Výroková a predikátová logika

J. Mlček

2012

Obsah

1 Úvod a předběžnosti **5**
- 1.1 Předběžnosti. 5
- 1.2 Booleovy algebry. 10
- 1.3 O lineárních uspořádáních. 17
- 1.4 Poznámky. 18

2 Koncept predikátové logiky **19**
- 2.1 Základní syntax. 20
- 2.2 Základní sémantika. 25
- 2.3 Vlastnosti struktur a teorií. Charakteristiky teorie. 34
- 2.4 Faktorstruktury. Algebry formulí. 47
- 2.5 Formalistické upřesnění – designátory. 50
- 2.6 Některé teorie v predikátové logice s rovností. 52
- 2.7 Poznámky. 59

3 Výroková logika **61**
- 3.1 Základní syntax. 61
- 3.2 Základní sémantika. 62
- 3.3 Existence modelu, kompletnost a kompaktnost. 66
- 3.4 Aplikace kompaktnosti. Axiomatizovatelnost. 68
- 3.5 Syntaktické důkazové metody. 70
- 3.6 Problém splnitelnosti. Rezoluce. 72
- 3.7 Vícehodnotová logika. 75
- 3.8 Poznámky. 76

4 Kompletnost predikátové logiky **77**
- 4.1 Elementární teorie dokazování. Prenexní tvar formulí. 77
- 4.2 Existence modelu, kompletnost, kompaktnost. 83
- 4.3 Extenze teorie o funkční symbol a definicemi. 89
- 4.4 Poznámky. 93

A Vlastnosti konkrétních teorií **95**
- A.1 Teorie SC_0, SC. 95
- A.2 Teorie DiLO, DiLO°. 97
- A.3 Teorie DeLO. 98
- A.4 Aritmetiky. 98
- A.5 Teorie vektorových prostorů. 102
- A.6 Teorie $\mathrm{CE}_{\mathrm{k}}(\infty)$, $\mathrm{C'E}_{\omega}$. 103
- A.7 Teorie unárního predikátu. 104
- A.8 Teorie bijekcí. 104
- A.9 Poznámky. 107

B Nerozhodnutelnost **109**
B.1 Základní pojmy. 109
B.2 Věty o nerozhodnutelnosti. 112

Kapitola 1

Úvod a předběžnosti

Text obsahuje výklad základů predikátové logiky. Přesněji půjde o predikátovou logiku prvního řádu, umožňující bezprostředně zacházet jen s predikcemi a kvantifikacemi individuí, nikoli však již se systémy individuí, systémy takových systémů atd; to je možné až v logikách vyšších řádů. Dále půjde jen o logiku dvouhodnotovou; vícehodnotový případ zmíníme pouze orientačně. Poznamenejme, že logika může pracovat navíc s tzv. neklasickými kvantifikacemi (značícími např. „existuje nekonečně mnoho“), s nekonečnými výrazy či modalitami; to vše je zde pominuto.

Nejprve bude vyložen koncept nastíněné predikátové logiky, pak bude rozvinuta dvouhodnotová výroková logika jako specificky důležitá část a následně rozvinuta predikátová logika, zejména pokud jde o její kompletnost.

Při výkladu je zapotřebí pracovat s řadou elementárních pojmů, jakými jsou konečné posloupnosti, relace, operace, velikosti množin, induktivní definice, důkaz indukcí podle složitosti induktivně definovaných objektů, případně další. Ty jsou stručně shrnuty v Předběžnostech.

V textu užijeme na mnoha místech značku $\Leftrightarrow$ pro „právě když“ a $\Rightarrow$ pro „implikuje“ českého jazyka. Značka $\leftrightarrow$ resp. $\rightarrow$ je symbol znamenající ekvivalenci resp. implikaci a patřící do nějakého matematickou logikou zkoumaného symbolického jazyka.

Místo „$\cdots$ resp. ___ resp. $\ldots$“ píšeme také „$\cdots$ [___/$\ldots$]“.

1.1 Předběžnosti.

Základní množinové pojmy.

Vlastnost (vztah) $\mathcal{V}(x)$ o množinách definuje třídu $\{x;\, \mathcal{V}(x)\}$; je-li to množina y píšeme $y = \{x;\, \mathcal{V}(x)\}$. Např. vztah $x = x$ definuje třídu $\mathbf{V}$ všech množin. Nemůže to být množina, neboť jinak by byla množinou i její podtřída $y = \{x;\, x \notin x\}$; pak ale $y \in y \Leftrightarrow y \notin y$, což je spor. Dále např. $\{x;\, x \neq x\}$ je tzv. prázdná množina, značená $\emptyset$.

Symboly $\cup, \cap, -, \dot{-}$ značí běžné známé operace s množinami, a to sjednocení, průnik, rozdíl a symetrickou diferenci dvou množin, $\{x, y\}$ je neuspořádaná dvojice množin x, y; obsahuje právě prvky x a y. $\{x_0, \ldots, x_{n-1}\}$ je množina, obsahující právě prvky $x_0, \ldots, x_{n-1}$; když $x_0 = x_1 = \cdots = x_{n-1}$, je to jednoprvková množina $\{x_0\}$. Dále $x \subseteq y$ značí, že x je podmnožina y. Potenci $\mathcal{P}(x)$ resp. sjednocení $\bigcup x$ množiny x definujeme takto:

$$\mathcal{P}(x) = \{y;\, y \subseteq x\} \quad \text{resp.} \quad \bigcup x = \{y;\, y \in z \text{ pro nějaké } z \in x\}.$$

Pokrytí množiny A je množina $S \subseteq \mathcal{P}(A) - \{\emptyset\}$ s $\bigcup S = A$. Když navíc jsou každé dva různé prvky u, v z S disjunktní, tj. $u \cap v = \emptyset$, je S disjunktní pokrytí A neboli rozklad A.

Poznamenejme, že uvedená tvrzení o tom, že $\emptyset$, $\{x, y\}$, $\mathcal{P}(x)$ atd. jsou množiny plynou z axiomů o množinách, tvořících např. Zermelo-Fraenkelovu axiomatiku. Níže uvedeme další množinové pojmy a jejich vlastnosti; ty budou plně v souladu se zmíněnou axioamtikou a navíc budou intuitivně dobře akceptovatelná. Množinový rámec tak představuje dostatečně ujasněný půdorys pro exaktní rozvoj dané matematické problematiky.

Relace, funkce, soubory. Základní porovnávání množin.

Uspořádaná dvojice (x, y) je množina $\{\{x\}, \{x, y\}\}$. Platí: $(x, y) = (x', y')$, právě když $x = x'$ a $y = y'$. Kartézský produkt (součin) $a \times b$ množin a a, b je tvořen právě všemi uspořádanými dvojicemi (x, y) s $x \in a$, $y \in b$. Nyní můžeme definovat disjunktní sjednocení $x \uplus y$ množin:

$$x \uplus y = (\{\emptyset\} \times x) \cup (\{\{\emptyset\}\} \times y).$$

Poznamenejme, že $\emptyset$ resp. $\{\emptyset\}$ chápeme též jako přirozená čísla 0 resp. 1, tudíž $x \uplus y = (\{0\} \times x) \cup (\{1\} \times y)$. Disjunktní sjednocení, kartézský součin a množinová mocnina jsou důležité množinové operace, úzce související s kalkulem velikostí množin.

Relace je jakákoli množina R uspořádaných dvojic; speciálně je $\emptyset$ relace. Místo $(x, y) \in R$ se píše též $R(x, y)$. Definiční obor resp. obor hodnot relace R je množina

$$\mathrm{dom}(R) = \{x;\ \text{existuje } y \text{ s } (x, y) \in R\} \quad \text{resp.} \quad \mathrm{rng}(R) = \{y;\ \text{existuje } x \text{ s } (x, y) \in R\};$$

zřejmě $R \subseteq \mathrm{dom}(R) \times \mathrm{rng}(R)$. Extenze prvku x v R je množina $R[x] = \{y;\ (x, y) \in R\}$. Parcializace $R \restriction u$ relace R na u je $\{(x, y) \in R;\ x \in u\}$; je $R \restriction \emptyset = \emptyset$. Dále $R^{-1} = \{(y, x);\ (x, y) \in R\}$ je relace inverzní k R. Je-li S také relace, definujeme složení $R \circ S$ relací R a S: $R \circ S = \{(x, y);\ \text{existuje } z \text{ s } (x, z) \in R \text{ a } (z, y) \in S\}$. Buď A množina. Pak $\mathrm{Id}_A = \{(a, a);\ a \in A\}$. Zřejmě pro $R \subseteq A \times A$ je $R \circ \mathrm{Id}_A = R = \mathrm{Id}_A \circ R$.

Relace R je reflexivní resp. symetrická resp. tranzitivní na A, když pro $a, b, c \in A$ platí:

$$R(a, a) \text{ resp. } R(a, b) \text{ implikuje } R(b, a) \text{ resp. když } R(a, b) \text{ a } R(b, c), \text{ tak } R(a, c).$$

Je-li relace R reflexivní, symetrická a tranzitivní na $A = \mathrm{dom}(R) = \mathrm{rng}(R)$, je to ekvivalence na A a pro $a \in A$ je $R[a]$ faktor prvku a dle R. Množina $A/R = \{R[a];\ a \in A\}$ je faktor-množina množiny A dle R. A/R je zřejmě rozklad A a naopak rozklad S na A určuje ekvivalenci E na A s $A/E = S$. Je-li relace reflexivní a tranzitivní na A, je to kvaziuspořádání na A, je-li navíc R antisymetrická na A, tj. z $R(x, y)$ a $R(y, x)$ plyne $x = y$ pro $x, y \in A$, je R uspořádání na A; $R - \mathrm{Id}_A$ je jeho ostrá verze. Často značíme uspořádání symbolem $\leq$; $<$ je pak jeho ostrá verze.

Relace R je funkce, když $R[x]$ je jednoprvková pro každé $x \in \mathrm{dom}(R)$. Je-li R funkce a platí $R[x] = \{y\}$, píšeme $R(x) = y$; y je hodnota R v x. Množina $\emptyset$ je (prázdná) funkce; $\mathrm{dom}(\emptyset) = \emptyset = \mathrm{rng}(\emptyset)$. Funkce značíme nejčastěji písmeny F, G, H, f, g, h. Symbol $f : x \to y$ značí, že f je funkce z x do y, tj. $\mathrm{dom}(f) = x$, $\mathrm{rng}(f) \subseteq y$. Funkce f je na y, když $\mathrm{rng}(f) = y$ a je prostá, když pro $a, b \in \mathrm{dom}(f)$ s $a \neq b$ je $f(a) \neq f(b)$. Dále množina všech funkcí z x do y se značí ${}^{x}y$. Prvky z ${}^{x}\{0, 1\}$ jsou charakteristické funkce na x. Pro funkce F, G definujeme $F \cdot G = G \circ F$; tedy $F \cdot G(x) = y$ právě když existuje z s $(x, z) \in G$ a $(z, y) \in F$ a také $F \cdot G(x) = F(G(x))$ pro $x \in \mathrm{dom}(G)$ s $G(x) \in \mathrm{dom}(F)$. Místo $F \cdot G$ se píše též FG. Je-li F funkce a X množina, značí $F[X]$ (též $F''X$) obraz X přes F, tj. množinu $\{y;\ \text{existuje } x \in X \text{ s } y = F(x)\}$.

Je-li f funkce s $\mathrm{dom}(f) = I$, říkáme také, že to je (indexovaný) soubor (s indexovou množinou I) a značíme jej $\langle f_i \rangle_{i \in I}$, stručněji $\langle f_i \rangle_I$; f_i je $f(i)$. Prázdný soubor se značí též $\langle\rangle$. Sjednocení $\bigcup(\mathrm{rng}(f))$ souboru $\langle f_i \rangle_{i \in I}$ se značí $\bigcup_{i \in I} f_i$, stručněji $\bigcup_I f_i$ a také $\bigcup\{f_i;\ i \in I\}$.

Základní porovnání velikosti množin je dáno subvalencí a ekvivalencí množin: Množina x je subvalentní ($\preccurlyeq$) resp. ekvivalentní ($\approx$) množině y, existuje-li prosté zobrazení x do y resp. navíc na y. Když $x \preccurlyeq y$ a není $x \approx y$, je x ostře subvalentní y. Zřejmě jsou $\preccurlyeq, \approx$ reflexivní a tranzitivní vztahy, $\approx$ navíc symetrický. Dále $\mathcal{P}(x) \approx {}^{x}\{0, 1\}$. Platí dvě důležité věty:

Cantor-Bernsteinova věta. *$x \preccurlyeq y$ a $y \preccurlyeq x$ implikuje $x \approx y$.*

Cantorova věta. *Množina x je ostře subvalentní $\mathcal{P}(x)$.*

Přirozená čísla.

Množina přirozených čísel se značí $\mathbb{N}$. Definuje se jako nejmenší induktivní množina, tj. taková množina w, že $\emptyset \in w$ a z $x \in w$ plyne $x \cup \{x\} \in w$. Pak pro každé přirozené číslo n platí $n = \{0, 1, \ldots, n-1\}$, speciálně $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{0, 1\}$. Dále je $m < n \Leftrightarrow m \in n \Leftrightarrow m \subsetneq n$. Uspořádání $<$ přirozených čísel je dobré, tj. každá neprázdná podmnožina množiny $\mathbb{N}$ má nejmenší prvek. Dále platí princip matematické indukce a lze konstruovat rekurzí podle předpisu $F(n) = G(F \restriction n, n)$ jedinou maximální funkci s $\mathrm{dom}(F) \in \mathbb{N}$ či $\mathrm{dom}(F) = \mathbb{N}$; G je tzv. konstruující funkce. Rekurzí se sestrojí obvyklé sčítání a násobení přirozených čísel. Dále definujeme: množina je konečná, je-li ekvivalentní nějakému přirozenému číslu $n \in \mathbb{N}$: $x \approx n$. Píšeme pak $|x| = n$ a říkáme, že n je velikost či kardinalita či mohutnost x. Přirozená čísla představují typy velikostí čili kardinalit konečných množin. Jejich aritmetika je dána sčítáním, násobením a mocněním přirozených čísel, přičemž význam této kardinální aritmetiky ukazují následující rovnosti pro konečné množiny x, y:

$$|x \uplus y| = |x| + |y|, \quad |x \times y| = |x| \cdot |y|, \quad |{}^x y| = |y|^{|x|}.$$

Označme $[x]^n$ množinu všech n-prvkových podmnožin množiny x. Pro x konečnou s $n \leq |x|$ je $|[x]^n| = \binom{|x|}{n}$.

Konečné sekvence.

Predikát „x je sekvence", značený jako $\mathrm{Seq}(x)$, je dán takto:

$$\mathrm{Seq}(x) \Leftrightarrow x \text{ je funkce, jejíž definiční obor je nějaké přirozené číslo.} \tag{1.1}$$

Základní pojmy vztahující se k sekvencím jsou: unární parciální funkce „délka sekvence" x, binární parciální funkce „y-tý člen (prvek) sekvence x", „konkatenace sekvencí x a y", „konkatenace sekvence x sekvencí ", binární predikce „sekvence x je počátkem sekvence y" a konstanta „prázdná sekvence". Značíme je po řadě symboly

$$\mathrm{lh}(x), \quad (x)_y, \text{ stručněji též } x_y, \quad x\smile y, \quad \sqcup(x), \quad x \lessdot y, \quad \emptyset.$$

Je-li x sekvence délky n, můžeme říkat, že to je n-sekvence. Je to ovšem soubor $\langle x_i \rangle_{i<n}$, který zapisujeme též jako

$$\langle x_0, \ldots, x_{n-1} \rangle.$$

Je-li navíc $\mathrm{rng}(x) \subseteq A$, je to sekvence v A. Množinu všech sekvencí v A značíme A^*; tedy

$$A^* = \bigcup_{n \in \mathbb{N}} {}^n A.$$

Sekvenci $\langle x_i \rangle_{i<n}$ resp. její délku značíme též symbolem

$$\overline{x} \quad \text{resp.} \quad \mathrm{l}(\overline{x});$$

pruh nad x má graficky vyznačit, že jde o sekvenci. Místo $\overline{x'}$, $\overline{x^0}$ apod. píšeme $\overline{x}'$, $\overline{x}^0$ apod. Tedy $\overline{x}'$ je $\langle x'_0, \ldots, x'_{n-1} \rangle$ pro nějaké $n \in \mathbb{N}$. Dále místo $\overline{x}_i$ píšeme též jen x_i.

Snadno se zjistí, že platí: konkatenace je asociativní a není komutativní, $\emptyset\smile s = s = s\smile\emptyset$ pro sekvenci s, $\mathrm{l}(s\smile s') = \mathrm{l}(s) + \mathrm{l}(s')$.

Poznamenejme, že $\langle x_0, \ldots, x_{n-1} \rangle$ je sekvence délky n; je prázdná pro $n = 0$ a $\langle x_0 \rangle$ pro $n = 1$.

Kartézská mocnina, n-tice.

Pro $n \in \mathbb{N}$ definujeme n-tou kartézskou mocninu A^n množiny A indukcí:

$$A^0 = \{\emptyset\}, \quad A^1 = A, \quad A^{n+1} = A^n \times A.$$

Prvky z A^n jsou (uspořádané) n-tice v A a dále n-tice je n-tice v nějakém A. Ukážeme, že ${}^n A$ a A^n můžeme „prakticky" ztotožnit. Definujme funkce $(\ )^n : {}^n A \to A^n$ indukcí:

$$(\emptyset)^0 = \emptyset, \qquad (\langle a \rangle)^1 = a \text{ pro } a \in A, \qquad (s\smile\langle b \rangle)^{n+1} = ((s)^n, b) \text{ pro } s \in {}^n A.$$

Každé $(\ )^n$ je prosté zobrazení ${}^n A$ na A^n. Díky tomu ztotožňujeme $s \in {}^n A$ s $(s)^n$ a (tedy) píšeme $\langle s_0, \ldots, s_{n-1} \rangle$ místo $(s)^n$, pokud to nevede k nedorozumění. Máme potom pro $n > 0$ rovnost $\langle a_0, \ldots, a_n \rangle_{n+1} = \langle \langle a_0, \ldots, a_{n-1} \rangle_n, a_n \rangle$.

POZNÁMKA. Uveďme, kdy ztotožnění může vést k nedorozumění. Je-li $s = \langle a_0, \ldots, a_{n-1} \rangle \in {}^n A$, pišme $(s)^n$ jako $(a_0, \ldots, a_{n-1})^n$. Potom tedy je $(a)^1 = a$ pro $a \in A$ a ztotožnění dává $a = \langle a \rangle$, což je neplatná rovnost, hledíme-li na $\langle a \rangle$ jako na sekvenci délky 1. Pro $n > 0$ je $(a_0, \ldots, a_n)^{n+1} = ((a_0, \ldots, a_{n-1})^n, a_n)$. Pro a_0, a_1, a_2 z A může být 3-tice $u = (a_0, a_1, a_2)^3$ $(\in A^3)$, také 2-ticí $((a_0, a_1), a_2)^2$ $(\in A^2)$, je-li (a_0, a_1) v A. Tedy $(s)^3 = u = (s')^2$ pro jisté $s \in {}^3 A$ a $s' \in {}^2 A$. Je ovšem $s \neq s'$ a ztotožnění tedy vede k neplatné rovnosti $s = s'$.

Poznamenejme, že je $|{}^n A| = |A^n| = |A|^n$, speciálně pro A konečné alespoň dvouprvkové je $|A^2| > |A|$. Existuje však nekonečná množina A taková, že $A^2 \subseteq A$.

Uveďme ještě několik užitečných pojmů. Pro n-tici $\overline{a}$ a $k < n$ symbol $\overline{a}(k/b)$ značí n-tici $\overline{a}'$ takovou, že $a'_i = a_i$ pro $k \neq i < n$, $a'_k = b$. Říkáme, že dvě sekvence $\overline{x}, \overline{y}$ jsou disjunktní, když $\mathrm{rng}(\overline{x}) \cap \mathrm{rng}(\overline{y}) = \emptyset$; píšeme též $\overline{x} \cap \overline{y} = \emptyset$.

n-ární relace a funkce.

Buď $n \in \mathbb{N}$. Množina $R \subseteq A^n$ je n-ární relace nad A; n nazýváme četnost R a značíme $\mathrm{ar}(R)$. Speciálně 0-ární relace nad A je $R \subseteq \{\emptyset\}$, 1-ární relace je jakákoli množina (a není to tedy nutně množina dvojic). Označme

$$\mathrm{RL}(A) = \{R;\ R \subseteq A^n \text{ pro nějaké } n \in \mathbb{N}\}.$$

Funkce $F \subseteq A^n \times B$ se nazývá n-ární (parciální) funkce či zobrazení z A do B; její četnost značíme $\mathrm{ar}(F)$ a tedy máme $\mathrm{ar}(F) = n$. Je to totální n-ární zobrazení z A do B, když navíc $\mathrm{dom}(F) = A^n$. Říkáme pak ještě, že to je n-ární operace nad A, když $B = A$. Speciálně 0-ární operace nad A je F tvaru $\{\langle\emptyset, a\rangle\}$ s $a \in A$ a ztotožňujeme ji s a.

Pro relaci $R \subseteq A^n$ resp. zobrazení $F : A^n \to B$ a $\overline{a} = \langle a_0, \dots, a_{n-1}\rangle \in A^n$

$$R(\overline{a}) \text{ značíme též } R(a_0, \dots, a_{n-1}) \qquad \text{resp.} \qquad F(\overline{a}) \text{ značíme též } F(a_0, \dots, a_{n-1}).$$

Induktivní definice.

Nechť F je n-ární funkce a X množina. *F-konkluze* X je množina $F[X^n]$; značíme ji $F\lceil X\rceil$. Tedy $F\lceil X\rceil$ je tvořeno právě prvky $F(x_1, \dots, x_n)$ s $\langle x_1, \dots, x_n\rangle \in X^n \cap \mathrm{dom}(F)$.

1.1.1. $\mathcal{F}$-uzávěr a odvození. Induktivní definice.

