rovnost $z = z$ zajisté platí. Proto musí platit i $(z = z\ \vee\ z \propto z)$, takže z axiomu (6) pro $x = y = z$ dostáváme $z \propto \beth(z)$. Pokud $\beth(z) = \daleth$, pak máme $z \propto \daleth$. To je ovšem ve sporu s axiomem (5), čili takové z nemůže existovat.

(b) Tvrzení neplatí.

Dané tvrzení je tvaru $(A\ \ \&\ \ B) \Leftrightarrow C$. Já dokáži, že platí C a platí $C \Rightarrow \neg A$, což dá v implikaci zprava doleva spor, neboť nemůže platit současně $\neg A$ a A.

Důkaz C**:** Zvolme libovolné a a označme $\varphi(b)$ tvrzení $a \propto b \Leftrightarrow (\exists c)\ b = a \oplus \beth(c)$ Použijeme axiom (4). První krok: $\varphi(\daleth)$ tvrdí $a \propto \daleth \Leftrightarrow (\exists c)\ \daleth = a \oplus \beth(c)$. Levá strana ekvivalence není nikdy splněna (axiom (5)). Dále platí $a \oplus \beth(c) = \beth(a \oplus c)$ podle axiomu (2), ale to by se mělo rovnat $\daleth$, což podle části (a) této úlohy nelze. Obě strany ekvivalence jsou nepravdivá tvrzení, takže ekvivalence je pravdivá (namaluj si tabulku pravdivostních hodnot).

Druhý krok: víme, že platí $\varphi(x)$, chceme dokázat $\varphi(\beth(x))$. Levá strana ekvivalence $\varphi(\beth(x))$ zní $a \propto \beth(b)$, což je podle axiomu (6) právě tehdy, když $(a \propto b\ \vee\ a = b)$. Dále rozebereme oba případy.

$$(a \propto b) \Leftrightarrow (b = a \oplus \beth(d)) \Leftrightarrow (\beth(b) = \beth(a \oplus \beth(d))) \Leftrightarrow (\beth(b) = a \oplus \beth(\beth(d)))$$

Postupným použitím i.p. a axiomů (1) a (3) máme hledané $c = \beth(d)$.

Axiom (1) a axiomy pro rovnost říkají, že $a = b \Leftrightarrow \beth(b) = \beth(a)$. Použitím axiomů (2) a (3) máme $\beth(a) = \beth(a \oplus \daleth) = a \oplus \beth(\daleth)$, a tedy hledané c je rovno $\daleth$.

Důkaz $C \Rightarrow \neg A$**:** $\varphi(x)$ označme tvrzení $\neg A$, tj. $\varphi(x) \Leftrightarrow \neg(x \propto x)$

Opět užijeme axiom (4): $\varphi(\daleth)$ tvrdí $\neg(\daleth \propto \daleth)$, což je přímo z axiomu (5).

Druhý krok: víme, že platí $\neg(x \propto x)$, chceme dokázat $\neg(\beth(x) \propto \beth(x))$. Sporem: pokud platí $\beth(x) \propto \beth(x)$, pak z předpokladu C plyne $\beth(x) = \beth(x) \oplus \beth(c) = \beth(x \oplus \beth(c))$ (podle Lemmatu 2

z příkladu 3) a tedy $x = x \oplus \beth(c)$ (axiom (1)), což dle předpokladu C znamená, že $x \propto x$. To je ale ve sporu s indukčním předpokladem.

5. úloha (Teorie grup)
Jazyk teorie: operace $\heartsuit$.

Axiomy:

(1) $a \heartsuit (b \heartsuit c) = (a \heartsuit b) \heartsuit c$
(2) $(\forall a)\ (\forall b)\ (\exists c)\ a \heartsuit c = c \heartsuit a = b$
(3) $a \neq b\ \Rightarrow\ (c \heartsuit a \neq c \heartsuit b\ \ \&\ \ a \heartsuit c \neq b \heartsuit c)$

Zjistěte, zda v této teorii platí $((\exists a)\ (\forall b)\ a \heartsuit b = b)\ \ \&\ \ ((\forall a)\ (\exists b)\ (\forall c)\ (b \heartsuit a) \heartsuit c = c)$.

Toto tvrzení platí.

Nejprve dokážeme levou půlku tvrzení. Zvolme libovolné x. Podle axiomu (2) (s přeznačenými proměnnými) existuje a takové, že $x \heartsuit a = a \heartsuit x = x$. Já tvrdím, že toto a je právě to, které hledáme, tj. pro které platí $(\forall b)\ a \heartsuit b = b$. Vezměme tedy libovolné b, a podle axiomu (2) pišme $b \heartsuit d = d \heartsuit b = b$. Následuje několik rovností.

$$(x \heartsuit b = x \heartsuit b)\ \Rightarrow\ ((x \heartsuit a) \heartsuit b = x \heartsuit (d \heartsuit b))\ \Rightarrow$$

$$\Rightarrow\ (x \heartsuit (a \heartsuit b) = x \heartsuit (d \heartsuit b))\ \Rightarrow\ (a \heartsuit b = d \heartsuit b)\ \Rightarrow\ (a = d)$$

O platnosti první rovnosti nikdo nepochybuje. Rozepíšeme x a b, pak použijeme axiom (1) na levou stranu, a nakonec dvakrát axiom (3). Vidíme, že není možné, aby existovalo $d \neq a$, které by splňovalo axiom (2), tj. a musí být pro všechny b stejné, což jsme chtěli dokázat.

Pravá půlka tvrzení plyne z levé triviálně. Stačí nám dokázat, že $(\forall c)\ (\exists b)\ b \heartsuit c = a$, kde a je to samé, co v levé půlce tvrzení. Tento výrok však není nic jiného, než axiom (2).

Poznámky opravovatele: Více než polovina řešení byla správných, až na jeden případ stejných jako vzorové. Nejrozšířenější chybou bylo prohazování kvantfikátorů $\forall$ a $\exists$. Rád bych uvedl věc na pravou míru.

Mějme tvrzení

$$P \quad \equiv \quad (\forall x)(\exists y)A(x,y)$$

$$Q \quad \equiv \quad (\exists y)(\forall x)A(x,y)$$

Platí $Q \Rightarrow P$. Q říká, že můžeme vzít nějaké pevné y_0, a potom bude pro libovolné x platit $A(x, y_0)$. P nám předepisuje, že máme vzít libovolné x a k němu najít y_x takové, aby platilo $A(x, y_x)$. Podle předpokladu však stačí vzít $y_x = y_0$.

Opačná implikace neplatí. P říká, že ke každému x mohu najít nějaké y_x tak, že platí $A(x, y_x)$. To ale neznamená, že všechna y_x jsou stejná, jak po nás požaduje Q !

Příkladem budiž tvrzení $A(x, y)$ tvaru $x + y = 0$ (pro $x, y \in \mathbb{Z}$). Platí P, neboť ke každému $x \in \mathbb{Z}$ existuje $y = -x$, pro které $x + y = 0$. Neplatí však Q — neexistuje žádné celé číslo y takové, že by pro libovolné x platilo $x + y = 0$.