Buď $\mathcal{F}$ množina funkcí konečných četností, X množina.

1. *$\mathcal{F}$-konkluze* X je množina $\bigcup\{F\lceil X\rceil;\ F \in \mathcal{F}\}$; značíme ji $\mathcal{F}\lceil X\rceil$. Tedy v $\mathcal{F}\lceil X\rceil$ jsou právě prvky $F(x_1, \dots, x_n)$ s $\langle x_1, \dots, x_n\rangle \in X^n \cap \mathrm{dom}(F)$ pro $F \in \mathcal{F}$, speciálně $F(\emptyset)$ pro $F \in \mathcal{F}$ nulární.

X je $\mathcal{F}$-uzavřená, když obsahuje svou $\mathcal{F}$-konkluzi, tj. když $\mathcal{F}\lceil X\rceil \subseteq X$. *$\mathcal{F}$-uzávěr* X je nejmenší $\mathcal{F}$-uzavřená nadmnožina X; $\mathcal{F}$-uzávěr X značíme $\mathcal{F}\langle X\rangle$.

2. *$\mathcal{F}$-odvození z X* je sekvence s, přičemž pro každé $i < \mathrm{lh}(s)$ je $s_i \in X$ nebo existuje F z $\mathcal{F}$ a $i_0, \dots, i_{n-1} < i$ tak, že n je četnost F a $s_i = F(s_{i_0}, \dots, s_{i_{n-1}})$; říká se pak, že s je $\mathcal{F}$-odvození z X prvku $y = (s)_{\mathrm{lh}(s)-1}$. Prvek je *$\mathcal{F}$-odvozený z X*, existuje-li jeho $\mathcal{F}$-odvození z X.

3. *Induktivní definice* množiny Y z $\mathcal{F}$ a X je seznam pravidel

- každý prvek z X je v Y,
- $F(y_1, \dots, y_n)$ je v Y, jakmile $F \in \mathcal{F}$ je četnosti n a $\langle y_1, \dots, y_n\rangle \in Y^n \cap \mathrm{dom}(F)$. (1.2)

O nejmenší množině Y vyhovující těmto pravidlům říkáme, že to je *množina definovaná induktivní definicí s pravidly* (1.2); je to ovšem množina $\mathcal{F}\langle X\rangle$.

Důkaz indukcí na objektech (též *podle složitosti objektů*) *z* $\mathcal{F}\langle X\rangle$, který prokazuje, že každý prvek z $\mathcal{F}\langle X\rangle$ má vlastnost V, je schema

- každý prvek z $X \cup \{F(\emptyset);\ F \in \mathcal{F} \text{ je nulární}\}$ má vlastnost V,
- když $y_1, \dots, y_n$ z $\mathcal{F}\langle X\rangle$ mají každé vlastnost V, má $F(y_1, \dots, y_n)$ vlastnost V, jakmile $F \in \mathcal{F}$ a $\langle y_1, \dots, y_n\rangle \in \mathrm{dom}(F)$. (1.3)

Druhá položka z (1.3) je *schéma indukčních kroků*, „nechť $y_1, \dots, y_n$ mají vlastnost V" je *indukční předpoklad* indukčního kroku v $y_1, \dots, y_n$ pro F.

Pokud $\mathcal{F}' = \mathcal{F} \cup \{F_x;\ x \in X\}$, kde $F_x = \{\langle\emptyset, x\rangle\}$ je nulární, v (1.2) i (1.3) lze vynechat prvý řádek a ve druhém psát $\mathcal{F}'$ místo $\mathcal{F}$.

TVRZENÍ 1.1.2. *Buď $\mathcal{F}$ množina funkcí konečných četností, X množina. Pak*

1) $\mathcal{F}\langle X\rangle = \bigcup_{n\in\mathbb{N}} X_n$, *kde* $X_0 = X$ *a* $X_{n+1} = X_n \cup \mathcal{F}\lceil X_n\rceil$.

2) $\mathcal{F}\langle X\rangle = \{y;\ y \text{ je } \mathcal{F}\text{-odvozený z } X\}$.

3) *Platí-li* (1.3)*, má každý prvek z* $\mathcal{F}\langle X\rangle$ *vlastnost* V.

4) $X' \subseteq X \Rightarrow \mathcal{F}\langle X'\rangle \subseteq \mathcal{F}\langle X\rangle$, $X \subseteq \mathcal{F}\langle X\rangle = \mathcal{F}\langle\mathcal{F}\langle X\rangle\rangle$.

Důkaz. 1) plyne snadno.

2) Inkluze $\supseteq$. Je-li s nějaké $\mathcal{F}$-odvození z X, je jeho poslední člen v $\mathcal{F}\langle X\rangle$; to plyne ihned indukcí dle délky s užitím $\mathcal{F}$-uzavřenosti $\mathcal{F}\langle X\rangle$. Odtud plyne dokazovaná inkluze.

Inkluze $\subseteq$. Indukcí plyne pro každé n: každé $y \in X_n$ je prvek $\mathcal{F}$-odvozený z X. Pro $n = 0$ to je jasné a indukční krok plyne takto: buď $y = F(z_1, \ldots, z_n) \in X_{n+1}$ s $z_1, \ldots, z_n$ z X_n a s_i buď $\mathcal{F}$-odvození z X prvku z_i pro $i = 1, \ldots n$. Pak $s_1 ⌣ \cdots ⌣ s_n ⌣ y$ je hledané odvození. Jelikož $\mathcal{F}\langle X\rangle = \bigcup_{n\in\mathbb{N}} X_n$, dokazovaná inkluze $\subseteq$ platí.

3) Indukcí snadno plyne pro každé n: každé y z X_n má vlastnost V.

4) Inkluze jsou zřejmé a poslední rovnost plyne z $\mathcal{F}$-uzavřenosti $\mathcal{F}\langle X\rangle$. □

Velikosti množin.

Dvě množiny x a y jsou stejně velké, když jsou ekvivalentní, tj. $x \approx y$. Existuje třída **Cn** tzv. kardinálních čísel, představující typy velikostí množin, tj. za předpokladu axiomu výběru lze ke každé množině x najít právě jedno $\kappa \in \mathbf{Cn}$ tak, že $x \approx \kappa$; uvedené κ je velikost či kardinalita či mohutnost x a značí se $|x|$. Je $\mathbb{N} \subseteq \mathbf{Cn}$ a pro x konečnou je $|x| \in \mathbb{N}$. Písmena κ, λ, μ značí kardinální čísla.

Na **Cn** je dáno dobré uspořádání $\leq$ a podobně jako pro přirozená čísla platí i pro všechny kardinály $\kappa < \lambda \Leftrightarrow \kappa \in \lambda \Leftrightarrow \kappa \subsetneq \lambda$. Navíc pro množinu $x \subseteq \mathbf{Cn}$ je $\bigcup x$ supremum x v tomto uspořádání. $\mathbb{N}$ je počáteční úsek uspořádání $\leq$. První kardinál z $\mathbf{Cn} - \mathbb{N}$ je nejmenší nekonečný kardinál a značí se ω či $\aleph_0$. Je $\omega = \mathbb{N}$ a prvek z ω, tj. přirozené číslo, je konečný kardinál. Množina kardinality ω se nazývá spočetná množina. Nekonečná množina, která není spočetná, se nazývá nespočetná. Nejmenší kardinál větší než κ se nazývá následník κ a značí se κ^+. Definujeme indukcí: $\omega_0 = \omega$, $\omega_{n+1} = (\omega_n)^+$. Dále ω_ω je nejmenší kardinál větší než každé ω_n s $n < \omega$. Místo ω_i se píše také $\aleph_i$ pro $i \leq \omega$. Třída **Cn** není množina, neboť jinak by pro supremum κ množiny **Cn** bylo $|\mathcal{P}(\kappa)| \leq \kappa$. Zápis $\kappa < \omega$ značí, že $\kappa \in \mathbb{N}$, $\kappa \geq \omega$ pak, že κ je nekonečný kardinál. Kardinalita množiny $\mathcal{P}(\mathbb{N})$ se značí $\mathfrak{c}$ a nazývá se kontinuum; tedy $\mathfrak{c} = |\mathcal{P}(\mathbb{N})| = |{}^\omega 2|$ a také $\mathfrak{c} = |\mathbb{R}|$. Podle Cantorovy věty je $\omega < \mathfrak{c}$, tedy $\mathfrak{c} \geq \omega^+$. Rovnost $\mathfrak{c} = \omega_1$ se nazývá hypotéza kontinua a značí se (CH). Z axiomů obvyklé, tj. Zermelo-Fraenkelovy teorie množin s axiomem výběru ZFC, nelze hypotézu kontinua ani dokázat ani vyvrátit. Je to jedno z nejznámějších nezávislých tvrzení teorie množin. Je-li teorie ZFC bezesporná, je bezesporná i s (CH), ale např. i s $\mathfrak{c} = \omega_5$. Začátek kardinální škály můžeme zapsat takto:

$$0 < 1 < 2 < \cdots < n < n+1 < \cdots < \omega < \omega_1 < \omega_2 < \cdots < \omega_\omega < (\omega_\omega)^+ < \cdots .$$

Aritmetika kardinálních čísel. Na **Cn** je definováno $+$, $\cdot$ a mocnina, přičemž tyto operace rozšiřují analogické na $\mathbb{N}$:

$$\kappa + \lambda \approx \kappa \uplus \lambda, \qquad \kappa \cdot \lambda \approx \kappa \times \lambda, \qquad \kappa^\lambda \approx {}^\lambda\kappa. \tag{1.4}$$

Značení.

1. Množina všech podmnožin $u \subseteq x$ s $|u| = \lambda$ resp. s $|u| < \lambda$ se značí

$$[x]^\lambda \text{ resp. } [x]^{<\lambda}.$$

Speciálně $[x]^{<\omega}$ je množina všech konečných podmnožin množiny x.

2. Pro $\diamond$ rovno $<$ či $\leq$ a velikost (číslo) κ značí symbol

$$\kappa(\diamond) \text{ resp. } \kappa(\diamond, \infty)$$

počet velikostí (čísel) λ takových, že $\lambda \diamond \kappa$ resp. navíc je λ nekonečné.
Např. tedy platí

$$n(<) = n \text{ pro } n \in \mathbb{N},\ \omega(<) = \omega = \omega(\leq),\ \omega(<, \infty) = 0,\ \omega(\leq, \infty) = 1,\ |\mathbf{Cn} \cap \kappa| = \kappa(<).$$

TVRZENÍ. (Počítání s kardinalitami a kardinály.)

C1) a) $|x \cup y| \leq |x| + |y|$. b) $|\bigcup_{i\in I} x_i| \leq |I| \cdot \lambda$, *je-li* $|x_i| \leq \lambda$ *pro každé* $i \in I$.

C2) a) $|\mathcal{P}(x)| = 2^{|x|} = |{}^x 2|$. b) $\mathfrak{c} = 2^\omega$.

C3) *Pro* $+, \cdot$ *platí obvyklá komutativita, asociativita a distributivita.*
Platí obvyklé vzorce o mocnině: $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$, $(\kappa^\lambda)^\mu = \kappa^{\lambda\cdot\mu}$.
Monotonie: když $\kappa \leq \kappa_0, \lambda \leq \lambda_0$, *tak* $\kappa + \lambda \leq \kappa_0 + \lambda_0$, $\kappa \cdot \lambda \leq \kappa_0 \cdot \lambda_0$, $0 < \kappa \Rightarrow \kappa^\lambda \leq \kappa_0^{\lambda_0}$.

C4) *Je-li alespoň jeden kardinál* κ, λ *nekonečný a oba jsou nenulové, platí*
$$\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda).$$
Speciálně: Je-li x *nekonečná,* $y \subseteq x$ *a* $|y| < |x|$, *tak* $|x - y| = |x|$.

C5) *Pro* $\kappa \geq \omega$ *a* $0 < n \in \mathbb{N}$ *platí:* a) $\kappa^n \approx \kappa$. b) $\lambda \leq \kappa \Rightarrow [\kappa]^\lambda = \kappa^\lambda$.
c) $|[\kappa]^{<\omega}| = \kappa$. d) $2 \leq \lambda \leq \kappa \Rightarrow 2^\kappa = \lambda^\kappa$.

Tedy např: $\omega = \omega + 1 = \omega + \omega = \omega \cdot \omega = \omega \cdot \omega + 5 = \omega^7 < \omega^\omega = 2^\omega = (2^\omega)^\omega$.

V následujícím tvrzení je uvedeno několik užitečných poznatků týkajících se velikosti množin.

TVRZENÍ.

1) *Pro nekonečnou množinu* x *platí:*
a) i) $x^* \approx x$, *ii)* $[x]^{|x|} \approx \mathcal{P}(x)$.
b) x *lze rozložit na* $|x|$ *disjunktních množin, majících každá kardinalitu* $|x|$.

2) *Všech relací resp. operací nad* A, *které mají konečné četnosti, je*
a) ω, *pokud* $2 \leq |A| < \omega$, *b)* $2^{|A|}$, *pokud* $|A| \geq \omega$.

3) *Buď* $A \neq \emptyset$. *Pro* $U, U' \subseteq A$ *je* $\langle A, U\rangle$ *izomorfní s* $\langle A, U'\rangle$, *píšeme* $\langle A, U\rangle \cong \langle A, U'\rangle$, *když existuje prosté zobrazení* A *na* A *převádějící* U *na* U'. *Pak platí:*
Až na izomorfnost je dvojic $\langle A, U\rangle$ *s* $U \subseteq A$ *právě* $|A|(\leq)$.

Důkaz. 1) a) i). Je $x^* = \bigcup_{i<\omega} {}^i x$. Tedy $x \preccurlyeq x^* \preccurlyeq \omega \cdot |x| \approx x$ a odtud $x \approx x^*$. Přitom jsme užili C1) b), C4), C5) a). ii) plyne ihned z C2) a) a C5) b), d). b) Buď $\kappa = |x|$; $\{\{i\} \times \kappa;\ i \in \kappa\}$ je rozklad $\kappa \times \kappa$ na κ disjunktních množin majících každá kardinalitu κ; díky $\kappa \times \kappa \approx \kappa$ platí dokazované.

2) a) Je $2 \leq |A| < \omega$. Pak množina všech uvažovaných relací je $\bigcup_{n<\omega} \mathcal{P}(A^n)$, což je spočetné sjednocení neprázdných konečných množin a tedy to je množina spočetná. Množina všech uvažovaných operací je $\bigcup_{n<\omega} {}^{A^n}\!A$, což je spočetné sjednocení neprázdných konečných množin a tedy to je množina spočetná. b) Relací $R \subseteq A^n$ s $0 < n < \omega$ je $|\mathcal{P}(A^n)| = 2^{|A|}$, neboť $|A^n| = |A|$ dle C5) a). Množina všech uvažovaných relací je tedy spočetné sjednocení množin kardinality $2^{|A|}$, což je množina kardinality $2^{|A|}$ dle C1) b) (neboť je alespoň kardinality $2^{|A|}$). Podobně je tomu s operacemi $F : A^n \to A$.

3) Zřejmě $\langle A, U\rangle \cong \langle A, U'\rangle \Leftrightarrow |U| = |U'|$ a $|A - U| = |A - U'|$. Stačí už tedy jen dokázat: Všech dvojic $\langle |U|, |A - U|\rangle$ s $U \subseteq A$ je právě $|A|(\leq)$. Pro $|A| < \omega$ to platí, neboť $|A - U|$ je jednoznačně určeno $|U|$. Buď $|A| \geq \omega$. Všech uvažovaných dvojic s $|U| < |A|$ je $|A|(<)$ a těch, pro které $|U| = |A|$, je právě $|A|(\leq)$ (neboť $|A - U|$ je libovolný kardinál $\leq |A|$); celkem jich tedy je právě $|A|(\leq)$. $\square$

1.2 Booleovy algebry.

1.2.1. Booleova algebra. Podalgebra. Homomorfizmus, vnoření, izomorfizmus.

1. *Booleova algebra*, krátce *algebra*, je šestice $\underline{B} = \langle B, -, \vee, \wedge, 0, 1\rangle$, kde
B je neprázdná množina,
$-$ je unární, $\vee, \wedge$ jsou binární operace na B, $0, 1$ jsou nějaké prvky z B,
přičemž jsou splněny tzv. *booleovské zákony* (též *axiomy*), tj. pro x, y, z z B platí:

asociativita	$x \diamond (y \diamond z) = (x \diamond y) \diamond z$	$\diamond$ je $\vee$ nebo $\wedge$
komutativita	$x \diamond y = y \diamond x$	$\diamond$ je $\vee$ nebo $\wedge$
distributivita	$x \diamond (y \diamond' z) = (x \diamond y) \diamond' (x \diamond z)$	$\diamond$ $[\diamond']$ je $\vee$ $[\wedge]$ nebo $\wedge$ $[\vee]$
absorbce	$x \vee (x \wedge y) = x = x \wedge (x \vee y)$	
komplementace	$x \vee (-x) = 1, \quad x \wedge (-x) = 0$	
netrivialita	$0 \neq 1.$	

B je *univerzum* algebry $\underline{B}$, $-$ komplement, $\vee$ spojení, $\wedge$ průsek, 0 resp. 1 je (booleovská) nula resp. jednička. Na 0 resp. 1 hledíme též jako na nulární operaci, přiřazující $\emptyset \in B^0$ hodnotu 0 resp. 1. *Velikost algebry* $\underline{B}$ je velikost jejího univerza. Poznamenejme, že Booleova algebra je tzv. struktura prvého řádu s jednou unární, dvěma binárními a dvěma nulárními operacemi, přičemž univerzum je alespoň dvouprvkové.

Vezme-li se místo netriviality zákon triviality, tj. $0 = 1$, nazývá se $\underline{B}$ *triviální Booleova algebra.*

2. *Podalgebra* Booleovy algebry $\underline{B} = \langle B, -, \vee, \wedge, 0, 1\rangle$ je algebra $\underline{A} = \langle A, -', \vee', \wedge', 0', 1'\rangle$, kde $A \subseteq B$ a každá operace $\diamond'$ je zúžením $\diamond$ na A (speciálně $0' = 0$, $1' = 1$.) Píšeme pak

$$\underline{A} \subseteq \underline{B}$$

a podalgebru $\underline{A}$ značíme také symbolem $\underline{B}\restriction A$. Zřejmě je $A \subseteq B$ univerzem nějaké podalgebry algebry $\underline{B}$, právě když je A neprázdná množina *uzavřená* na všechny operace algebry $\underline{B}$, tj. každá operace Booleovy algebry $\underline{B}$ zobrazí prvky z A do A; speciálně je $0, 1 \in A$. Je-li tedy A neprázdná podmnožina B uzavřená na operace algebry B, je $\underline{B}\restriction A$ podalgebra $\underline{B}$ s univerzem A. Zřejmě je $\underline{A} = \underline{B}\restriction \{0, 1\}$ podalgebra algebry $\underline{B} = \langle B, -, \vee, \wedge, 0, 1\rangle$; $\underline{A}$ nemá vlastní podalgebru (tj. s univerzem menším než A).

3. Buďte $\underline{B} = \langle B, -, \vee, \wedge, 0, 1\rangle$, $\underline{B'} = \langle B', -', \vee', \wedge', 0', 1'\rangle$ Booleovy algebry. Zobrazení h univerza B do B' je *homomorfizmus* algebry $\underline{B}$ do $\underline{B'}$, když platí:

pro každé $a, b \in B$ je $h(-a) = -'h(a)$, $h(a \diamond b) = h(a) \diamond' h(b)$, kde $\diamond$ je $\vee$ nebo $\wedge$,

$h(0) = 0'$, $h(1) = 1'$.

Je-li navíc h prosté, je to *(izomorfní) vnoření* $\underline{B}$ do $\underline{B'}$. Je-li ještě navíc h zobrazení na B', je to *izomorfizmus* $\underline{B}$ a $\underline{B'}$; říkáme pak, že $\underline{B}$ je izomorfní s $\underline{B'}$ *via* h a píšeme také $\underline{B} \cong \underline{B'}$ (via h).

1.2.2. Produkt a mocnina Booleových algeber.

Buď $\langle \underline{B}_i\rangle_I$ neprázdný soubor Booleových algeber; jeho *produkt* je algebra $\langle \prod_I B_i, -^*, \vee^*, \wedge^*, 0^*, 1^*\rangle$, kde každá operace je definována „po složkách“:

$$(-^* f)(i) = -^{B_i} f(i), \quad (f \diamond^* g)(i) = f(i) \diamond^{B_i} g(i), \quad \diamond^*(i) = \diamond^{B_i} \text{ pro každé } i \in I,$$

přičemž $\diamond$ je $\vee$, $\wedge$, 0 či 1. Tento produkt značíme

$$\textstyle\prod_I \underline{B}_i.$$

Když $\underline{B}_i = \underline{B}$ pro každé $i \in I$, píšeme ${}^I\underline{B}$ místo $\prod_I \underline{B}_i$ a říkáme, že to je I-tá *mocnina* $\underline{B}$. Když $0 < n \in \omega$, píšeme $\underline{B}_0 \times \cdots \times \underline{B}_{n-1}$ místo $\prod_n \underline{B}_i$. Dále ${}^1\underline{B}$ ztotožňujeme s $\underline{B}$. *Projekce* $\pi_j : \prod_I B_i \to B_j$ je definovaná vztahem $\pi_j(f) = f(j)$ pro $j \in I$. Zřejmě to je homomorfizmus $\prod_I \underline{B}_i$ na $\underline{B}_j$.

PŘÍKLADY 1.2.3.

1. a) *Potenční Booleova algebra* je algebra

$$\underline{\mathcal{P}}(I) = \langle \mathcal{P}(I), -^I, \cup, \cap, \emptyset, I\rangle,$$

kde $-^I$ je komplement do I, tj. operace $-^I : \mathcal{P}(I) \to \mathcal{P}(I)$ taková, že pro $u \subseteq I$ je $-^I u = I - u$; místo $-^I$ píšeme stručně jen $-$. Pro $I = \emptyset$ jde o triviální algebru.

b) Podalgebra $\underline{\mathcal{P}}(I)$ s univerzem tvořeným konečnými a kokonečnými (tj. komplementy konečných) podmnožinami I se značí

$$\mathrm{FA}(I). \tag{1.5}$$

Je-li I konečná, je to $\underline{\mathcal{P}}(I)$, jinak má velikost jako množina I.

2. a) Dvouprvková Booleova algebra (pravdy a lži) je

$$\underline{2} = \langle 2, -_1, \vee_1, \wedge_1, 0, 1\rangle, \tag{1.6}$$

kde $2 = \{0,1\}$, $-_1 : 2 \to 2$ a $-_1(0) = 1$, $-_1(1) = 0$, $\vee_1 : 2 \times 2 \to 2$ a $\vee_1(x,y) = \max(x,y)$, $\wedge_1 : 2 \times 2 \to 2$ a $\wedge_1(x,y) = \min(x,y)$.

b) Obecněji pro $I \neq \emptyset$ je ${}^{I}\underline{2} = \langle {}^{I}2, -_I, \vee_I, \wedge_I, 0_I, 1_I\rangle$ a zřejmě pak

$$\underline{\mathcal{P}}(I) \cong {}^{I}\underline{2} \text{ via } u \mapsto \mathrm{ch}_u, \text{ kde } \mathrm{ch}_u \text{ je charakteristická funkce } u \text{ na } I.$$

Pro $0 < m < n \in \mathbb{N}$ je každá Booleova algebra ${}^{m}\underline{2}$ až na izomorfizmus podalgebrou ${}^{n}\underline{2}$ a také podalgebrou ${}^{\mathbb{N}}\underline{2}$.

3. a) $\underline{\mathrm{C}}_p$ pro $0 < p \in \mathbb{N}$ je podalgebra algebry ${}^{\mathbb{N}}\underline{2}$ s univerzem $\mathrm{C}_p \subseteq {}^{\mathbb{N}}2$ tvořeným právě všemi funkcemi $f \in {}^{\mathbb{N}}2$, které mají periodu p, tj. $f(i) = f(i+p)$ pro každé $i \in \mathbb{N}$.

b) $\underline{\mathrm{C}}_\infty$ je podalgebra algebry ${}^{\mathbb{N}}\underline{2}$ s univerzem $\mathrm{C}_\infty \subseteq {}^{\mathbb{N}}2$ tvořeným právě všemi funkcemi $f \in {}^{\mathbb{N}}2$, které mají nějakou periodu p, $0 < p \in \mathbb{N}$, tj. $f(i) = f(i+p)$ pro každé $i \in \mathbb{N}$.

1.2.4. Booleovské operace. Disjunktnost, konečné rozklady jedničky.

1. *Booleovská operace* je operace složená z operací komplement, spojení, průsek, konstant nula a jedna Booleovy algebry a z identity; její zápis pomocí symbolů značících operaci komplementu, spojení, průseku, nulu, jedničku a proměnnou je booleovský term. Booleovský term je například $(x \wedge -y) \vee z$; je v proměnných x, y, z. Je-li $t(x_0, \dots, x_{n-1})$ booleovský term v proměnných $x_0, \dots, x_{n-1}$ a $b_0, \dots, b_{n-1}$ jsou prvky algebry $\underline{B}$, značí $t(b_0, \dots, b_{n-1})$ hodnotu booleovské operace představované termem t, spočítané v $\underline{B}$ v argumentech $b_0, \dots, b_{n-1}$. Je-li h izomorfizmus $\underline{B}$ a $\underline{A}$, je $t(h(b_0), \dots, h(b_{n-1})) = h(t(b_0, \dots, b_{n-1}))$.

Jsou-li $t_1, \dots, t_n$ booleovské termy, tak term tvaru

$$t_1 \vee \ldots \vee t_n \quad \text{resp.} \quad t_1 \wedge \ldots \wedge t_n$$

se nazývá *konečné spojení* resp. *průsek termů* $t_1, \dots, t_n$. Jeho hodnota počítaná v dané algebře nezávisí na pořadí a uzávorkování argumentů díky komutativitě a asociativitě, tudíž závorky jsme vypustili. *Elementární průsek* je konečný průsek tvaru $x_0^{\sigma(0)} \wedge \cdots \wedge x_{n-1}^{\sigma(n-1)}$, kde $x_0, \dots, x_{n-1}$ jsou různé proměnné a $\sigma : n \to 2$. Přitom zde značí x^0 resp. x^1 term $-x$ resp. proměnnou x.

2. Buď $\underline{B} = \langle B, -, \vee, \wedge, 0, 1\rangle$. Množina $X \subseteq B$ je *disjunktní*, když neobsahuje nulu a každé její dva různé prvky jsou *disjunktní prvky*, tj. jejich průsekem je nula v $\underline{B}$. Množina $\{b_0, \dots, b_{n-1}\}$ je rozklad jedničky v $\underline{B}$, je-li to množina disjunktní a $b_0 \vee \cdots \vee b_{n-1} = 1$.

TVRZENÍ 1.2.5. (O konečných podalgebrách.) *Buďte $b_0, \dots, b_{n-1}$ prvky Booleovy algebry $\underline{B}$. Pak hodnoty elementárních průseků $b_0^{\sigma(0)} \wedge \cdots \wedge b_{n-1}^{\sigma(n-1)}$ s $\sigma \in {}^{n}2$ a po vynechání nuly tvoří disjunktní rozklad D jedničky v $\underline{B}$ a všechna konečná spojení prvků z D univerzum nejmenší podalgebry algebry $\underline{B}$, obsahující $b_0, \dots, b_{n-1}$; tato podalgebra má nejvýše 2^{2^n} prvků.*

Důkaz. Indukcí dle n se dokáže, že D je disjunktní rozklad jedničky. Pro $n = 1$ to platí. Indukční krok z n na $n+1$: máme-li již D pro $b_0, \dots, b_{n-1}$, vzniknou z každého prvku $a \in D$ nejvýše dva nenulové prvky $a \wedge b_n$, $a \wedge -b_n$ a jejich spojením je právě a. Prvky $a \wedge b_n$, $a \wedge -b_n$ s $a \in D$ jsou tedy právě nenulové elementární průseky $b_0^{\sigma(0)} \wedge \cdots \wedge b_n^{\sigma(n)}$ a tvoří zjevně rozklad D' jedničky. Jasně je každý prvek b_i s $i \leq n$ spojení některých prvků z D'. Zbytek tvrzení je zřejmý. □

1.2.6. *Booleovská identita v algebře $\underline{B}$* je nějaká rovnost booleovských termů, platná identicky v $\underline{B}$. Je to *booleovská identita*, pokud to je booleovská identita v každé Booleově algebře.

TVRZENÍ 1.2.7. (O booleovských identitách.) *Rovnost booleovkých termů je booleovská identita, právě když to je booleovská identita v algebře $\underline{2}$.*

Důkaz. Stačí dokázat implikaci z prava do leva. Nech $t(x_1, \dots, x_n) = s(x_1, \dots, x_n)$ je booleovská identita v $\underline{2}$. Pak to je booleovská identita v konečné algebře $\mathcal{A}$, protože $\underline{A} \cong {}^{m}\underline{2}$ pro jisté m a operace v ${}^{m}\underline{2}$ jsou definovány po složkách v $\underline{2}$. Buď $\underline{B}$ libovolná algebra, $b_1, \dots, b_n$ její prvky. Máme ukázat, že $t(b_1, \dots, b_n) = s(b_1, \dots, b_n)$. Buď $\underline{A}$ konečná podalgebra algebry $\underline{B}$ s $\{b_1, \dots, b_n\} \subseteq A$; taková podalgebra existuje. Víme již, že $t(b_1, \dots, b_n) = s(b_1, \dots, b_n)$ počítáno v $\underline{A}$. Hodnoty

$t(b_1, \dots, b_n)$, $s(b_1, \dots, b_n)$ počítané v $\underline{A}$ a $\underline{B}$ jsou stejné, tedy $t(b_1, \dots, b_n) = s(b_1, \dots, b_n)$ počítáno v $\underline{B}$, což jsme měli dokázat. $\Box$

Uspořádání Booleovy algebry. Booleovská pravidla.

1.2.8. Kanonické uspořádání, $-$, $\dot{-}$, $\to$, $\leftrightarrow$. Booleovské operace a identity.

V Booleově algebře $\underline{B} = \langle B, -, \vee, \wedge, 0, 1\rangle$ definujeme *kanonické uspořádání* $\le$ na B a binární operace $-$ *rozdíl*, *symetrická diference* $\dot{-}$, (booleovskou) *implikaci* $\to$, (booleovskou) *ekvivalenci* $\leftrightarrow$ takto:

$$\begin{aligned} a \le b \Leftrightarrow a = a \wedge b, \quad & a - b = a \wedge (-b), \quad & a \dot{-} b = (a - b) \vee (b - a),\\ & a \to b = -a \vee b, \quad & a \leftrightarrow b = (a \to b) \wedge (b \to a). \end{aligned}$$

1.2.9. Booleovská pravidla jsou následující booleovské identity popř. tvrzení platná v Booleově algebře $\langle B, -, \vee, \wedge, 0, 1\rangle$ pro $x, y, z, x', y' \in B$:

Idempotence:	$x \vee x = x$, $x \wedge x = x$
	$x \vee y = x \Leftrightarrow x \wedge y = y$
	$\le$ je uspořádání, $x \vee y = \sup_{\le}\{x, y\}$, $x \wedge y = \inf_{\le}\{x, y\}$
Monotonie:	$x \le y$ a $x' \le y' \Rightarrow x \vee x' \le y \vee y'$ a $x \wedge x' \le y \wedge y'$
Extremalita:	$x \vee 1 = 1$, $x \wedge 0 = 0$
Neutralita:	$x \vee 0 = x$, $x \wedge 1 = x$
	$x \wedge y = 0$ a $x \vee y = 1 \Leftrightarrow y = -x$, $0 = -1$, $1 = -0$
De Morgan:	$x \wedge y = -(-x \vee -y)$, $\quad x \vee y = -(-x \wedge -y)$

$$\begin{aligned} &-(-x) = x, && x \le y \Leftrightarrow -y \le -x\\ &x \dot{-} y = y \dot{-} x, && (x \dot{-} y) \dot{-} z = x \dot{-} (y \dot{-} z)\\ &-(x - y) = x \to y, && -(x \dot{-} y) = x \leftrightarrow y\\ &x \wedge y = 1 \Leftrightarrow x = 1 = y, && x \vee y = 0 \Leftrightarrow x = 0 = y \end{aligned}$$
$$x \le y \Leftrightarrow (x \to y = 1)$$

Důkaz lze provést zcela rutinně pomocí booleovských zákonů nebo pomocí 1.2.7. $\Box$

Vidíme, že kanonické uspořádání $\le$ Booleovy algebry $\underline{B}$ má nejmenší prvek 0 a největší 1 a každá konečná množina $s \subseteq B$ má supremum a infimum, $\langle B, \le\rangle$ je tedy svaz. Definujeme operace $\bigvee$ a $\bigwedge$ z množiny $\{u \subseteq B;\ u$ je konečná$\}$ do B:

$$\bigvee u = \sup_{\le} u, \quad \bigwedge u = \inf_{\le} u; \qquad \text{speciálně je} \quad \bigvee \emptyset = 0, \quad \bigwedge \emptyset = 1.$$

Platí ovšem

$$\bigwedge\{x_0, \dots, x_{n-1}\} = x_0 \wedge \dots \wedge x_{n-1}, \qquad \bigvee\{x_0, \dots, x_{n-1}\} = x_0 \vee \dots \vee x_{n-1};$$

závorky v uvedených výrazech díky asociativitě a komutativitě vynecháváme.

1.2.10. Relativizace Booleovy algebry na prvek.

Buď B Booleova algebra, $a \in B$. *Relativizace* B *na* a je Booleova algebra s univerzem $B \restriction a = \{x;\ x \le a\}$ a s operacemi $\wedge, \vee, 0$ algebry B jakožto průsekem, spojením, nulou algebry, komplementem $-^{B \restriction a} x = a - x$ (pro $x \in B \restriction a$) a jednotkou a. Značíme ji

$$B \restriction a.$$

Poznamenejme, že jde jasně o Booleovu algebru. Jejím kanonickým uspořádádním je zřejmě parcializace kanonického uspořádání algebry B na množinu $B \restriction a$. Dále je zřejmě „projekce“ $x \mapsto x \wedge a$ homomorfizmus algebry B na algebru $B \restriction a$.

TVRZENÍ 1.2.11. *Buď B Booleova algebra, $a \in B$. Pak platí*

$$B \cong (B \restriction a) \times (B \restriction -a).$$

Důkaz. Buďte $g : B \to (B \restriction a) \times (B \restriction -a)$ a $h : (B \restriction a) \times (B \restriction -a) \to B$ definovány takto:

$$g(x) = \langle x \wedge a, x \wedge -a\rangle, \quad h(\langle y, z\rangle) = y \vee z.$$

Zřejmě je g homomorfizmus, neboť $g(-x) = \langle -x \wedge a, -x \wedge -a\rangle = \langle -^{B\upharpoonright a}x, -^{B\upharpoonright -a}x\rangle$ a je to izomorfizmus, neboť h je inverzní ke g. □

Atomy a (bez)atomárnost.

1.2.12. Atomy v Booleově algebře.

1. *Atom* v Booleově algebře je nenulový prvek, pod kterým leží jen nula a on sám. Jinak řečeno: atomy Booleovy algebry jsou právě minimální prvky množiny jejích nenulových prvků v kanonickém uspořádání. Množinu všech atomů Booleovy algebry $\underline{B}$ označíme At_B.

2. Booleova algebra je *atomární*, leží-li pod každým jejím nenulovým prvkem atom. Booleova algebra je *bezatomární*, neexistuje-li v ní žádný atom.

Zřejmě platí:

Každá konečná netriviální Booleova algebra je atomární.

Nenulový prvek a Booleovy algebry $\underline{B}$ je její atom, právě když platí:

$$\text{pro každé } b \in B \text{ je } a \leq^B b \text{ nebo } a \leq^B -b. \tag{1.7}$$

TVRZENÍ 1.2.13. *Buď $\underline{B}$ atomární Booleova algebra. Zobrazení $h : B \to \mathcal{P}(\mathrm{At}_B)$, kde $h(b) = \{a;\ a \leq b, a \text{ je atom v } \underline{B}\}$, je izomorfizmus $\underline{B}$ a nějaké podalgebry potenční algebry $\underline{\mathcal{P}}(\mathrm{At}_B)$. Je-li $\underline{B}$ konečná, je h izomorfizmus $\underline{B}$ a $\underline{\mathcal{P}}(\mathrm{At}_B)$.*

Speciálně jsou každé dvě konečné Booleovy algebry izomorfní, právě když mají týž počet atomů.

Důkaz. Buďte $b, b' \in B$. h je prosté, neboť když $b - b' \neq 0$, existuje atom $a \leq b - b'$; pak není $a \leq b'$ a tedy $h(b') \neq h(b)$. Zřejmě $h(-^B b) = \mathrm{At}_B - h(b)$, $h(b \wedge^B b') = h(b) \cap h(b')$, $h(b \vee^B b') = h(b) \cup h(b')$. $h(0^B) = \emptyset$ a $h(1^B) = \mathrm{At}_B$; h je tedy izomorfizmus B a podalgebry $\underline{\mathcal{P}}(\mathrm{At}_B)$ s univerzem $\{h(b);\ b \in B\}$. Je-li $\underline{B}$ konečná, je At_B konečné a h je zřejmě na $\underline{\mathcal{P}}(\mathrm{At}_B)$. □

TVRZENÍ 1.2.14. *$\underline{\mathrm{C}}_\infty$ je spočetná bezatomární Booleova algebra. Je to až na izomorfizmus jediná spočetná bezatomární Booleova algebra.*

Důkaz. C_∞ je sjednocením spočetně množin C_p s $0 < p \in \mathbb{N}$, přičemž $|\mathrm{C}_p| = 2^p$; tudíž C_∞ je spočetná množina. Je-li $f \in {}^{\mathbb{N}}2$ nenulová s periodou $0 < p \in \mathbb{N}$ a $i < p$ splňuje $f(i) = 1$, pak g lišící se od f jen v $i + 2kp$ pro každé $k \in \mathbb{N}$ je nenulový prvek algebry $\underline{\mathrm{C}}_\infty$ a menší než f. Buďte $\underline{A}$, $\underline{B}$ spočetné bezatomární Booleovy algebry, h izomorfizmus konečné podalgebry $\underline{A}\upharpoonright A'$ a $\underline{B}\upharpoonright B'$. Pak pro $a \in A - A'$ existuje $b \in B$ tak, že h lze rozšířit do izomorfizmu $\underline{A}\upharpoonright A''$ a $\underline{B}\upharpoonright B''$, kde $\underline{A}\upharpoonright A''$ resp. $\underline{B}\upharpoonright B''$ je nejmenší podalgebra algebry $\underline{A}$, obsahující $A' \cup \{a\}$ resp. $\underline{B}$, obsahující $B' \cup \{b\}$. Univerza A'', B'' jsou konečná a jejich existence plyne z bezatomárnosti $\underline{A}$, $\underline{B}$. Na základě tohoto poznatku můžeme indukcí sestrojit hledaný izomorfizmus, vyjdeme-li z $A' = \{0, 1\} \subseteq A$, $B' = \{0, 1\} \subseteq B$. □

POZNÁMKA. Algebra AV výroků nad spočetně prvovýroky je spočetná bezatomární Booleova algebra. AV je tvořená faktory $\varphi/\!\sim\, = \{\psi;\ \varphi \sim \psi\}$ výroků φ nad uvažovanou spočetnou množinou prvovýroků, přičemž $\varphi \sim \psi \ \Leftrightarrow\ \models \varphi \leftrightarrow \psi$. Booleovským operacím odpovídají $\neg$, $\vee$, &, $\perp$ (falešný výrok), $\top$ (tautologie).

Kongruence, faktoralgebry. Ideály a filtry.

Faktorizace Booleovy algebry $\underline{B}$ podle netriviální kongruence $\sim$ je důležitá konstrukce, poskytující tzv. faktoralgebru $\underline{B}/\!\sim$ často velmi odlišnou od $\underline{B}$. Neformálně řečeno je $\sim$ nová rovnost na B (hrubší než identita), prvky univerza $\underline{B}/\!\sim$ jsou faktory ekvivalence $\sim$ (tvaru $b/\!\sim$ s $b \in B$), a operace algebry $\underline{B}$ se definují korektně pomocí reprezentantů faktorů. S faktorizací je úzce spojen pojem ideálu a filtru v Booleově algebře.

1.2.15. Kongruence, ideály a filtry v Booleově algebře.

Buď $\underline{B}$ Booleova algebra.

1. *Netriviální kongruence pro $\underline{B}$* je ekvivalence $\sim$ na B s alespoň dvěma faktory a taková, že platí, přičemž $\diamond$ značí $\vee$ nebo $\wedge$:

$$a \sim a', b \sim b' \;\Rightarrow\; -a \sim -a',\, a \diamond b \sim a' \diamond b'.$$

Pak na množině $B/{\sim} = \{a/{\sim};\, a \in B\}$ faktorů ekvivalence $\sim$ se definují operace $\tilde{-}$, $\tilde{\diamond}$ korektně pomocí reprezentantů a $\langle B/{\sim}, \tilde{-}, \tilde{\vee}, \tilde{\wedge}, 0/{\sim}, 1/{\sim}\rangle$ je Booleova algebra, zvaná *faktoralgebra* $\underline{B}$ podle $\sim$; značí se $\underline{B}/{\sim}$; to že v ní platí axiom $0 \neq 1$ je právě zaručeno netriviálností kongruence $\sim$: $0^B/{\sim} \neq 1^B/{\sim}$.

2. *Ideál* resp. *filtr* v $\underline{B}$ je neprázdná množina $D \subseteq B$ taková, že

$$1 \notin D, \quad a, b \in D \Rightarrow a \vee b \in D, \quad a \leq b \in D \Rightarrow a \in D \quad \text{resp.}$$
$$0 \notin D, \quad a, b \in D \Rightarrow a \wedge b \in D, \quad a \geq b \in D \Rightarrow a \in D.$$

Duální filtr k ideálu D je $\{-a;\, a \in D\}$, *duální ideál* k filtru D je $\{-a;\, a \in D\}$.

Hlavní filtr je filtr, který obsahuje nejmenší prvek (v uspořádání Booleovy algebry). *Ultrafiltr* je filtr D takový, že pro každé $a \in B$ je $a \in D$ nebo $-a \in D$. Množina všech ultrafiltrů algebry $\underline{B}$ je *Stoneův prostor* $\underline{B}$ a značí se $\mathrm{S}(\underline{B})$. Duální ideál k ultrafiltru se nazývá *prvoideál*.

Zřejmě je hlavní filtr právě horní množina nad nějakým nenulovým prvkem. Dále filtr může obsahovat nejvýše jeden atom díky uzavřenosti na průsek a filtr s jedním atomem je právě hlavní ultrafiltr.

TVRZENÍ 1.2.16. (O faktorizaci, kongruencích a filtrech Booleovy algebry.) *Buď B Booleova algebra.*

1) (O faktorizaci.) *Je-li $\sim$ netriviální kongruence pro B, je $B/{\sim}$ Booleova algebra.*

2) *Buď $\sim$ netriviální kongruence pro B. Pak $0/{\sim}$ je ideál v B a $1/{\sim}$ filtr v B; jsou vzájemně duální.*

3) a) *Buď I ideál v B. Pak ekvivalence $\sim_I$ na B, definovaná vztahem $a \sim_I b \Leftrightarrow a \dot{-} b \in I$, je netriviální kongruence pro B a $0/{\sim_I} = I$.*

b) *Buď I filtr v B. Pak ekvivalence $\sim^F$ na B, definovaná vztahem $a \sim^F b \Leftrightarrow a \leftrightarrow b \in F$, je netriviální kongruence pro B a $1/{\sim^F} = F$.*

Důkaz. 1) V $B/{\sim}$ platí všechny identické rovnosti z B a z netriviálnosti $\sim$ plyne $0 \not\sim 1$; tudíž v $B/{\sim}$ platí všechny axiomy Booleových algeber. 2), 3) plynou zcela rutinně využitím booleovských pravidel. □

TVRZENÍ 1.2.17. (O kongruencích a homomorfizmech Booleovy algebry.)

1) a) *Homomorfizmus h algebry B do Booleovy algebry určuje netriviální kongruenci $\sim_h$ pro B takto: $a \sim_h b \Leftrightarrow h(a) = h(b)$. Platí:*

$$b/{\sim_h} = h^{-1}[h(b)] \text{ pro } b \in B, \quad h[B] \cong B/{\sim_h}. \tag{1.8}$$

b) *Netriviální kongruence $\sim$ pro B určuje homomorfizmus $h_\sim$ algebry B na $B/{\sim}$ takto:*

$$h_\sim(a) = a/{\sim};$$

pak $\sim_{h_\sim}$ je $\sim$. Homomorfizmus $h_\sim$ se nazývá faktorprojekce *B na $B/{\sim}$.*

Důkaz plyne zcela rutinně využitím booleovských pravidel. □

1.2.18. Faktorizace Booleovy algebry podle ideálu a filtru.

Podle 1.2.16 jsou netriviální kongruence a ideály (a korelativně filtry) v jednoznačné korespondenci via $\sim \mapsto 0/{\sim}$ (korelativně $\sim \mapsto 1/{\sim}$). Je-li I ideál resp. F filtr v Booleově algebře B, značí se proto $B/{\sim_I}$ resp. $B/{\sim^F}$ též symbolem

$$B/I \;\text{ resp. }\; B/F. \tag{1.9}$$

Vidíme nyní, že ještě díky 1.2.17 platí následující

TVRZENÍ 1.2.19. (O epimorfizmu Booleových algeber.) *Je-li h homomorfizmus Booleovy algebry A na Booleovu algebru B, tak platí:*

$$B \cong A/{\sim_h} = A/h^{-1}[0] = A/h^{-1}[1], \quad h^{-1}[1] \text{ je filtr a } h^{-1}[0] \text{ k němu duální ideál v } A.$$

TVRZENÍ 1.2.20. (O ultrafiltrech Booleovy algebry.) *Buď B Booleova algebra.*

1) a) *Ultrafiltry v B jsou právě maximální filtry v B (vzhledem k inkluzi).*

   b) *Každý filtr v B je obsažen v nějakém ultrafiltru v B (jako část).*

2) *Filtr F v B je ultrafiltr v B, právě když platí $B/F \cong \underline{2}$.*

Důkaz. 1) a) Buď F filtr v B. Je-li to ultrafiltr a $F' \supseteq F$ je filtr takový, že existuje $a \in F' - F$, máme $-a \in F'$ a tedy $0 \in F'$ – spor. Nechť F není ultrafiltr. Buď $a \in B$, $a \notin F$, $-a \notin F$. Pak pro $b \in F$ je $a \wedge b \neq 0$, neboť jinak $b \leq -a$ a tedy $-a \in F$. Tudíž $F' = \{c \in B;\ a \wedge b \leq c$ pro nějaké $b \in F\}$ je filtr obsahující a a $F' \supsetneq F$. F tedy není maximální. b) Existence maximálního filtru obsahujícího daný filtr F plyne z principu maximality, aplikovaného na množinu všech filtrů rozšiřujících F, uspořádanou inkluzí; toto uspořádání splňuje předpoklad majorizovatelnosti řetězů. 2) i) Buď F ultrafiltr. Pro $a \in B$ je buď $a \in F$ a pak $a \sim^F 1$, nebo $-a \in F$ a pak $-a \sim^F 1$ a tedy $a \sim^F 0$. ii) Buď $B/F \cong \underline{2}$. Algebra B/F má jen nulu a jedničku, tedy pro $b \in B$ máme buď $b/F = 1$ a pak $b \in F$, nebo $b/F = 0$, pak $-b/F = 1$ a tedy $-b \in F$. □

1.2.21. Fréchetův ideál a filtr.

Buď $\underline{B}$ nekonečná atomární Booleova algebra. *Fréchetův ideál* v $\underline{B}$ je ideál

$$\mathrm{I_f}(\underline{B}) = \{\bigvee u;\ u \text{ je konečná množina atomů v } \underline{B}\}.$$

Fréchetův filtr je k němu duální filtr, značený $\mathrm{F_f}(\underline{B})$. Pokud je $\underline{B}$ potenční algebra $\underline{\mathcal{P}}(X)$, píšeme též $\mathrm{I_f}(X)$ resp. $\mathrm{F_f}(X)$ místo $\mathrm{I_f}(\underline{B})$ resp. $\mathrm{F_f}(\underline{B})$. Pro ultrafiltr F v $\underline{B}$ zřejmě platí:

$$F \text{ není hlavní, právě když } \mathrm{F_f}(\underline{B}) \subseteq F.$$

PŘÍKLADY 1.2.22.

1. Buď I nekonečná množina.
   a) Algebra $\mathrm{FA}(X)$ je atomární, $\{a\}$ s $a \in I$ jsou právě její atomy a $\mathrm{FA}(X) = \mathrm{I_f}(X) \cup \mathrm{F_f}(X)$.
   b) $\mathrm{F_f}(X)$ je jediný nehlavní ultrafiltr v $\mathrm{FA}(X)$. Velikost Stoneova prostoru $\mathrm{S}(\mathrm{FA}(X))$ je $|X|$.
   c) $\mathrm{FA}(X)/\mathrm{F_f}(X) \cong \underline{2}$.

2. Buď I nekonečná množina; označme $\underline{B}$ algebru $\underline{\mathcal{P}}(X)$.
   a) $\underline{B}$ je atomární, $\{a\}$ s $a \in X$ jsou právě její atomy.
   b) O ultrafiltrech.
      i) Buď $w \subseteq I$ nekonečná. Pak

$$F_w = \{u \subseteq X;\ \text{existuje } u' \in \mathrm{F_f}(X) \text{ s } u \supseteq w \cap u'\}$$

je filtr v $\underline{B}$, $w \in F_w \supseteq \mathrm{F_f}(X)$.

ii) Existuje alespoň $|I|$ nehlavních ultrafiltrů v $\underline{B}$. Buď totiž $W \subseteq \mathcal{P}(I)$ množina velikosti $|X|$ po dvou disjunktních množin, z nichž má každá velikost $|X|$; takové W existuje díky nekonečnosti X, neboť pak X je stejně velké, jako $X \times I$. Pak $\{F^*_w;\ w \in W\}$, kde F^*_w je ultrafiltr obsahující F_w z b), je množina nehlavních ultrafiltrů, která má velikost $|I|$ (neboť pro $w \neq w'$ z W je $F^*_w \neq F^*_{w'}$ díky tomu, že $w \cap w' = 0$, $w \in F^*_w$, $w' \in F^*_{w'}$).

iii) Stoneův prostor $\mathrm{S}(\underline{B})$ má velikost $2^{2^{|X|}}$. Důkaz je obtížnější; neuvádíme jej.

c) $\underline{B}/\mathrm{F_f}(\underline{B})$ je bezatomární a má velikost jako $\underline{B}$, tj. $2^{|X|}$. Dokažme to. Označme F filtr $\mathrm{F_f}(\underline{B})$. Buď u/F, nenulový prvek $\underline{B}/F$. Pak u je nekonečná část I a existují nekonečné disjunktní u_0, u_1 s $u_0 \cup u_1 = u$. Pak u_i/F jsou nenulové, disjunktní a jejich spojení je u/F, vše v $\underline{B}/F$; tudíž pod u/F leží menší nenulový prvek a tedy u/F není atom. Konečně faktorů u/F je právě $2^{|I|}$, neboť $|u/F| = |I|$, protože u' z u/F se liší od u o konečnou množinu (tj. $u \mathbin{\dot{-}} u' \in \mathrm{I_f}(I)$) a konečných podmnožin množiny I je $|X|$ (díky nekonečnosti X).

1.3 O lineárních uspořádáních.

TVRZENÍ 1.3.1. (O neizomorfních lineárních uspořádáních.)

1) a) *Existuje právě kontinuum neizomorfních spočetných lineárních uspořádání.*

   b) *Pro nekonečné* κ *je právě* 2^κ *neizomorfních lineárních uspořádání kardinality* κ.

2) *Pro nekonečné* κ *je právě* 2^κ *neizomorfních lineárních diskrétních uspořádání kardinality* κ.

3) *Pro nespočetné* κ *je právě* 2^κ *neizomorfních hustých lineárních uspořádání bez konců, které mají kardinalitu* κ.

1.4 Poznámky.

Kapitola 2

Koncept predikátové logiky

Základní úlohou predikátové logiky je objasnit, co je soud o individuích, co je jeho důkaz z axiomů dané axiomatické teorie a co je jeho pravdivost vzhledem k této teorii. Formálně je soud výraz nějakého jazyka L, chápaný jako jistá konečná posloupnost čili sekvence symbolů jazyka; soudům říkáme formule jazyka L čili L-formule.

Nastíněná logika má dvě stránky, patřící přirozeně k jazyku a souzení vůbec: syntaktickou a sémantickou. Syntaktická se týká zejména skladby či struktury jazyka, formulí a dalších výrazů v něm vytvořených a dále struktury dokazování čili dedukování. Základním materiálem jsou tu symboly, sekvence (symbolů), sekvence sekvencí a jisté operace s nimi. Základními syntaktickými pojmy jsou pak jazyk, term, formule, logické axiomy, pravidla dedukce, teorie, důkaz v teorii. Sémantická stránka se týká významové interpretace a pravdivosti formulí. Základními sémantickými pojmy jsou struktury (prvního řádu) jakožto významové interpretace uvažovaných jazyků, pojem platnosti čili pravdivosti ve struktuře, pojem modelu teorie a pravdivosti v teorii. Můžeme říci, že logika je dána koncepcí čili rozvrhem základní syntaxe a sémantiky.

Požadavkem na dokazování je jeho tzv. korektnost, totiž to, aby dokazatelná formule z nějakých axiomů byla pravdivá v těch významových interpretacích, ve kterých jsou pravdivé axiomy. Heslovitě řečeno: „Dokazatelné je pravdivé“. Zásadním poznatkem predikátové logiky je, že platí i opačná netriviální implikace a tedy nakonec tvrzení o kompletnosti:

„Dokazatelné je právě to, co je pravdivé“.

2.0.1. Klíčové pojmy a značení.

Základní syntax.

Pojem	Značení	Obor
jazyk	L	
term	t, s	Term_L
(atomická) formule	φ, ψ, χ	(AFm_L) Fm_L
logické axiomy		LAx_L

Pojem	Značení	Obor
pravidla dedukce	MP, Gen	
teorie	T	
důkaz v teorii		
φ je dokazatelná v T	$T \vdash \varphi$	$\mathrm{Thm}(T)$

Základní sémantika.

Pojem	Značení	Obor
struktura pro L čili L-struktura	$\mathcal{A} \models L$	$\mathsf{M}(L)$
φ platí v $\mathcal{A}$ (při ohodnocení e proměnných)	$\mathcal{A} \models \varphi$ ($\mathcal{A} \models \varphi[e]$)	$\mathrm{Thm}(\mathcal{A})$
$\mathcal{A}$ je model T	$\mathcal{A} \models T$	$\mathsf{M}(T)$
φ je pravdivá v T	$T \models \varphi$	$\mathrm{Tru}(T)$

2.1 Základní syntax.

Jazyk.

2.1.1. Symboly. Signatura. Velikost jazyka. Extenze, restrikce, izomorfizmus jazyků.

Jazyk je tvořen symboly logickými, mimologickými a eventuálně binárním relačním symbolem rovnosti $=$. Navíc se užívají tři pomocné symboly (delimitery) (,).

Logické symboly jsou:

– Logické spojky $\neg$ *negace* a $\rightarrow$ *implikace*, další jsou zavedené jako zkratky.
– Proměnné, tvořící spočetnou množinu Var; značíme je často x, y, z.
  Buď $v_0, v_1, \ldots$ prosté pevné očíslování všech proměnných.
– Univerzální čili obecné kvantifikace $\forall_x$ s x z Var; $\forall_x$ čteme „pro každé x“. Existenční kvantifikaci $\exists_x$, čteme „existuje x“, zavádíme jako zkratku. (Poznamenejme, že $\forall_x$ je jeden symbol.)

Mimologické symboly jsou *relační*, vyjadřující vztahy o individuích a *funkční*, vyjadřující operace s individui. Četnosti uvažovaných vztahů jsou konečné. Nulární funkční symbol se nazývá *konstantní* symbol. K formálnímu zápisu užijeme pojem *obecné notace*, což je dvojice $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$ značená $\underline{\mathcal{S}}$ a taková, že $\emptyset \notin \mathcal{S}$ a $Ar_{\mathcal{S}} : \mathcal{S} \to \mathbb{N}$; $S \in \mathcal{S}$ je symbol a $Ar_{\mathcal{S}}(S)$ jeho četnost. Je-li $\mathcal{S} = \emptyset$, jde o prázdnou obecnou notaci. Výčet mimologických symbolů je *signatura jazyka* $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$, kde $\underline{\mathcal{R}}$, $\underline{\mathcal{F}}$ jsou obecné notace takové, že $\mathcal{R} \cap \mathcal{F} = \emptyset$ a $\mathcal{R} \cup \mathcal{F}$ neobsahuje žádný logický symbol ani $=$. $\underline{\mathcal{R}}$ resp. $\underline{\mathcal{F}}$ je výčet relačních resp. funkčních symbolů; oba výčty mohou být prázdné; pak jde o prázdnou signaturu, značenou $\emptyset$. Signaturu jazyka značíme často L a jazyk s uvedenou signaturou značíme zpravidla stejným symbolem. Je to dále *jazyk s rovností*, obsahuje-li binární relační symbol $=$ rovnosti; jinak to je *jazyk bez rovnosti*. Jazyk musí vždy obsahovat nějaký relační symbol. Signatura a také jazyk je *čistě relační* resp. *čistě funkční*, též *algebraický*, je-li každý jeho mimologický symbol relační resp. funkční. Jazyk zapisujeme uvedením jeho signatury, často v následujícím přehledném a praktickém tvaru:

$$\langle R_0, \ldots, F_0, \ldots, c_0, \ldots \rangle,\ R_0 \text{ je } m_0\text{-ární relační symbol}, \ldots,$$
$$F_0 \text{ je } n_0\text{-ární funkční symbol}, \ldots, c_0 \text{ je konstantní symbol}, \ldots.$$

Nemusíme pak ani nejprve vypisovat relační a pak funkční symboly, ale můžeme je uvádět v libovolném pořadí, avšak tak, aby byly patrné četnosti a to, o jaký druh symbolu jde.

Např. signatura jazyka s rovností uspořádaných těles je $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$, kde
$\underline{\mathcal{R}}$ je $\langle \{\leq\}, Ar_{\mathcal{R}} \rangle$ s $Ar_{\mathcal{R}}(\leq) = 2$,
$\underline{\mathcal{F}}$ je $\langle \{+, -, \cdot, 0, 1\}, Ar_{\mathcal{F}} \rangle$ s $Ar_{\mathcal{F}}(+) = Ar_{\mathcal{F}}(\cdot) = 2$, $Ar_{\mathcal{F}}(-) = 1$, $Ar_{\mathcal{F}}(0) = Ar_{\mathcal{F}}(1) = 0$.
Zpravidla ji zapisujeme v přehledném tvaru: $L = \{\leq, +, -, \cdot, 0, 1\}$, $\leq$ je binární relační symbol, $+, \cdot$ jsou binární funkční symboly, $-$ je unární funkční symbol, $0, 1$ jsou konstantní symboly.

Velikost čili *kardinalita* $\|L\|$ *jazyka* L je maximum z velikosti množiny mimologických symbolů a spočetné velikosti; velikost $\|L\|$ je tedy vždy alespoň spočetná.

Buďte L, L' dva jazyky. Jazyk L' je *extenze* L a L je *restrikce* L', pokud každý mimologický symbol jazyka L je mimologickým symbolem jazyka L' téhož typu a četnosti v L' jako v L a dále je-li L s rovností, je i L'; píšeme $L \subseteq L'$. Jazyky L a L' jsou *izomorfní*, jsou-li oba buď s rovností nebo oba bez rovnosti a dále existuje prosté zobrazení h množiny mimologických symbolů jazyka L na množinu mimologických symbolů jazyka L' tak, že pro každý mimologický symbol S z L je $h(S)$ téhož typu a četnosti v L' jako S v L.

2.1.2. Termy a formule.

Termy a formule jsou výrazy daného jazyka $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ takové, že prvé vyjadřují symbolicky funkce složené z funkčních symbolů z $\mathcal{F}$ a druhé tvrzení.

Množinu Term_L všech *termů* jazyka L čili L-termů definujeme induktivně pravidly: t1) Každá proměnná je term. t2) Je-li F z $\mathcal{F}$ četnosti n a $t_0, \ldots, t_{n-1}$ jsou termy, je $F(t_0, \ldots, t_{n-1})$ term.

Atomická formule jazyka L je právě výraz tvaru $R(t_0, \ldots, t_{n-1})$, kde R je z $\mathcal{R}$ a n-ární a $t_0, \ldots, t_{n-1}$ jsou termy. Je to tedy právě predikce o termech; obor všech atomických formulí jazyka L značíme AFm_L. Atomická formule nebo její negace se nazývá *literál*.

Množina Fm_L všech *formulí* jazyka L čili L-formulí má induktivní definici s pravidly: f1) Každá atomická formule je formule. f2) Jsou-li φ, ψ formule, jsou jimi i $\neg(\varphi)$, $(\varphi \to \psi)$. f3) Je-li φ formule a x proměnná, je $\forall_x(\varphi)$ formule. Induktivní definice s pravidly f1) a f2) definuje obor OFm_L všech *otevřených* čili *bezkvantifikátorových* formulí jazyka L. Zřejmě je $\mathrm{AFm}_L \subseteq \mathrm{OFm}_L \subseteq \mathrm{Fm}_L$. Řekneme-li dále term resp. formule, míníme tím term resp. formuli nějakého jazyka, patrného z kontextu nebo na jehož bližším určení nezáleží. Ve formuli $(\varphi \to \psi)$ je φ *antecedent* a ψ *konsekvent*.

Indukcí dle složitosti formule definujeme *podformule* takto: a) podformule atomické formule je právě ona sama. b) podformule $\neg\varphi$ či $\forall_x(\varphi)$ resp. $(\varphi \to \psi)$ je právě ona sama nebo každá podformule φ resp. navíc i každá podformule ψ.

Nevnořený term resp. *nevnořená atomická formule* je term resp. atomická formule tvaru

$$F(x_0, \dots, x_{n-1}) \quad \text{resp.} \quad R(x_0, \dots, x_{n-1}),\ F(x_0, \dots, x_{n-1}) = y,\ x = y,\ x = c,$$

kde R, F či c je relační, funkční či konstantní symbol uvažovaného jazyka.

2.1.3. Termy a formule jako sekvence; prefixní a infixní tvar. Designátory.

Termy daného jazyka $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ lze chápat jako konečné posloupnosti čili sekvence vytvořené ze symbolů jazyka induktivně pomocí funkcí F°, kde $F \in \mathcal{F}$ nebo F je proměnná. Přitom funkce $F^\circ : (\mathcal{F}^*)^n \to \mathcal{F}^*$ s $n = Ar_{\mathcal{F}}(F)$ (a $n = 0$, je-li F proměnná) je taková, že pro $s = \langle s_0, \dots, s_{n-1} \rangle \in (\mathcal{F}^*)^n$ je $F^\circ(s) = \langle F \rangle \smile \sqcup(s)$; sekvence $\langle F \rangle \smile \sqcup(s)$ je tzv. *prefixní* zápis výrazu v *polské notaci.* My jsme ji zapsali v definici termů jako $F(s_0, \dots, s_{n-1})$, tj. v „obvyklé notaci“, k čemuž jsme užili oproti polské notaci tři pomocné delimitery), (. Dále pro F nulární jsme psali $F()$ místo sekvence $\langle F \rangle$, pro proměnnou x jakožto nulární symbol pak jen x místo $\langle x \rangle$. Zcela podobně je tomu s definicí formulí. Tam roli funkčních symbolů hrají $\neg$ jako unární, $\to$ jako binární a každé $\forall_x$ jako unární, atomické formule pak jako nulární. Přitom $\langle \to \rangle \smile \sqcup(\langle \varphi, \psi \rangle)$ jsme zapsali jako $(\varphi \to \psi)$, tj. v *infixním* tvaru; „obvyklý“ prefixní tvar je $\to(\varphi, \psi)$. Infixní tvar užíváme z důvodů lepší čitelnosti.

Vidíme abstraktněji, že nám jde o sekvence v polské notaci induktivně vytvořené vzhledem k nějaké obecné notaci $\underline{\mathcal{S}} = \langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$, obsahující aspoň jeden nulární symbol; říkáme pak že $\underline{\mathcal{S}}$ je *notace.* Zmíněná sekvence se nazývá *designátor* notace $\underline{\mathcal{S}}$ a množina $\mathrm{D}(\mathcal{S})$ designátorů notace $\underline{\mathcal{S}}$ je tedy definovaná induktivní definicí:

$$\text{Pro } S \in \mathcal{S} \text{ a sekvenci } s \text{ designátorů délky } Ar_{\mathcal{S}}(S) \text{ je } \langle S \rangle \smile \sqcup(s) \text{ designátor.}$$

Je-li $S \in \mathcal{S}$ a $s = \langle s_0, \dots, s_{n-1} \rangle$ sekvence, užíváme pro grafický zápis sekvence $\langle S \rangle \smile \sqcup(s)$ „obvyklou“ prefixní nebo infixní notaci, tj.

$$\langle S \rangle \smile \sqcup(\langle s_0, \dots, s_{n-1} \rangle) \text{ značíme } S(s_0, \dots, s_{n-1}), \text{ také (infixně) } (s_0 S s_1), \text{ když } n = 2.$$

Poznamenejme, že pro $n = 0$ často píšeme místo $S()$ jen S. Je patrné, že termy jazyka $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ jsou designátory notace $\underline{\mathcal{F}}'$, která je rozšířením $\underline{\mathcal{F}}$ o nulární symboly x, kde x je proměnná. Množina OFm_L resp. Fm_L je množina designátorů notace

$$\mathrm{AFm}_L \cup \{\neg, \to\} \quad \text{resp.} \quad \mathrm{AFm}_L \cup \{\neg, \to\} \cup \{\forall_x;\ x \in \mathrm{Var}\},$$

kde každé φ z AFm_L je nulární, $\neg$ unární, $\to$ binární a každé $\forall_x$ je unární. Přitom $\langle \varphi \rangle$ pro $\varphi \in \mathrm{AFm}_L$ zapisujeme jako φ (místo $\varphi()$) a atomická formule tak je formule.

Připomeňme, že sekvence x je *podsekvence* sekvence y, existují-li sekvence y_0, y_1 tak, že platí $y_0 \smile x \smile y_1 = y$; říkáme pak také, že x má *výskyt v* y. *Poddesignátor* nějakého designátoru η je designátor mající výskyt v η. Poddesignátor formule φ je podformule φ. *Výskyt termu* ve formuli φ je jeho výskyt v nějaké atomické podformuli φ. Povšimněme si, že výskyt symbolu $\forall_x$ ve formuli neznamená, že proměnná x má v této formuli výskyt.

Platí dále následující tři důležitá a intuitivně dobře akceptovatelná tvrzení o designátorech (viz 2.5.2, 2.5.4, 2.5.6), umožňující mimo jiné korektně pracovat s výskytem a substitucí.

TVRZENÍ 2.1.4. (O designátorech.)

1) (O jednoznačnosti.) *Každý designátor je jednoznačně tvaru* $\langle S \rangle \smile \sqcup(s)$ *pro jisté* $S \in \mathcal{S}$ *a jisté* $s \in \mathrm{D}(\mathcal{S})^{Ar(S)}$.
2) (O výskytech.) *Každý výskyt designátoru* η' *v designátoru* η *tvaru* $\langle S \rangle \smile \sqcup(s)$ *s* $S \in \mathcal{S}$ *a* $s \in \mathrm{D}(\mathcal{S})^{Ar_{\mathcal{S}}(S)}$ *je buď* η *nebo je to výskyt v některém členu* $(s)_i$.

3) (O substituci.) *Nahradí-li se výskyt designátoru η' v designátoru η designátorem η'', získá se designátor.*

2.1.5. Indukce dle délky.

Každý designátor má jednoznačný tvar a délku. To dovoluje *dokazovat indukcí dle délky* designátorů, že všechny mají nějakou vlastnost a *definovat indukcí dle délky* designátorů nějakou vlastnost designátorů či hodnotu designátorům přiřazenou (tj. konstruovat ji rekurzivně).

2.1.6. Zavedení &, $\vee$, $\exists$. Konvence o zápisu formulí.

Binární logické spojky $\vee$ *disjunkce* (čili *nebo*), & *konjunkce* (čili *a*) a $\leftrightarrow$ *ekvivalence* zavádíme jako zkratky dané následovně:

$$(\varphi \vee \psi) \;\text{ za }\; (\neg(\varphi) \to \psi), \quad (\varphi \,\&\, \psi) \;\text{ za }\; \neg(\varphi \to \neg(\psi)),$$
$$(\varphi \leftrightarrow \psi) \;\text{ za }\; ((\varphi \to \psi) \,\&\, (\psi \to \varphi)).$$

Místo & se může psát také $\wedge$. Existenční kvantifikace $\exists_x(\varphi)$ je zavedena jako zkratka za $\neg(\forall_x(\neg(\varphi)))$; $\exists$ je *existenční kvantifikátor.*

Následující *konvence o zápisu formulí* se užívají pro lepší čitelnost.

• Často se vynechávají vnější závorky, místo $\neg(\varphi)$ se píše $\neg\varphi$. Používá se též konvence, že $\neg$ má v zápise vyšší prioritu než spojky & a $\vee$, ty zase než $\leftrightarrow$ a ta zase než $\to$. Místo $((\varphi \,\&\, (\neg\psi)) \to (\chi \vee \psi))$ tak máme $\varphi \,\&\, \neg\psi \to \chi \vee \psi$; můžeme ovšem použít i méně radikální zkrácení, jako např. $(\varphi \,\&\, \neg\psi) \to (\chi \vee \psi)$. Místo $(\varphi_1 \diamond (\varphi_2 \diamond \cdots \diamond \varphi_n) \dots)$ píšeme též $\varphi_1 \diamond \varphi_2 \diamond \cdots \diamond \varphi_n$, kde $\diamond$ je $\to$, & nebo $\vee$; nekumulujeme zde tedy závorky zprava. Formule $\varphi_1 \diamond \varphi_2 \diamond \cdots \diamond \varphi_n$, kde $\diamond$ je & resp. $\vee$ se nazývá *konjunkce s konjunkty* $\varphi_1, \dots, \varphi_n$ resp. *disjunkce s disjunkty* $\varphi_1, \dots, \varphi_n$. Závorky můžeme pro zlepšení čitelnosti i přidat.

• Formuli $\forall_x(\varphi)$ resp. $\exists_x(\varphi)$ zapisujeme jako $(\forall x)\varphi$ resp. $(\exists x)\varphi$. Tedy $(\exists x)\varphi$ je zkratka za $\neg(\forall x)\neg\varphi$. Je-li Q kvantifikátor, píšeme též $(Qx_1, \dots, x_n)\varphi$ za $(Qx_1) \cdots (Qx_n)\varphi$.

• Je-li R resp. F nějaký nulární relační resp. funkční symbol, píšeme zpravidla místo atomické formule $R()$ resp. termu $F()$ jen R resp. F. Je-li $\diamond$ binární relační symbol, píše se též $t \not\diamond s$ za $\neg(t \diamond s)$.

2.1.7. Volné a vázané proměnné. Uzavřená formule. Generální uzávěr.

1. *Výskyt proměnné x* ve formuli φ je *vázaný* ve φ, je-li to výskyt v nějaké podformuli $(\forall x)\psi$ formule φ; v opačném případě je tento výskyt *volný* ve φ. Říkáme, že *proměnná x je volná* resp. *vázaná* ve φ, jestliže některý její výskyt je volný resp. vázaný ve φ. Proměnná x je *[ne]kvantifikovaná ve formuli* φ, když [není]je ve φ výskyt $(\forall x)$. Proměnná *patří* formuli φ, má-li výskyt ve φ či je kvantifikovaná ve φ; jinak *nepatří* φ.

Proměnná může být zároveň volná i vázaná v nějaké formuli. Jsou-li proměnné x, y různé, tak volné výskyty x v $\neg\varphi$, $(\forall y)\varphi$ resp. $\varphi \to \psi$, jsou právě volné výskyty ve φ resp. φ a ψ; to plyne z tvrzení o jednoznačnosti designátorů. Dále x nemá volný výskyt v $(\forall x)\varphi$. (Upozorněme, že v $(\forall x)\varphi$ není x těsně za $\forall$ výskyt proměnné x.)

2. Formule se nazývá *uzavřená*, čili *sentence*, není-li v ní volná žádná proměnná. *(Generální) uzávěr* φ je formule $(\forall x_1, \dots, x_n)\varphi$, kde mezi $x_1, \dots, x_n$ jsou všechny volné proměnné formule φ.

2.1.8. Formule a term v daných proměnných. Symboly $t(\overline{x})$, $\varphi(\overline{x})$.

Term t resp. formule φ *je (právě) v proměnných* $\overline{x}$, je-li $\overline{x} = \langle x_0, \dots, x_{n-1}\rangle$ prostá (n-)tice různých proměnných, mezi kterými jsou (právě) všechny proměnné termu t resp. volné proměnné formule φ. Píšeme pak

$$t(\overline{x}) \text{ či } t(x_0, \dots, x_{n-1}) \qquad \text{resp.} \qquad \varphi(\overline{x}) \text{ či } \varphi(x_0, \dots, x_{n-1})$$

a tento nápis právě znamená, že t resp. φ je v $\overline{x}$. Term či formule je *v n proměnných* s $n \in \mathbb{N}$, je-li v $\langle v_0, \dots, v_{n-1}\rangle$ a Fm^n_L je množina všech L-formulí v n proměnných. Řekneme-li, že φ je (právě) v proměnných $\overline{x}, \overline{y}$, znamená to, že φ je (právě) v $\overline{x} \smile \overline{y}$ a $\overline{x}$, $\overline{y}$ jsou disjunktní. Užíváme pak, obdobně jako výše, symbol $\varphi(\overline{x}, \overline{y})$, eventuálně $\varphi(\overline{x}; \overline{y})$. Často se potom $\overline{x}$ resp. $\overline{y}$ interpretují jako tzv. *předmětné* resp. *parametrické* proměnné uvažované formule. Podobně je tomu s termy. Můžeme analogicky užít i „trojný“ seznam $\overline{x}, \overline{y}, \overline{z}$ a psát $\varphi(\overline{x}, \overline{y}, \overline{z})$ atd.

PŘÍKLAD. a) Buď $+$ binární funkční symbol. $+$ není term. v_1+v_1 je nevnořený term právě ve $\langle v_1\rangle$. $v_1+v_1(v_0,v_1,v_2)$ znamená, že term v_1+v_1 je v proměnných $\langle v_0,v_1,v_2\rangle$. b) Buď F binární funkční symbol. $F(v_5,v_1)$ je nevnořený term právě ve $\langle v_5,v_1\rangle$. $F(v_5,v_1)(\langle v_0,v_1,v_5\rangle)$ znamená, že term $\langle v_5,v_1\rangle$ je v proměnných $\langle v_0,v_1,v_5\rangle$. $F(v_5,v_1)(v_0;v_5)$ znamená, že term $F(v_5,v_1)$ je v proměnných $\langle v_0,v_5\rangle$ a v_0 resp. v_5 považujeme za předmětnou resp. parametrickou proměnnou.

2.1.9. **Substituce, instance, varianta.**

1. Term t je *substituovatelný* za x do φ, jestliže pro každou proměnnou y termu t žádná podformule $(\forall y)\psi$ formule φ neobsahuje výskyt x, který je volný ve φ.

Substituce termu t do formule φ za proměnnou x se provádí tak, že všechny volné výskyty proměnné x ve φ se nahradí termem t, pokud(!) je term t substituovatelný za x do φ. Snadno se indukcí dle složitosti φ dokáže, že získaný výraz je formule; zapisujeme ji jako $\varphi(x/t)$ a pokud je tento symbol užit, znamená to, že t je substituovatelné za x do φ. Je-li φ bezkvantifikátorová formule, je zřejmě každý term substituovatelný za každou proměnnou do φ.

2. *Instance* formule φ je formule značená $\varphi(x_1/t_1,\dots,x_n/t_n)$ a získána z φ nahražením všech volných výskytů $x_1,\dots,x_n$ za $t_1,\dots,t_n$, přičemž $x_1,\dots,x_n$ jsou různé proměnné, term t_i je substituovatelný za x_i do φ pro $i=1,\dots,n$ a substituce se provádí simultánně. Obecně není instancí formule φ formule $\varphi(x_1/t_1)(x_2/t_2)\cdots(x_n/t_n)$ získána postupně prováděnou substitucí.

Obdobně $t(x_1/t_1,\dots,x_n/t_n)$ značí term získaný z termu t simultánním nahražením všech výskytů $x_1,\dots,x_n$ za $t_1,\dots,t_n$, přičemž $x_1,\dots,x_n$ jsou různé proměnné. Výsledkem je term, jak plyne z tvrzení o substituci v designátorech. Místo $\varphi(x_1/t_1,\dots,x_n/t_n)$ resp. $t(x_1/t_1,\dots,x_n/t_n)$ píšeme též, nevede-li to k nedorozumění, jen $\varphi(t_1,\dots,t_n)$ resp. $t(t_1,\dots,t_n)$.

Poznamenejme, že $\varphi(x_1/t_1,\dots,x_n/t_n)$ můžeme získat postupně prováděnou substitucí t_i za x_i' do $\varphi(x_1/x_1',\dots,x_n/x_n')$, kde $x_1',\dots,x_n'$ jsou různé, nejsou kvantifikované ve φ a nevyskytují se ani ve φ ani v žádném t_i (a tedy x_i' je substituovatelné za x_i do φ). Obdobně je tomu s termy.

3. *Varianta* formule φ je formule, která se získá z φ konečnou aplikací kroků: podformuli $(\forall x)\psi$ nahraď $(\forall y)\psi(x/y)$, kde proměnná y není volná ve ψ (a je substituovatelná za x do ψ).

POZNÁMKA 2.1.10. 1. Substituovatelnost vyjadřuje korektnost substituce, tj. že pro L-formuli $\varphi(x)$ a L-strukturu $\mathcal{A}$ je $\mathcal{A}\models\varphi(x)\Rightarrow\mathcal{A}\models\varphi(x/t)$. Buď $\varphi(x)$ formule $(\exists y)(x\neq y)$. Pak platí v $\mathcal{A}$, je-li A alespoň dvouprvková, avšak formule $(\exists y)(y\neq y)$, získaná z φ nekorektní substitucí termu y za x, neplatí v $\mathcal{A}$. Později ukážeme, že dokazatelnost formule implikuje dokazatelnost její instance.

2. Nechť y není volná ve φ a je substituovatelná za x do φ, φ' je $\varphi(x/y)$. Pak $\varphi'(y/x)$ je φ. Oba předpoklady dohromady totiž zaručují, že volný výskyt y ve φ' je právě tam, kde je volný výskyt x v φ. Tedy x je substituovatelné za y do φ' a také totožnost obou uvažovaných formulí platí.

3. a) Buď φ formule $(\exists x)(x<y)\vee(x=y)$ s různými proměnnými x,y. Je-li proměnná z různá od x,y, je $(\exists z)(z<y)\vee(x=y)$ varianta φ. Nelze však „variovat x na y“, neboť y má volný výskyt v $(\exists x)(x<y)$.

b) Chceme, aby varianta φ' formule byla ekvivalentní s φ; že tomu tak je, dokážeme později jako tvrzení o variantách. Pokud bychom nedodrželi pravidla vytváření varianty, neplatilo by to. Vezmeme-li totiž za φ formuli $(\exists x)(x\neq y)$ s různými x,y a budeme chybně (neboť y má volný výskyt v $x\neq y$) „variovat“ x na y, získáme φ' tvaru $(\exists y)(y\neq y)$, což zjevně není ekvivalentní s φ. Nelze pominout ani podmínku substituovatelnosti. Buď totiž φ formule $(\exists y)(\exists x)(x\neq y)$; budeme-li chybně (díky tomu, že x není substituovatelné za y do $(\exists x)(x\neq y)$) „variovat“ y na x, získáme φ' tvaru $(\exists x)(\exists x)(x\neq x)$, což zjevně není ekvivalentní s φ.

Pomocí tvrzení o variantách lze až na ekvivalenci docílit, aby v dané formuli nebyla žádná proměnná zároveň vázaná i volná. Například ve formuli φ, která má tvar $(\forall x)(x<y)\ \&\ x+0=x$ s různými x,y, je x volná i vázaná. Buď x' proměnná různá od x,y. Pak je $(\forall x')(x'<y)\ \&\ x+0=x$ varianta φ, ve které není žádná proměnná zároveň vázaná i volná.

Dedukce.

2.1.11. **Logické axiomy a pravidla dedukce.**

Logické axiomy jazyka L jsou jisté pravdivé L-formule; můžeme je použít vždy při dokazování jako axiom, aniž bychom porušili korektnost dokazování. Máme dvě skupiny logických axiomů: *o logických spojkách* a *o kvantifikátorech*. Jde-li o jazyk s rovností, patří mezi logické axiomy *axiomy rovnosti*. Množinu logických axiomů jazyka L značíme LAx_L.

- Axiomy o logických spojkách jsou následující tři schemata formulí:
  (PL1) $\varphi \to (\psi \to \varphi)$,
  (PL2) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$,
  (PL3) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$.
- Axiomy o kvantifikátorech jsou následující dvě schemata:
  Axiomy substituce: L-formule $(\forall x)\varphi \to \varphi(x/t)$, je-li term t substituovatelný za proměnnou x do formule φ.
  Axiomy $\forall$-zavedení: L-formule $(\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$, není-li proměnná x volná ve φ.
- Axiomy rovnosti: $x = x$,
  $x_1 = y_1 \to \ldots \to x_n = y_n \to R(x_1, \ldots, x_n) \to R(y_1, \ldots, y_n)$,
  pokud R je n-ární relační symbol jazyka L včetně $=$, $n > 0$.
  $x_1 = y_1 \to \ldots \to x_n = y_n \to F(x_1, \ldots, x_n) = F(y_1, \ldots, y_n)$,
  pokud F je n-ární funkční symbol jazyka L, $n > 0$.

Pravidla dedukce (čili odvozování) jsou:

Modus ponens (MP): Z φ a $(\varphi \to \psi)$ odvoď ψ. Symbolicky: $\frac{\varphi, (\varphi\to\psi)}{\psi}$.

Pravidlo generalizace (Gen): Z φ odvoď $\forall_x(\varphi)$. Symbolicky: $\frac{\varphi}{\forall_x(\varphi)}$.

2.1.12. **Teorie. Důkaz.** $\mathrm{Thm}(T)$**,** $\mathrm{Th}(T)$**.**

1. *Axiomatika* v jazyce L je libovolná množina $T \subseteq \mathrm{Fm}_L$. Říkáme pak, že dvojice $\langle L, T\rangle$ je *teorie* a také, že T je L-teorie či teorie v L, stručněji teorie, nehrozí-li nedorozumění. Říkáme také, že formule z $T - \mathrm{LAx}_L$ jsou *mimologické axiomy* teorie $\langle L, T\rangle$. *Prázdná* L-teorie je L-teorie $\langle L, \emptyset\rangle$; můžeme ji značit stručně $\emptyset$. *Formule teorie* je formule jazyka této teorie, jazyk teorie T se značí $L(T)$. *Část*, též *fragment*, teorie T je $L(T)$-teorie T' s $T' \subseteq T$. Jsou-li $\varphi_0, \ldots, \varphi_n$ formule, značíme $T \cup \{\varphi_0, \ldots, \varphi_n\}$ též $T, \varphi_0, \ldots, \varphi_n$. Teorie je *konečně axiomatizovaná* resp. *otevřená*, má-li jen konečně mimologických axiomů resp. je-li každý její mimologický axiom otevřená formule. Nevede-li to k nedorozumění, uvádíme často teorii jen výčtem jejich mimologických axiomů. Píšeme pak $T = \{\varphi_0, \varphi_1, \ldots\}$, což značí, že T je teorie s axiomatikou $\{\varphi_0, \varphi_1, \ldots\} \cup \mathrm{LAx}_L$, kde L je jazyk teorie T (daný předem či patrný z kontextu).

Důkaz v L-teorii T je konečná sekvence $\varphi_0, \ldots, \varphi_n$ nějakých L-formulí, kde φ_i je buď axiom z T nebo logický axiom, nebo je φ_i vyvozeno pomocí nějakého pravidla dedukce z některých φ_j s $j < i$. Uvedený důkaz je *důkaz formule* φ v T, je-li φ některé φ_i. Existuje-li pro L-formuli φ důkaz v T, je φ *dokazatelná v* T čili *teorémem* T; píšeme pak

$$T \vdash \varphi.$$

Je-li T prázdná L-teorie, píšeme $\vdash$ místo $T \vdash$ a „v T“ vynecháváme nebo říkáme *v* L či *v logice*.

Dále

$$\mathrm{Thm}(T) \text{ či } \mathrm{Thm}_T \quad \text{resp.} \quad \mathrm{Th}(T) \text{ či } \mathrm{Th}_T$$

značí množinu všech teorémů T resp. teorémů T, které jsou navíc sentencemi.

2. Pro L-teorii T a L-formule φ, ψ definujeme:

φ *je vyvratitelná* (*spor*) *v* T,	když $T \vdash \neg\varphi$,
φ *je konzistentní s* T,	když $T \nvdash \neg\varphi$,
φ *je nezávislá v* T,	když $T \nvdash \varphi$ a $T \nvdash \neg\varphi$,
φ *je silnější než* ψ *v* T,	když $T \vdash \varphi \to \psi$.

Je-li T prázdná, vynecháváme „v T“.

2.1.13. Spornost, kompletnost, extenze, ekvivalence, axiomatizovatelnost teorií.

1. Teorie je *sporná*, lze-li v ní dokázat každou její formuli; jinak je *bezesporná*.

2. Teorie je *kompletní*, je-li bezesporná a každá její sentence je v ní dokazatelná či vyvratitelná.

3. *Extenze* teorie T je teorie T' taková, že $L(T) \subseteq L(T')$ a $\mathrm{Thm}(T) \subseteq \mathrm{Thm}(T')$; je to *jednoduchá* extenze, je-li navíc $L(T) = L(T')$. Dvě teorie jsou *ekvivalentní*, je-li každá z nich extenzí druhé. *Konzervativní extenze* teorie T je její extenze T' taková, že pro každou $L(T)$-formuli φ platí

$$T' \vdash \varphi \ \Rightarrow \ T \vdash \varphi.$$

4. *Konečně* resp. *otevřeně axiomatizovatelná teorie* je taková, která je ekvivalentní s konečně axiomatizovanou resp. otevřenou teorií.

TVRZENÍ 2.1.14.

1) *Množina* $\mathrm{Thm}(T)$ *je definovaná induktivně pravidly:*
   a) *Každý logický i mimologický axiom* T *je v* $\mathrm{Thm}(T)$.
   b) *Jsou-li* φ, $\varphi \to \psi$ *v* $\mathrm{Thm}(T)$, *jsou tam i* ψ, $(\forall x)\varphi$ *pro každé* x.

2) a) $\mathrm{Thm}(T) = \mathrm{Thm}(\mathrm{Thm}(T))$. b) T *je bezesporná* $\Leftrightarrow$ $\mathrm{Thm}(T)$ *je bezesporná.*

Důkaz. 1) plyne buď z obecné věty o induktivní definici a odvození, nebo indukcí podle délky důkazu v T pro jednu inkluzi a indukcí podle složitosti právě definovaných objektů pro druhou inkluzi. 2) a) plyne z 1), b) z a). □

2.1.15. Teorie čisté rovnosti.

Teorie čisté rovnosti je teorie v jazyce s rovností bez mimologických symbolů, která nemá mimologické axiomy. Tato teorie resp. její jednoduchá extenze o jeden axiom „existuje právě n prvků“ s $0 < n \in \mathbb{N}$ pak $\mathrm{PE_n}$ resp. její jednoduchá extenze o schema „existuje nekonečně prvků“ se značí

$$\mathrm{PE} \quad \text{resp.} \quad \mathrm{PE(n)} \quad \text{resp.} \quad \mathrm{PE}(\infty).$$

2.2 Základní sémantika.

Struktura pro signaturu.

2.2.1. Struktura pro signaturu. Podstruktura a generovaná podstruktura. Redukt.

1. • *Struktura* pro signaturu $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ je $\langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$, kde:

A je neprázdná množina, zvaná *univerzum* $\mathcal{A}$,
$\mathcal{R}^A$ je soubor $\langle R^A;\ R \in \mathcal{R} \rangle$, relací tvaru $R^A \subseteq A^{Ar_{\mathcal{R}}(R)}$ s $R \in \mathcal{R}$,
$\mathcal{F}^A$ je soubor $\langle F^A;\ F \in \mathcal{F} \rangle$ funkcí $F^A : A^{Ar_{\mathcal{F}}(F)} \to A$ s $F \in \mathcal{F}$.

Říkáme pak, že to je L-*struktura* čili *struktura pro* L a také *model jazyka* L. Uvedenou strukturu značíme stručně $\mathcal{A}$ a můžeme psát $\mathcal{A} \models L$. R^A resp. F^A je *realizace* symbolu R resp. F.

• *Velikost* čili *kardinalita* struktury $\mathcal{A}$ je velikost (kardinalita) jejího univerza; značí se $\|\mathcal{A}\|$. Třída všech L-struktur se značí $\mathsf{M}(L)$.

• *Triviální* L-*struktura velikosti* $\kappa \neq 0$ je L-struktura $\mathcal{A}$ s univerzem κ, přičemž pro každý relační mimologický symbol R jazyka L četnosti m je $R^\kappa = \kappa^m$, pro každý funkční mimologický symbol F jazyka L četnosti n je $F^\kappa = \kappa^n \times \{0\}$. Speciálně je každý konstantní symbol interpretován jako 0. Takovou strukturu značíme κ_L; speciálně je 1_L jednoprvková triviální L-struktura.

2. Buď $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ struktura pro $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$. *Podstruktura* struktury je struktura $\mathcal{B} = \langle B, \mathcal{R}^B, \mathcal{F}^B \rangle$ pro $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ taková, že $B \subseteq A$ a dále

$$R^B = R^A \cap B^m \text{ pro } R \in \mathcal{R},\ m = Ar_{\mathcal{R}}(R),\ F^B = F^A \cap (B^n \times B) \text{ pro } F \in \mathcal{F},\ n = Ar_{\mathcal{F}}(F);$$

píšeme pak

$$\mathcal{B} \subseteq \mathcal{A}$$

a podstrukturu $\mathcal{B}$ můžeme zapsat jako $\langle B, \mathcal{R}^A, \mathcal{F}^A \rangle$.

Je-li $\mathcal{B} \subseteq \mathcal{A}$, je B uzavřeno na všechny funkce struktury $\mathcal{A}$ a tedy také každá konstanta struktury $\mathcal{A}$ patří do B. Zřejmě je neprázdná podmnožina $Y \subseteq A$ univerzem nějaké podstruktury

struktury $\mathcal{A}$, právě když je Y uzavřeno na všechny funkce struktury $\mathcal{A}$ (a tedy speciálně každá konstanta struktury $\mathcal{A}$ je v Y); takovou podstrukturu pak značíme

$$\mathcal{A}\restriction Y.$$

Pokud je tedy $\mathcal{B} \subseteq \mathcal{A}$, tak $\mathcal{B} = \mathcal{A}\restriction B$.

3. Pro $X \subseteq A$ je *množina generovaná v $\mathcal{A}$ z X* nejmenší podmnožina A obsahující X a uzavřená na každou funkci z $\mathcal{F}^A$; je to tedy $\mathcal{F}^A$-uzávěr X, který značíme $\mathcal{F}^A\langle X\rangle$ – viz 1.1.1. Je-li $\mathcal{F}^A\langle X\rangle \neq \emptyset$, je to univerzum nejmenší podstruktury struktury $\mathcal{A}$ obsahující X; značíme ji $\mathcal{A}\langle X\rangle$ a říkáme, že to je *podstruktura generovaná* X a prvky z X jsou *generátory* $\mathcal{A}\langle X\rangle$. Je tedy $\mathcal{A}\langle X\rangle = \mathcal{A}\restriction \mathcal{F}^A\langle X\rangle$. Zřejmě když $\mathcal{F}^A$ obsahuje konstantu c^A, je $c^A \in \mathcal{F}^A\langle X\rangle$. Když $\mathcal{F} = \emptyset$, tak $\mathcal{F}^A\langle X\rangle = X$. Pro $\overline{a} \in A^n$ s nějakým $n \in \mathbb{N}$ značí $\mathcal{A}\langle\overline{a}\rangle$ strukturu $\mathcal{A}\langle X\rangle$, kde $X = \{\overline{a}_i : i < n\}$.

4. Buďte L, L' jazyky s $L \subseteq L'$, $\mathcal{A}'$ nějaká L'-struktura. *Redukce* či *redukt $\mathcal{A}'$ na L* je L-struktura $\mathcal{A}$, která vznikne z $\mathcal{A}'$ odebráním realizací symbolů, které nejsou v L; značíme ji $\mathcal{A}' \,|\, L$. Říkáme též, že $\mathcal{A}'$ je *expanze $\mathcal{A}$ do L'*.

Příkladem L-struktury s $L = \langle \leq, +, -, \cdot, 0, 1\rangle$ je $\mathcal{A} = \langle \mathbb{R}, \leq^{\mathbb{R}}, +^{\mathbb{R}}, -^{\mathbb{R}}, \cdot^{\mathbb{R}}, 0^{\mathbb{R}}, 1^{\mathbb{R}}\rangle$, kde $\mathbb{R}$ je množina reálných čísel a uvedené uspořádání a operace ($-$ je unární a značí opačnost) a konstanty mají obvyklý význam. Struktura je zapsaná v přehledném tvaru podobně jako L výše. Nazývá se uspořádané těleso reálných čísel. Často, pokud to nevede k nedorozumění, horní index u relací a operací nějaké struktury vynecháváme pro lepší přehlednost zápisu; místo $\langle A, R^A, \ldots, F^A, \ldots\rangle$ tak píšeme jen $\langle A, R, \ldots, F, \ldots\rangle$. Nevede-li to k nedorozumění, zapisujeme $\langle A, R, \ldots, F, \ldots\rangle\restriction B$ pro stručnost též jako $\langle B, R, \ldots, F, \ldots\rangle$. Expanzi struktury $\mathcal{A}$ o relace $R_0, \ldots$ a funkce $F_0, \ldots$ značíme též $\langle \mathcal{A}, R_0, \ldots, F_0, \ldots\rangle$.

Struktura $\langle \mathbb{N}, \leq, +, -, \cdot, 0, 1\rangle$, kde $-$ je unární operace přičítání jedničky (značená obvykle S) a $\leq$ a ostatní operace a konstanty mají obvyklý význam, se nazývá standardní model přirozených čísel. Redukt $\mathcal{A} \,|\, L^g = \langle \mathbb{R}, +, -, 0\rangle$, kde $L^g = \langle +, -, 0\rangle$ je jazyk teorie grup (v aditivní verzi), je tzv. aditivní grupa reálných čísel. Každá Booleova algebra $\langle A, -, \vee, \wedge, 0, 1\rangle$ je struktura pro jazyk $\langle -, \vee, \wedge, 0, 1\rangle$ teorie Booleových algeber.

TVRZENÍ 2.2.2. (Odhad počtu L-struktur s daným univerzem.) *L-struktur s univerzem $\kappa \geq \omega$ resp. $2 \leq \kappa < \omega$ je nejvýše $2^{\kappa\cdot\|L\|}$ resp. $2^{\|L\|}$.*

Důkaz. Buď $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$. Množina *Rel* resp. *Op* všech relací resp. operací konečných četností nad κ má kardinalitu nejvýše 2^κ pro $\kappa \geq \omega$ a ω jinak. Označme $\lambda = \|L\|$. Je-li $\mathcal{A} = \langle \kappa, \mathcal{R}^A, \mathcal{F}^A\rangle$, je $\mathcal{R}^A : \mathcal{R} \to \mathit{Rel}$, $\mathcal{F}^A : \mathcal{F} \to \mathit{Op}$. Tudíž uvažovaných dvojic $\langle \mathcal{R}^A, \mathcal{F}^A\rangle$ je nejvýše tolik, kolik je kardinalita množiny $(2^\kappa)^\lambda \times (2^\kappa)^\lambda$ resp. $\omega^\lambda \times \omega^\lambda$, což je $2^{\kappa\cdot\lambda}$ resp. 2^λ, neboť $\lambda \geq \omega$. $\square$

Hodnota termu a platnost formule ve struktuře.

2.2.3. **Hodnota termu, hodnocení a platnost formule ve struktuře. Vztah $\models$. $\top$, $\bot$.** Buď $\mathcal{A}$ nějaká L-struktura. Funkce $e : \mathrm{Var} \to A$, čili $e \in {}^{\mathrm{Var}}A$, je *ohodnocení proměnných v A*. Pro ně označme $e(x/a)$ funkci, která vznikne z e právě tak, že e změníme jen v x, a to na hodnotu a.

1. *Hodnota $t^A[e]$* (též $t^{\mathcal{A}}(e)$) *termu t v $\mathcal{A}$ při ohodnocení e* se definuje indukcí dle délky t:
   a) Je-li t proměnná x, je $t^A[e] = e(x)$.
   b) Je-li t tvaru $F(t_0, \ldots, t_{n-1})$ a F je n-ární funkční symbol, tak
$$t^A[e] = F^A(t_0^A[e], \ldots, t_{n-1}^A[e]).$$

2. *Hodnota $\mathrm{H}_{at}^{\mathcal{A}}(\varphi, e)$ atomické formule φ v $\mathcal{A}$ při ohodnocení e* je definována takto:
Když φ je tvaru $R(t_0, \ldots, t_{n-1})$, kde R je n-ární relační symbol z L (tj. i $=$, je-li L s rovností) a $t_0, \ldots, t_{n-1}$ jsou termy, tak definovaná hodnota je 1 resp. 0, právě když $R^A(t_0^A[e], \ldots, t_{n-1}^A[e])$ platí resp. neplatí; přitom $=^A$ je identita na A. Pro R nulární speciálně máme $\mathrm{H}_{at}^{\mathcal{A}}(R()) = 1 \Leftrightarrow R^A(\emptyset) \Leftrightarrow R^A = \{\emptyset\}$.

3. • Zobrazení $\mathrm{H}^{\mathcal{A}} : \mathrm{Fm}_L \times {}^{\mathrm{Var}}A \to 2$, nazývané *hodnocení ve struktuře $\mathcal{A}$*, definujeme indukcí dle délky φ takto:

$$\begin{array}{rcll}
\mathrm{H}^{\mathcal{A}}(\varphi,e) & = & \mathrm{H}^{\mathcal{A}}_{at}(\varphi,e), & \text{když } \varphi \text{ je atomická,}\\
& & -_1\mathrm{H}^{\mathcal{A}}(\varphi_0,e), & \text{když } \varphi \text{ je } \neg(\varphi_0),\\
& & \mathrm{H}^{\mathcal{A}}(\varphi_0,e) \to_1 \mathrm{H}^{\mathcal{A}}(\varphi_1,e), & \text{když } \varphi \text{ je } (\varphi_0 \to \varphi_1),\\
& & \min\{\mathrm{H}^{\mathcal{A}}(\varphi_0,e(x/a));\ a \in A\}, & \text{když } \varphi \text{ je } \forall_x(\varphi_0).
\end{array}$$

Přitom $-_1$ resp. $\to_1$ je komplement resp. operace implikace v Booleově algebře $\underline{2}$, tj. $-_1(0) = 1$, $-_1(1) = 0$, pro $a, b \in \{0,1\}$ je $a \to_1 b = 1$, právě když $a = 0$ nebo $b = 1$.

• $\mathrm{H}^{\mathcal{A}}(\varphi, e)$ je *hodnota formule φ v $\mathcal{A}$ při ohodnocení e.*

Indukcí se snadno dokáže, že hodnota $\mathrm{H}^{\mathcal{A}}(\varphi, e)$ nezávisí na e, nevyskytuje-li se ve φ žádná proměnná; pišme pak místo $\mathrm{H}^{\mathcal{A}}(\varphi, e)$ jen

$$\mathrm{H}^{\mathcal{A}}(\varphi).$$

4. *Formule φ platí v $\mathcal{A}$ při ohodnocení e*, právě když $\mathrm{H}^{\mathcal{A}}(\varphi, e) = 1$; píšeme pak

$$\mathcal{A} \models \varphi[e]$$

a říkáme též, že *φ je splněná e v $\mathcal{A}$* nebo *e splňuje φ v $\mathcal{A}$*. Platí-li φ v $\mathcal{A}$ při každém ohodnocení proměnných v A, říkáme, že *φ platí* či *je splněná* či *je pravdivá v $\mathcal{A}$*, píšeme

$$\mathcal{A} \models \varphi.$$

5. Buď $\top$ sentence $\varphi \to \varphi$, kde φ je nějaká fixovaná atomická L-sentence, existuje-li, či uzávěr atomické L-sentence. Buď $\perp$ negace $\top$.

LEMMA 2.2.4. (O hodnocení a platnosti ve struktuře.) *Nechť $\mathcal{A}$ je L-struktura, $e : \mathrm{Var} \to A$, φ, ψ dvě L-formule.*

1) a) $\mathrm{H}^{\mathcal{A}}(\perp, e) = 0$, $\mathrm{H}^{\mathcal{A}}(\top, e) = 1$,
   b) $\mathrm{H}^{\mathcal{A}}(\varphi \vee \psi, e) = \mathrm{H}^{\mathcal{A}}(\varphi, e) \vee_1 \mathrm{H}^{\mathcal{A}}(\psi, e)$, $\mathrm{H}^{\mathcal{A}}(\varphi \,\&\, \psi, e) = \mathrm{H}^{\mathcal{A}}(\varphi, e) \wedge_1 \mathrm{H}^{\mathcal{A}}(\psi, e)$,
   c) $\mathrm{H}^{\mathcal{A}}(\varphi \to \psi, e) = 1 \Leftrightarrow \mathrm{H}^{\mathcal{A}}(\varphi, e) \leq \mathrm{H}^{\mathcal{A}}(\psi, e)$, $\mathrm{H}^{\mathcal{A}}(\varphi \leftrightarrow \psi, e) = 1 \Leftrightarrow \mathrm{H}^{\mathcal{A}}(\varphi, e) = \mathrm{H}^{\mathcal{A}}(\psi, e)$.

2) *Je-li $\diamond$ po řadě $\vee, \&, \to, \leftrightarrow$ a „$\diamond$“ je po řadě nebo, a, implikuje, právě když, tak*
   a) $\mathcal{A} \models \neg\varphi[e]$ *resp.* $\mathcal{A} \models (\varphi \diamond \psi)[e] \Leftrightarrow \mathcal{A} \not\models \varphi[e]$ *resp.* $\mathcal{A} \models \varphi[e]$ „$\diamond$“ $\mathcal{A} \models \psi[e]$,
   b) $\mathcal{A} \models (\forall x)\varphi[e] \Leftrightarrow$ *pro každé $a \in A$ je* $\mathcal{A} \models \varphi[e(x/a)]$,
   c) $\mathcal{A} \models (\exists x)\varphi[e] \Leftrightarrow$ *existuje $a \in A$ s* $\mathcal{A} \models \varphi[e(x/a)]$,
   d) $\mathcal{A} \models \varphi(x_0, \ldots, x_{n-1}) \Leftrightarrow \mathcal{A} \models (\forall x_0, \ldots, x_{n-1})\varphi$.

Důkaz. 1) Jde o je triviální důsledky definic. 2) a) je pro negaci jasné a pro ostatní reformulace 1). b) $\mathcal{A} \models (\forall x)\varphi[e] \Leftrightarrow$ pro každé $a \in A$ je $\mathrm{H}^{\mathcal{A}}(\varphi, e(x/a)) = 1 \Leftrightarrow$ pro každé $a \in A$ je $\mathcal{A} \models \varphi[e(x/a)]$.

c) $\mathcal{A} \models (\exists x)\varphi[e] \Leftrightarrow \mathcal{A} \models \neg(\forall x)\neg\varphi[e] \Leftrightarrow$ není pro každé $a \in A$ splněno $\mathcal{A} \not\models \varphi[e(x/a)] \Leftrightarrow$ existuje $a \in A$ s $\mathcal{A} \models \varphi[e(x/a)]$.

d) Indukcí dle n. Pro $n = 0$ není co dokazovat. Indukční krok z n na $n + 1$ (e je ohodnocení proměnných v A):

$$\begin{array}{rcl}
\mathcal{A} \models \varphi(x_0, \ldots, x_n) & \Leftrightarrow & \text{pro každé } e \text{ je } \mathcal{A} \models \varphi[e]\\
& \Leftrightarrow & \text{pro každé } e \text{ a každé } a \in A \text{ je } \mathcal{A} \models \varphi[e(x_n/a)]\\
& \Leftrightarrow & \text{pro každé } e \text{ je } \mathcal{A} \models (\forall x_n)\varphi[e]\\
& \Leftrightarrow & \mathcal{A} \models (\forall x_0, \ldots, x_{n-1})(\forall x_n)\varphi
\end{array}$$

Prvá ekvivalence je dána definicí, druhá plyne triviálně, třetí plyne z b) a čtvrtá z indukčního předpokladu. □

TVRZENÍ 2.2.5.

1) (O hodnotě a platnosti v reduktu.) *Buďte $L \subseteq L'$, $\mathcal{A}' \models L'$, $\mathcal{A}$ redukt $\mathcal{A}'$ na L, e ohodnocení proměnných v A ($= A'$). Pak*
   a) *pro L-term t platí* $t^{A}[e] = t^{A'}[e]$, b) *pro L-formuli φ platí* $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{A}' \models \varphi[e]$.

2) *Nechť X je podmnožina univerza L-struktury $\mathcal{A}$ a L obsahuje konstantní symbol či $X \neq \emptyset$. Pak univerzum struktury $\mathcal{A}\langle X\rangle$ je množina $B = \{t^{A}[e];\ t$ je L-term a $e : \mathrm{Var} \to X\}$.*

3) (O platnosti otevřených formulí.)

$$\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{A}' \models \varphi[e] \textit{ pro } \varphi \textit{ otevřenou, } \mathcal{A}' \subseteq \mathcal{A} \textit{ a } e : \mathrm{Var} \to A'. \tag{2.1}$$

Důsledky:

a) *Otevřená formule platí ve struktuře, právě když platí v každé její konečně generované podstruktuře, právě když platí v každé podstruktuře.*

b) *Podstruktura modelu otevřeně axiomatizovatelné teorie T je modelem teorie T.*

Důkaz. 1) a) Snadno indukcí na L-termech. b) Snadno indukcí na L-formulích.

2) Zřejmě je B univerzem podstruktury struktury $\mathcal{A}$. Je-li $\mathcal{B}' \subseteq \mathcal{A}$ a $X \subseteq B'$, je jasně $B \subseteq B'$.

3) Je-li φ atomická, jasně to platí, neboť hodnota termu v podstruktuře $\mathcal{A}' \subseteq \mathcal{A}$ je stejná jako v $\mathcal{A}$. Indukcí podle složitosti φ plyne snadno dokazované. Důsledek a) plyne ihned z (2.1), b) je důsledkem a). □

TVRZENÍ 2.2.6. (O nezávislosti hodnoty a platnosti na proměnných.) *Nechť $\mathcal{A}$ je L-struktura a t resp. φ nějaký L-term resp. L-formule, e, e' jsou ohodnocení proměnných v A, která se rovnají na všech proměnných termu t resp. volných proměnných formule φ. Pak platí:*

$$\text{a) } t^A[e] = t^A[e'], \qquad \text{b) } \mathcal{A} \models \varphi[e], \textit{ právě když } \mathcal{A} \models \varphi[e'].$$

Speciálně pro t bez proměnných a sentenci φ nezávisí $t^A[e]$ a $\mathcal{A} \models \varphi[e]$ na e.

Důkaz. a) plyne bezprostředně indukcí na termech. b) se dokáže snadno indukcí na formulích; uveďme jen indukční krok pro univerzální kvantifikátor. Buď φ tvaru $(\forall x)\psi$ a nechť pro ψ tvrzení platí. Volné proměnné formule ψ jsou volné proměnné formule φ a eventuálně ještě proměnná x. Pak zřejmě platí:

$$\begin{aligned} \mathcal{A} \models \varphi[e] \quad &\Leftrightarrow \quad \text{pro každé } a \in A \text{ je } \mathcal{A} \models \psi[e(x/a)] \\ &\Leftrightarrow \quad \text{pro každé } a \in A \text{ je } \mathcal{A} \models \psi[e'(x/a)] \quad \Leftrightarrow \quad \mathcal{A} \models \varphi[e']. \end{aligned}$$

□

2.2.7. Parciální ohodnocení proměnných pro term či formuli. Rozšíření vztahu $\models$.

Pomocí 2.2.6 rozšíříme přirozeně význam $t^A[e]$ a $\mathcal{A} \models \varphi[e]$. Řekneme, že zobrazení $e \subseteq \mathrm{Var} \times A$ je *parciální ohodnocení proměnných v A*, a dále, že je *pro t* resp. *φ v A*, pokud definiční obor e obsahuje každou proměnnou termu t resp. volnou proměnnou formule φ. Pro takové e nechť značí

$$t^A[e] \quad \text{resp.} \quad \mathcal{A} \models \varphi[e]$$

hodnotu $t^A[e']$ resp. vztah $\mathcal{A} \models \varphi[e']$, kde $e' : \mathrm{Var} \to A$ s $e \subseteq e'$ je libovolné; to je dle 2.2.6 korektní.

ZNAČENÍ 2.2.8. Je-li $\overline{x} = \langle x_0, \dots, x_{n-1} \rangle$ prostá sekvence proměnných a $\overline{a} = \langle a_0, \dots, a_{n-1} \rangle \in A^n$, značíme parciální ohodnocení proměnných $e = \{\langle x_i, a_i \rangle;\ i < n\}$ jako

$$\overline{x}|\overline{a}, \ \text{stručněji} \ \langle a_0, \dots, a_{n-1} \rangle \ \text{nebo jen} \ \overline{a} \tag{2.2}$$

(nevede-li to k nedorozumění). Pro proměnnou y pak značí $\overline{a}(y/b)$ ohodnocení, nabývající hodnotu b v y a hodnotu a_i pro x_i různé od y. Speciálně je výše uvedené e, tj. $\langle a_0, \dots, a_{n-1} \rangle$ čili $\overline{a}$, ohodnocení pro term $t(x_0, \dots, x_{n-1})$ a formuli $\varphi(x_0, \dots, x_{n-1})$ v A. Píšeme pak

$$\begin{array}{ccccccc} t^A[\overline{x}|\overline{a}] & \text{či} & t^A[a_0, \dots, a_{n-1}] & \text{či} & t^A[\overline{a}] & \text{místo} & t^A[e], \\ \mathcal{A} \models \varphi[\overline{x}|\overline{a}] & \text{či} & \mathcal{A} \models \varphi[a_0, \dots, a_{n-1}] & \text{či} & \mathcal{A} \models \varphi[\overline{a}] & \text{místo} & \mathcal{A} \models \varphi[e]. \end{array}$$

2.2.9. Extenze L_X jazyka o jména. Expanze $\mathcal{A}_X$.

O prvcích univerza dané L-struktury $\mathcal{A}$ můžeme referovat pomocí extenze L_A jazyka L o tzv. jména prvků z A. Definujme to poněkud obecněji následovně.

Nechť $\mathcal{A}$ je L-struktura, $X \subseteq A$. *Extenze* jazyka L o *jména prvků* z množiny X je extenze $\langle L, c_a \rangle_{a \in X}$ jazyka L o nové navzájem různé konstantní symboly $\langle c_a;\ a \in X \rangle$. Značíme ji

$$L_X.$$

Konstantní symbol c_a prezentuje individuum a v jazyce; říkáme, že to je *individuální konstanta.* Buď navíc $\mathcal{B}$ je nějaká L-struktura, $X \subseteq A$ a $f : X \to B$. Pak přirozená expanze struktury $\mathcal{A}$ o jména prvků z X resp. přirozená expanze struktury $\mathcal{B}$ o jména prvků z X via f je L_X-struktura

$$\mathcal{A}_X = \langle \mathcal{A}, a \rangle_{a \in X} \quad \text{resp.} \quad \mathcal{B}_{fX} = \langle \mathcal{B}, fa \rangle_{a \in X};$$

c_a je v prvé resp. druhé interpretováno jako a resp. fa pro každé $a \in X$.

Nechť $\varphi(\overline{x}, \overline{y})$ je L-formule, $\langle a_0, \ldots, a_{n-1} \rangle = \overline{a} \in A^{\mathrm{l}(\overline{a})}$. Píšeme též

$$\varphi(\overline{a}, \overline{y}) \quad \text{místo} \quad \varphi(x_0/c_{a_0}, \ldots, x_{n-1}/c_{a_{n-1}}, \overline{y});$$

podobně je tomu s L-termem $t(\overline{x}, \overline{y})$ a dále se symboly $t(\overline{a}, \overline{b})$, $\varphi(\overline{a}, \overline{b})$ s $\overline{b} \in A^{\mathrm{l}(\overline{y})}$. Analogicky je tomu s $\varphi(\overline{x}, \overline{y}, \overline{z})$ atd. Místo $\mathcal{A}_X \models \psi(\overline{a})$ píšeme též někdy jen $\mathcal{A} \models \psi(\overline{a})$.

LEMMA 2.2.10. (O jménech.) *Nechť $\mathcal{A}$ je L-struktura, $X \subseteq A$, $t(\overline{x}, \overline{y})$ je L-term, $\varphi(\overline{x}, \overline{y})$ je L-formule, $\overline{a} \in A^{\mathrm{l}(\overline{x})}$, $\overline{b} \in X^{\mathrm{l}(\overline{y})}$. Pak*

$$t^{\mathcal{A}}[\overline{a}, \overline{b}] \;=\; t(\overline{b})^{\mathcal{A}_X}[\overline{a}], \qquad \mathcal{A} \models \varphi(\overline{x}, \overline{y})[\overline{a}, \overline{b}] \;\Leftrightarrow\; \mathcal{A}_X \models \varphi(\overline{x}, \overline{b})[\overline{a}]. \tag{2.3}$$

Speciálně pro L-formuli $\psi(\overline{y})$ je $\mathcal{A} \models \psi[\overline{b}] \Leftrightarrow \mathcal{A}_X \models \psi(\overline{b})$.

Důkaz. Tvrzení o termech plyne indukcí podle složitosti t bezprostředně. Odtud plyne ihned (2.3) pro φ atomickou. Zbytek plyne snadno indukcí podle složitosti φ. □

Model teorie. Axiomatizovatelnost tříd struktur.

2.2.11. Model teorie, třída modelů teorie. Axiomatizovatelnost třídy struktur.

1. *Model L-teorie T* je L-struktura $\mathcal{A}$, ve které platí každý axiom L-teorie T; píšeme

$$\mathcal{A} \models T.$$

2. *Třída všech modelů teorie T* resp. *velikosti κ* resp. *konečných* resp. *nekonečných* se značí

$$\mathsf{M}(T) \text{ resp. } \mathsf{M}_\kappa(T) \text{ resp. } \mathsf{M}_{<\infty}(T) \text{ resp. } \mathsf{M}_\infty(T),$$

Je-li T prázdná L-teorie, místo $\mathsf{M}_*(T)$ píšeme $\mathsf{M}_*(L)$. Platí tedy např.

$$\mathsf{M}_\kappa(T) \subseteq \mathsf{M}_{<\infty}(T) \cup \mathsf{M}_\infty(T) = \mathsf{M}(T) \subseteq \mathsf{M}(L).$$

Zřejmě je $\kappa_L \in \mathsf{M}_\kappa(L)$ pro každé $\kappa \neq \emptyset$.

3. Buď K třída L-struktur, tj. $\mathsf{K} \subseteq \mathsf{M}(L)$. Třída K je *axiomatizovatelná* resp. *konečně axiomatizovatelná*, existuje-li L-teorie T resp. navíc konečná tak, že $\mathsf{K} = \mathsf{M}(T)$. Symbolem $-\mathsf{K}$ dále značíme *komplement třídy modelů K*, tj. třídu $\mathsf{M}(L) - \mathsf{K}$.

Problémem, jak vypadá $\mathsf{M}(T)$ konkrétněji, jaké jsou třídy $\mathsf{M}_\kappa(T)$ a jaké druhy modelů jsou v nich, se v plné šíři zabývá teorie modelů.

Pravdivost v teorii.

2.2.12. Pravdivost v teorii: $T \models \varphi$.

1. *Formule φ platí* čili *je pravdivá v teorii T*, je-li φ formule teorie T, která platí v každém modelu teorie T; píšeme

$$T \models \varphi.$$

Když $T \models \neg\varphi$, je φ *lživá v T*. Není-li φ ani pravdivá ani lživá v T, je *sémanticky nezávislá v T*. Obor všech formulí [sentencí] pravdivých v T resp. formulí [sentencí] lživých v T značíme

$$\mathrm{Tru}(T) \ [\mathrm{Tr}(T)] \quad \text{resp.} \quad \mathrm{nTru}(T) \ [\mathrm{nTr}(T)].$$

2. Formule φ je *sémanticky konzistentní s T*, když není lživá v T, tj. když $T \not\models \neg\varphi$, čili když existuje struktura $\mathcal{A}$ s $\mathcal{A} \models T \cup \{(\exists\overline{v})\varphi\}$, pokud je φ v proměnných $\overline{v}$.

Je-li T prázdná L-teorie, píšeme $\models$ či $L \models$ místo $T \models$ a frázi „v(s) T" vynecháváme či říkáme *v L* eventuálně jen *v logice*, a píšeme $\mathrm{Tru}(L)$ resp. $\mathrm{nTru}(L)$ místo $\mathrm{Tru}(T)$ resp. $\mathrm{nTru}(T)$ atd.

Nyní je přehledně formulovatelná zásadní, zatím nedokázaná věta o kompletnosti predikátové logiky: *Pro teorii T a její formuli φ je $T \vdash \varphi \Leftrightarrow T \models \varphi$.* Platnost implikace $\Rightarrow$ se nazývá korektnost predikátové logiky; důkaz je snadný, jak uvádíme níže. Obtížnější důkaz implikace $\Leftarrow$ uvedeme později, a to na základě zásadního poznatku predikátové logiky: $\mathsf{M}(T) \neq \emptyset \Leftrightarrow T$ je bezesporná.

Následující lemmata formulují elementární vlastnosti sémantiky spojek $\neg, \vee, \&, \rightarrow, \leftrightarrow$.

LEMMA 2.2.13. (O sémantice $\neg, \vee, \&$.) *Nechť $\mathcal{A}$ je L-struktura a $\varphi_0, \ldots, \varphi_n$ jsou L-formule. Pak:*

1) a)
$$\begin{aligned} \mathcal{A} \models \varphi_0 &\Rightarrow \mathcal{A} \not\models \neg\varphi_0 \\ \mathcal{A} \models \varphi_1 \textit{ nebo } \cdots \textit{ nebo } \mathcal{A} \models \varphi_n &\Rightarrow \mathcal{A} \models \varphi_1 \vee \cdots \vee \varphi_n \\ \mathcal{A} \models \varphi_1 \textit{ a } \cdots \textit{ a } \mathcal{A} \models \varphi_n &\Leftrightarrow \mathcal{A} \models \varphi_1 \& \cdots \& \varphi_n \\ \mathcal{A} \models \varphi_0 &\Leftrightarrow \mathcal{A} \models \text{g.c.}(\varphi_0). \end{aligned}$$

b)
$$\begin{aligned} \mathsf{M}(T, \varphi_0) &\subseteq \mathsf{M}(T) - \mathsf{M}(\neg\varphi_0) = \mathsf{M}(T) - \mathsf{M}(T, \neg\varphi_0) \\ \mathsf{M}(T, \varphi_1) \cup \cdots \cup \mathsf{M}(T, \varphi_n) &\subseteq \mathsf{M}(T, \varphi_1 \vee \cdots \vee \varphi_n) \\ \mathsf{M}(T, \varphi_1) \cap \cdots \cap \mathsf{M}(T, \varphi_n) &= \mathsf{M}(T, \varphi_1 \& \cdots \& \varphi_n) \\ \mathsf{M}(T, \text{g.c.}(\varphi_0)) &= \mathsf{M}(T, \varphi_0) \end{aligned}$$

c) *Uvedené dvě implikace $\Rightarrow$ resp. inkluze $\subseteq$ nelze obrátit. Jsou-li však $\varphi_0, \ldots, \varphi_n$ sentence, lze je i obrátit.*

2) *Nechť T je L-teorie. Píšeme-li v* 1) a) *T místo $\mathcal{A}$, získané vztahy platí a $\Rightarrow$ nelze obrátit.*

Důkaz. 1) Dokážeme a); b) je bezprostředním důsledkem. Nechť e je ohodnocení proměnných v A. První implikace: z $\mathcal{A} \models \varphi_0[e]$ plyne $\mathcal{A} \not\models \neg\varphi_0[e]$; tudíž dokazované platí. Podobně snadno plynou ostatní tři vztahy. c) Prvou implikaci $\Rightarrow$ nelze obrátit. Buď totiž φ_0 formule $x \leq 0$, $\mathcal{A} = \langle \mathbb{Z}, \leq, 0 \rangle$. Pak $\mathcal{A} \not\models \neg\varphi_0$, $\mathcal{A} \not\models \varphi_0$. Podobně je to s druhou implikací $\Rightarrow$. Odtud pak plyne, že nelze obrátit ani inkluze $\subseteq$. Nechť e je ohodnocení proměnných v A. Je-li φ_0 sentence, tak
$$\mathcal{A} \models \varphi_0 \quad \Leftrightarrow \quad \mathcal{A} \models \varphi_0[e] \quad \Leftrightarrow \quad \mathcal{A} \not\models \neg\varphi_0[e] \quad \Leftrightarrow \quad \mathcal{A} \not\models \neg\varphi_0,$$
neboť hodnota $\mathcal{A} \models \varphi_0[e]$ nezávisí na e. Podobně je tomu s disjunkcí.

2) je bezprostřední důsledek 1) a). □

PŘÍKLAD. Pro sentence nemusí platit $\Leftrightarrow$ místo $\Rightarrow$ v prvém vztahu z 2.2.13 2). Je-li totiž T teorie s modelem, tak $T \models \varphi \Leftrightarrow T \not\models \neg\varphi$ platí pro každou $L(T)$-sentenci φ, právě když je T sémanticky kompletní, tj. právě když je každá $L(T)$-sentence nebo její negace v T pravdivá.

LEMMA 2.2.14. (O sémantice $\rightarrow$, $\leftrightarrow$) *Nechť T je teorie a φ, ψ, χ její formule.*

1) *Platí*
$$T \models \varphi \rightarrow \psi \Rightarrow \mathsf{M}(T, \varphi) \subseteq \mathsf{M}(T, \psi), \qquad T \models \varphi \leftrightarrow \psi \Rightarrow \mathsf{M}(T, \varphi) = \mathsf{M}(T, \psi).$$
Implikace $\Rightarrow$ nelze obecně obrátit, jsou-li však φ_0, φ_1 sentence, lze je obrátit.

2) *Platí:*
$$\begin{aligned} T \models \varphi \rightarrow \psi & &\Leftrightarrow&\quad T \models \neg\psi \rightarrow \neg\varphi \\ T \models \varphi \leftrightarrow \psi & &\Leftrightarrow&\quad T \models \varphi \rightarrow \psi \;\; \textit{a} \;\; T \models \psi \rightarrow \varphi \\ T \models \varphi \rightarrow \psi \;\; \textit{a} \;\; T \models \psi \rightarrow \chi & &\Rightarrow&\quad T \models \varphi \rightarrow \chi \\ T \models \varphi \leftrightarrow \psi \;\; \textit{a} \;\; T \models \psi \leftrightarrow \chi & &\Rightarrow&\quad T \models \varphi \leftrightarrow \chi \\ T \models \varphi \leftrightarrow \psi & &\Rightarrow&\quad (T \models \varphi \Leftrightarrow T \models \psi). \textit{ Implikaci nelze obrátit.} \end{aligned}$$

3) *Rozbor případů.*
$$\begin{aligned} \text{a)}\quad & T \models (\varphi \vee \psi) \rightarrow \chi \quad \Leftrightarrow \quad (T \models \varphi \rightarrow \chi \;\; \textit{a} \;\; T \models \psi \rightarrow \chi) \\ \text{b)}\quad & (T \models \varphi \rightarrow \psi \;\; \textit{a} \;\; T \models \neg\varphi \rightarrow \psi) \quad \Rightarrow \quad T \models \psi \end{aligned}$$

Důkaz. 1) Implikace $\Rightarrow$ plynou snadno. Prvou $\Rightarrow$ nelze obrátit. Buď totiž T teorie v jazyce $L = \langle 0, 1 \rangle$ s rovností a jediným mimologickým axiomem „existují alespoň dva prvky“. Pak $\mathsf{M}(T, x = 0) = \emptyset = \mathsf{M}(T, x = 1)$, avšak $T \not\models x = 0 \rightarrow x = 1$, neboť $\mathcal{A} \not\models (x = 0 \rightarrow x = 1)[0]$, kde $\mathcal{A} = \langle \{0, 1\}, 0, 1 \rangle \models T$. Podobně je tomu s $\leftrightarrow$ a tvrzení o sentencích se dokáže snadno.

2) Důkazy $\Leftrightarrow$ a $\Rightarrow$ plynou bezprostředně z definice $\models$. Dokážeme neobratitelnost poslední $\Rightarrow$. Buď $L = \langle U, c, d \rangle$, kde U je unární relační a c, d konstantní symboly. Zřejmě $\not\models U(c)$, $\not\models U(d)$, tedy $\models U(c) \Leftrightarrow \models U(d)$. Avšak $\not\models U(c) \leftrightarrow U(d)$.

3) a) plyne bezprostředně z definice $\models$, b) je důsledek a). □

2.2.15. Struktura formulí.

Nechť L je jazyk. Zřejmě $\models \top$, $\models \neg\bot$, tj. $\top$ je pravdivá L-sentence a $\bot$ lživá.

Struktura formulí jazyka L je struktura

$$\underline{\mathrm{Fm}}_L = \langle \mathrm{Fm}_L, \neg, \vee, \&, \bot, \top \rangle$$

pro jazyk Booleových algeber; logické spojky chápeme jako operace, $\bot$ a $\top$ jako konstanty 0 a 1. Operace $\vee$ není komutativní, neboť formule $\varphi \vee \psi$ s různými φ, ψ není jako výraz (tice) roven $\psi \vee \varphi$; podobně je tomu s $\&$.

Buď n přirozené. Pak $\underline{\mathrm{Fm}}_L^n$ značí podstrukturu $\underline{\mathrm{Fm}}_L$ s univerzem Fm_L^n: $\underline{\mathrm{Fm}}_L^n = \underline{\mathrm{Fm}}_L \restriction \mathrm{Fm}_L^n$.

Výroková logika – expozice.

2.2.16. **Koncept syntaxe a sémantiky.**

1. **Syntax.** Nechť $L^{\mathbb{P}}$ značí jazyk bez rovnosti, který má jako mimologické symboly jen nulární relační symboly, tvořící neprázdnou množinu $\mathbb{P}$. Symboly z $\mathbb{P}$ se nazývají též *prvovýroky* či *výrokové proměnné*, bezkvantifikátorové $L^{\mathbb{P}}$-formule se nazývají *výroky*, obšírněji $\mathbb{P}$-výroky, a též *výrokové formule* nad $\mathbb{P}$; jejich množinu značíme $\mathrm{VF}_{\mathbb{P}}$. Jsou to formule *výrokové logiky.* Její *jazyk* a *bazální syntax* (jež je „výrokovou restrikcí“ syntaxe predikátové logiky bez rovnosti s jazykem $L^{\mathbb{P}}$) jsou dány takto:

- *Logické symboly jazyka jsou* spojky $\neg, \rightarrow$*,* mimologické pak tvoří neprázdná množina $\mathbb{P}$ prvovýroků. Říkáme též, že $\mathbb{P}$ je *jazyk výrokové logiky.* $\mathrm{VF}_{\mathbb{P}}$ *je množina všech* $\mathbb{P}$*-výroků. Symbol* $\mathbb{P}$ *dále vždy značí množinu všech prvovýroků nějakého výrokového jazyka a také takový jazyk.*
- Logické axiomy výrokové logiky jsou dány schematy (PL1) – (PL3), pravidlem dedukce je pravidlo modus ponens.
- Dvojice $\mathbb{P}, T$ s $T \subseteq \mathrm{VF}_{\mathbb{P}}$, stručněji T, je *výroková teorie nad* $\mathbb{P}$ či $\mathbb{P}$-teorie; $L(T)$ značí jazyk T. Pojem důkazu v T a $T \vdash \varphi$ jsou stejné jako v predikátové logice bez rovnosti, odhlédneme-li od logických axiomů o kvantifikátorech a pravidla generalizace. Pro názornost můžeme psát $\vdash_{\mathbb{P}}$ místo $\vdash$.

Základní rozvoj syntaxe výrokové logiky s jazykem $\mathbb{P}$ je týž, jako u predikátové logiky s jazykem $L^{\mathbb{P}}$ s uvedenými restrikcemi. Např. spojky $\vee, \&, \leftrightarrow$ zavádíme jako zkratky atd.

Je patrné, že pro jazyk L predikátové logiky jsou L-formule výroky nad množinou $\mathbb{P}_L$ atomických a kvantifikací začínajících L-formulí jakožto prvovýroků, a že pro výrok φ nad $\mathbb{P}_L$ platí:

$$\vdash_{\mathbb{P}_L} \varphi \quad \Rightarrow \; \vdash \varphi.$$

2. **Sémantika.** Nějaká $L^{\mathbb{P}}$-struktura $\mathcal{A} = \langle A, p^A \rangle_{p \in \mathbb{P}}$ je zřejmě z hlediska platnosti formulí plně určená funkcí $v : \mathbb{P} \to 2$ takovou, že pro $p \in \mathbb{P}$ je

$$v(p) = p^A \; (\subseteq A^0);$$

říkáme, že takové v je *pravdivostní ohodnocení prvovýroků* a také *model výrokového jazyka* $\mathbb{P}$; zřejmě nezávisí na A. Extenze ohodnocení $\overline{v} : \mathrm{VF}_{\mathbb{P}} \to 2$ se sestrojí rekurzí pravidly:

$$\overline{v}(p) = v(p), \qquad \overline{v}(\neg\varphi) = -_1\overline{v}(\varphi), \qquad \overline{v}(\varphi \to \psi) = \to_1 (\overline{v}(\varphi), \overline{v}(\psi)).$$

Zřejmě nyní pro výrok φ platí, jak plyne snadno indukcí dle složitosti φ: $\mathcal{A} \models \varphi \quad \Leftrightarrow \quad \overline{v}(\varphi) = 1$. Místo $\overline{v}(\varphi) = 1$ můžeme též psát $v \models \varphi$. Uvedené poznatky nás vedou k následujícím definicím.

Buď T výroková teorie nad $\mathbb{P}$.

• Funkce $v \in {}^{\mathbb{P}}2$ je *model* T, když $\overline{v}(\varphi) = 1$ pro každý axiom T; píšeme

$$v \models T;$$

Má-li teorie T či formule φ model, říkáme, že je *splnitelná.* Množinu všech modelů teorie T značíme $\mathsf{M}_{\mathbb{P}}(T)$, stručněji $\mathsf{M}(T)$, je-li T prázdná, pak $\mathsf{M}(\mathbb{P})$; tudíž

$$\mathsf{M}_{\mathbb{P}}(T) \subseteq \mathsf{M}(\mathbb{P}) = {}^{\mathbb{P}}2.$$

• Výrok φ je *pravdivý* resp. *lživý v* T, platí-li v každém resp. žádném modelu teorie T; je-li φ výrok pravdivý v T, píšeme

$$T \models \varphi.$$

Když je T prázdná, píšeme jen $\models \varphi$, někdy $\mathbb{P} \models \varphi$, a říkáme pak též, že φ je *tautologie.* Množinu všech pravdivých resp. lživých výroků v T značíme

$$\mathrm{Tru}_{\mathbb{P}}(T), \text{ stručněji } \mathrm{Tru}(T) \qquad \text{resp.} \qquad \mathrm{nTru}_{\mathbb{P}}(T), \text{ stručněji } n\mathrm{Tru}(T).$$

Když T je prázdná, nepíšeme T. Množina všech tautologií resp. splnitelných výroků se značí též $\mathrm{T{\small AUT}}_{\mathbb{P}}$ resp. $\mathrm{S{\small AT}}_{\mathbb{P}}$.

Zřejmě pro L-formuli φ platí: $\mathbb{P}_L \models \varphi \Rightarrow \models \varphi$. To můžeme zformulovat též následovně:

TVRZENÍ 2.2.17. (O pravdivosti tautologií v predikátové logice.) *Pro jazyk L (v predikátové logice) a jeho formuli φ platí: φ je tautologie (jakožto výrok nad $\mathbb{P}_L$) $\Rightarrow$ $\models \varphi$.*

PŘÍKLADY. 1. Platí $\models ((\forall x)\psi \mathbin{\&} \varphi) \to \neg(\neg\varphi \vee \neg(\forall x)\psi)$. Označíme-li totiž χ „prvovýrok" $(\forall x)\psi$, jde o tautologii $(\chi \mathbin{\&} \varphi) \to \neg(\neg\varphi \vee \neg\chi)$.

2. Implikaci v 2.2.17 nelze obrátit, jak ukazují následující a), b).

a) Buď L jazyk s rovností. Pak $\models x = x$, ale $\mathbb{P}_L \not\models x = x$.

b) Buď L jazyk bez rovnosti, s relačním symbolem R. Pak $\models (\forall \overline{x})R(\overline{x}) \to R(\overline{x})$ (s $\mathrm{l}(\overline{x}) = n$), ale $\mathbb{P}_L \not\models (\forall \overline{x})R(\overline{x}) \to R(\overline{x})$, protože v uvedené implikaci jsou antecedent a konsekvent různé prvovýroky.

Sémantické verze pojmů.

2.2.18.

Pojmy spornost, kompletnost, extenze a ekvivalence, konečná či otevřená axiomatizovatelnost teorií, jsme definovali syntakticky, užitím $\vdash$. Definici sémantické verze obdržíme nahrazením vztahu $\vdash$ v „syntaktické" definici vztahem $\models$. Získáme tak příslušný pojem sémanticky, např. pojem teorie je sporná sémanticky, kompletní sémanticky atd. Takový pojem bude ekvivalentní s původním „syntaktickým"; to vyplyne až z kompletnosti predikátové logiky. Syntaktické verze pojmů jsou užitečné pro porozumění sémantice, aniž bychom se dovolávali kompletnosti predikátové logiky. Formulujme je výslovně (i když schema tvorby jejich definic jsme již uvedli).

1. Teorie T je *sporná sémanticky*, pokud $T \models \varphi$ pro každou $L(T)$-formuli φ; jinak je T *bezesporná sémanticky.*

Zřejmě platí:

$$T \text{ je bezesporná sémanticky} \Leftrightarrow T \text{ má model} \Rightarrow T \text{ je bezesporná.}$$

Opačná implikace, tj. T je bezesporná $\Rightarrow$ T má model, je značně netriviální tvrzení, které, jak ukážeme později, je ekvivalentní s $T \models \varphi \Rightarrow T \vdash \varphi$ pro každou $L(T)$-formuli φ.

2. Teorie T je *kompletní sémanticky*, pokud má model a každá $L(T)$-sentence je pravdivá či lživá v T.

Zřejmě platí:

Má-li teorie model a je kompletní, je kompletní sémanticky.

3. Teorie T' je *extenze teorie T sémanticky* T, když $L(T) \subseteq L(T')$ a $\mathrm{Tru}(T) \subseteq \mathrm{Tru}(T')$. Pokud $L(T) = L(T')$, je to *jednoduchá extenze teorie T sémanticky.* Pokud $\mathrm{Tru}(T) = \mathrm{Tru}(T') \cap \mathrm{Fm}_{L(T)}$, je to *konzervativní extenze teorie T sémanticky.*

4. Teorie T' je *ekvivalentní s teorií T sémanticky*, je-li T' extenzí T sémanticky a naopak.

5. Teorie je *konečně* resp. *otevřeně axiomatizovatelná sémanticky*, pokud je ekvivalentní s nějakou teorií sémanticky, která je konečně axiomatizovaná resp. otevřená.

Následující tvrzení sumarizují užitečné vlastnosti některých uvedených pojmů. ($\restriction$ značí redukt.)

TVRZENÍ 2.2.19.

1) (Vlastnosti $\mathrm{Tru}(T)$.)

a) $\mathsf{M}(\mathrm{Tru}(T)) = \mathsf{M}(T)$. b) $\mathrm{Tru}(T) \subseteq \mathrm{Tru}(T') \Leftrightarrow \mathsf{M}(T') \restriction L(T) \subseteq \mathsf{M}(T)$.

c) $\mathrm{Tru}(T) = \mathrm{Tru}(\mathrm{Tru}(T))$. d) $T \subseteq T' \Rightarrow \mathrm{Tru}(T) \subseteq \mathrm{Tru}(T')$.

2) (O extenzi a ekvivalenci teorií sémanticky.)

a) *T' je extenze T sémanticky* $\Leftrightarrow$ *$L(T) \subseteq L(T')$ a $\mathsf{M}(T') \restriction L(T) \subseteq \mathsf{M}(T)$.*

b) *T' je ekvivalentní s T sémanticky* $\Leftrightarrow$ *$L(T) = L(T')$ a $\mathsf{M}(T') = \mathsf{M}(T)$.*

Důkaz. 1) a) Když $\mathcal{A} \models T$, tak $\mathcal{A} \models \mathrm{Tru}(T)$. Když $\mathcal{A} \models \mathrm{Tru}(T)$, tak $\mathcal{A} \models T$ díky $T \subseteq \mathrm{Tru}(T)$.b) Implikace $\Rightarrow$. Buď $\mathcal{A}' \models T'$ a $\varphi \in T$; dokazujeme $\mathcal{A}' \,|\, L(T) \models \varphi$. Je $\varphi \in \mathrm{Tru}(T')$, tedy $\mathcal{A}' \models \varphi$ a tedy i $\mathcal{A}' \,|\, L(T) \models \varphi$. Implikace $\Leftarrow$. Buď $\varphi \in \mathrm{Tru}(T')$, $\mathcal{A}' \models T$; dokazujeme $\mathcal{A}' \models \varphi$. Je $\mathcal{A}' \,|\, L(T) \in \mathsf{M}(T)$, tedy $\mathcal{A}' \,|\, L(T) \models \varphi$, tedy i $\mathcal{A}' \models \varphi$. 1) c) plyne z a). d) je jasné.

2) a) plyne ihned z definice a 1) b). b) je důsledkem a). □

Zřejmě platí

$$\models \neg(\exists x)\varphi \leftrightarrow (\forall x)\neg\varphi,$$

neboť $\models \neg(\exists x)\varphi \leftrightarrow \neg\neg(\forall x)\neg\varphi$ plyne z definice $\exists$ a díky $\models \psi \leftrightarrow \psi$, díky $\models \neg\neg\psi \leftrightarrow \psi$ a tranzitivitě $\leftrightarrow$ pak platí $\models \neg(\exists x)\varphi \leftrightarrow (\forall x)\neg\varphi$.

Velmi užitečná jsou následující tvrzení.

TVRZENÍ 2.2.20. *Nechť T je teorie.*

1) (Pravidlo distribuce kvantifikátoru sémanticky.) *Když Q je $\forall$ nebo $\exists$, tak*
$$(T \models \varphi \to [\leftrightarrow]\, \psi) \quad \Rightarrow \quad T \models (Qx)\varphi \to [\leftrightarrow]\, (Qx)\psi.$$
2) (O ekvivalenci sémanticky.) *Platí*
$$T \models \psi_0 \leftrightarrow \psi'_0, \ldots, T \models \psi_{n-1} \leftrightarrow \psi'_{n-1} \;\;\Rightarrow\;\; T \models \varphi \leftrightarrow \varphi^*,$$
kde φ^* se získá z φ nahrazením nějakých výskytů podformule ψ_i ve φ formulí ψ'_i pro $i < n$.

Důkaz. 1) Předpokládáme
$$\mathcal{A} \models T,\, e : \mathrm{Var} \to A,\, a \in A \quad \Rightarrow \quad \mathrm{H}^{\mathcal{A}}(\varphi, e(x/a)) \leq [=]\, \mathrm{H}^{\mathcal{A}}(\psi, e(x/a)).$$
Užitím definice $\mathrm{H}^{\mathcal{A}}((Qx)\varphi, e)$ a $\mathrm{H}^{\mathcal{A}}((Qx)\psi, e)$ (pomocí minima a maxima) dostaneme dokazované
$$\mathcal{A} \models T,\, e : \mathrm{Var} \to A \quad \Rightarrow \quad \mathrm{H}^{\mathcal{A}}((Qx)\varphi, e) \leq [=]\, \mathrm{H}^{\mathcal{A}}((Qx)\psi, e).$$
2) Indukcí dle složitosti φ. Je-li φ atomická, φ^* je φ nebo některé ψ'_i a φ je ψ_i; tvrzení platí.

Nechť φ je tvaru $\neg\varphi_0$ resp. $\varphi_0 \to \varphi_1$ a pro φ_0 a φ_1 to platí. Máme dokázat:
$$\mathcal{A} \models T,\, e : \mathrm{Var} \to A \quad \Rightarrow \quad \mathrm{H}^{\mathcal{A}}(\varphi, e) = \mathrm{H}^{\mathcal{A}}(\varphi', e). \tag{2.4}$$
Dosadíme-li v (2.4) za φ formuli $\neg\varphi_0$ resp. $\varphi_0 \to \varphi_1$ a podobně pro hvězdičkovanou verzi (což je φ^*), vidíme že (2.4) opět platí. Indukční krok pro $\forall$ plyne ihned z 1) pro $\leftrightarrow$ a Q rovno $\forall$. □

Korektnost.

TVRZENÍ 2.2.21. (O korektnosti substituce.) *Nechť $\mathcal{A}$ je L-struktura, t, s jsou termy, φ je formule jazyka L a e ohodnocení proměnných v A. Platí:*

$$1)\;\; t(x/s)[e] = t[e(x/s[e])]. \qquad\qquad 2)\;\; \mathcal{A} \models \varphi(x/s)[e] \Leftrightarrow \mathcal{A} \models \varphi[e(x/s[e])].$$

Důkaz. 1) Indukcí na termech. Buď t proměnná y. Je-li y proměnná x, je vlevo $s[e]$ a vpravo je také $s[e]$. Když y není x, je vlevo $e(y)$ a vpravo také. Nechť t je $F(t_1, \ldots, t_m)$, kde F je m-ární funkční symbol a pro termy $t_1, \ldots, t_m$ tvrzení platí. Pak $t(x/s)[e] = F(t_1(x/s), \ldots)[e] = F^A(t_1(x/s)[e], \ldots) = F^A(t_1[e(x/s[e])], \ldots) = t[e(x/s[e])]$.

2) Indukcí na formulích. Pro φ atomickou tvaru $R(t_1, \ldots, t_m)$ to platí, neboť

$$\mathcal{A} \models \varphi(x/s)[e] \Leftrightarrow \mathcal{A} \models R(t_1(x/s), \ldots)[e] \Leftrightarrow$$
$$\Leftrightarrow R^A(t_1(x/s)[e], \ldots) \Leftrightarrow R^A(t_1[e(x/s[e])], \ldots) \Leftrightarrow \mathcal{A} \models R(t_1, \ldots)[e(x/s[e])].$$

Indukční krok pro $\neg, \to$ plyne díky tomu, že $(\neg\varphi_0)(x/s)$ je $\neg\varphi_0(x/s)$ a $(\varphi_0 \to \varphi_1)(x/s)$ je $\varphi_0(x/s) \to \varphi_1(x/s)$.

Buď φ tvaru $(\forall y)\psi$ a pro ψ nechť to platí. a) x nemá volný výskyt ve φ. Pak je $\varphi(x/s)$ rovno φ a e, $e(x/s[e])$ se rovnají na všech volných proměnných formule φ a dokazovaná ekvivalence tedy platí. b) x má volný výskyt ve φ. Pak díky substituovatelnosti s za x do φ máme:

b1) y není x, b2) y není v s a tedy $s[e(y/a)] = s[e]$.

$$\begin{array}{llll} \text{Platí } \mathcal{A} \models \varphi(x/s)[e] & \Leftrightarrow & \mathcal{A} \models \psi(x/s)[e(y/a)] & \text{pro každé } a \in A \\ & \Leftrightarrow & \mathcal{A} \models \psi[e(y/a)(x/s[e(y/a)])] & \text{pro každé } a \in A \\ & \Leftrightarrow & \mathcal{A} \models \psi[e(x/s[e])(y/a)] & \text{pro každé } a \in A \\ & \Leftrightarrow & \mathcal{A} \models (\forall y)\psi[e(x/s[e])]. & \end{array}$$

Prvou ekvivalenci dává definice platnosti, druhou indukční předpoklad, třetí záměna pořadí úpravy e a b2), poslední definice platnosti. □

TVRZENÍ 2.2.22. (O korektnosti predikátové logiky.)

1) a) *Každý logický axiom je pravdivý.*

   b) *Když* $\mathcal{A} \models \{\varphi, \varphi \to \psi\}$, *tak* $\mathcal{A} \models \psi$ *a* $\mathcal{A} \models (\forall x)\varphi$.

2) *Pro teorii* T *a její formuli* φ *platí:* $T \vdash \varphi \Rightarrow T \models \varphi$.

Důkaz. 1) Nechť $\mathcal{A}$ je L-struktura. a) Každá L-formule tvaru (PL1) – (PL3) jasně platí v $\mathcal{A}$ výpočtem v $\underline{2}$. Z definice platnosti atomické formule plyne platnost axiomů rovnosti v $\mathcal{A}$. Buď t term substituovatelný do φ za x a e ohodnocení proměnných v A; dokážeme, že platí $\mathcal{A} \models ((\forall x)\varphi \to \varphi(x/t))[e]$. Nechť $\mathcal{A} \models (\forall x)\varphi[e]$. Pak $\mathcal{A} \models \varphi[e(x/t[e])]$ a dle tvrzení 2.2.21 o korektnosti substituce je $\mathcal{A} \models \varphi(x/t)[e]$. Snadno se dokáže také i platnost každého axiomu $\forall$-zavedení, tj. formule $(\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$, není-li proměnná x volná ve φ, užijeme-li toho, že $\mathcal{A} \models \varphi[e]$ nezávisí na $e(x)$, není-li x volná ve φ. b) Evidentně $\mathcal{A} \models \psi$. Protože $\mathcal{A} \models \varphi$ značí, že $\mathcal{A} \models \varphi[e]$ pro každé ohodnocení proměnných v A, jasně $\mathcal{A} \models (\forall x)\varphi$.

2) plyne indukcí na teorémech T bezprostředně užitím 1). □

POZNÁMKA 2.2.23.

1. Nechť T je teorie v jazyce s rovností a $\mathcal{A}$ alespoň dvouprvkový model T. Pak formule φ tvaru $x \neq y$ je nezávislá v T, tj. $T \nvdash \varphi$ a $T \nvdash \neg\varphi$, neboť $\mathcal{A} \not\models \varphi$ a $\mathcal{A} \not\models \neg\varphi$.

2. Formule $\varphi \to (\forall x)\varphi$ není obecně pravdivá, tedy ji nelze vzít za logický axiom. Buď totiž např. φ tvaru $U(x)$, kde U je unární relační symbol. Pak $\langle 2, \{0\}\rangle \not\models \varphi \to (\forall x)\varphi$.

2.3 Vlastnosti struktur a teorií. Charakteristiky teorie.

Všeobecnou úlohou predikátové logiky je získávat poznatky o logickém charakteru dané teorie s ohledem na bezespornost, kompletnost, počet jednoduchých kompletních extenzí, konečnou či otevřenou axiomatizovatelnost atd., na straně modelů pak jde o počet neizomorfních modelů, existenci minimálních modelů apod. V následujícím se budeme věnovat těmto otázkám převážně na straně sémantické, užívajíce sémantických verzí pojmů jako bezespornost, kompletnost, axiomatizovatelnost atd.

Klíčovými pojmy v následujícím jsou:

> Elementární ekvivalence, teorie struktury. Algebry definovatelných množin. Homomorfizmus, vnoření, izomorfizmus. Kategoričnost. Elementární vnoření a podstruktura, modelová kompletnost. Prvomodely. Jednoduché kompletní extenze. Eliminace: eliminační množina, eliminace kvantifikátorů.

Elementární ekvivalence, teorie struktury.

2.3.1. Elementární ekvivalence. Teorie struktury.

1. Dvě L-struktury $\mathcal{A}, \mathcal{B}$ jsou *elementárně ekvivalentní*, platí-li v nich právě tytéž L-formule; píše se pak

$$\mathcal{A} \equiv \mathcal{B}.$$

2. *Teorie L-struktury* $\mathcal{A}$ je množina L-sentencí platných v $\mathcal{A}$; značíme ji $\mathrm{Th}(\mathcal{A})$.

Zřejmě platí:

• $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$, tj. dvě L-struktury jsou elementárně ekvivalentní, právě když v nich platí právě tytéž L-sentence. (Formule totiž platí ve struktuře, právě když v ní platí její generální uzávěr, což je sentence.)

• Teorie $\mathrm{Th}(\mathcal{A})$ struktury $\mathcal{A}$ je kompletní. (Neboť pro sentenci φ je $\mathrm{Th}(\mathcal{A}) \vdash \varphi \Leftrightarrow \mathcal{A} \models \varphi$.)

Poznamenejme dále, že třída $\mathsf{M}(T)$ všech modelů teorie T je uzavřená na elementární ekvivalenci, tj. $\mathcal{A} \equiv \mathcal{B} \in \mathsf{M}(T) \Rightarrow \mathcal{A} \in \mathsf{M}(T)$; uzavřenost na elementární ekvivalenci a ovšem také na izomorfní kopie jsou tedy nutné podmínky na axiomatizovatelnost třídy struktur. Speciálně jednoprvková třída $\{\mathcal{A}\}$ není axiomatizovatelná.

TVRZENÍ 2.3.2. (O teorii kompletní sémanticky.) *Pro teorii T s modelem je ekvivalentní* a) – d)*:*

a) *T je kompletní sémanticky.*
b) *Každé dva modely teorie T jsou elementárně ekvivalentní.*
c) $\mathrm{Tr}(T) = \mathrm{Th}(\mathcal{A})$ *pro každý model* $\mathcal{A} \models T$.
d) $\mathrm{Tr}(T) = \mathrm{Th}(\mathcal{A})$ *pro nějaký model* $\mathcal{A} \models T$.

Důkaz plyne snadno z definic. □

Předešlé tvrzení říká toto: L-teorie T je kompletní sémanticky, právě když má až na elementární ekvivalenci právě jeden model, a to nastává, právě když je T ekvivalentní sémanticky s $\mathrm{Th}(\mathcal{A})$ pro nějakou L-strukturu $\mathcal{A}$.

TVRZENÍ 2.3.3. *Buď L jazyk s rovností.*

1) *Dvě konečné elementárně ekvivalentní L-struktury jsou izomorfní.*

2) *L-teorie kompletní sémanticky a s konečným modelem má každé dva modely izomorfní.*

Důkaz. 1) Buďte $\mathcal{A}, \mathcal{A}'$ konečné a elementárně ekvivalentní L-struktury. Pro nějaké $k \in \mathbb{N}$ je $k = |A| = |A'|$. Dokážeme, že platí:

$$\text{Pro } a \in A \text{ existuje } a' \in A' \text{ tak, že } \langle \mathcal{A}, a\rangle \equiv \langle \mathcal{A}', a'\rangle. \tag{2.5}$$

Pomocí (2.5) snadno sestrojíme prosté posloupnosti $a_0, \dots, a_{k-1}$ v A a $a'_0, \dots, a'_{k-1}$ v A' tak, že $\langle \mathcal{A}, a_i\rangle_{i<l} \equiv \langle \mathcal{A}', a'_i\rangle_{i<l}$ platí pro každé $l \le k$; pro $l = 0$ jde o předpoklad $\mathcal{A} \equiv \mathcal{A}'$. Pak zobrazení $a_i \mapsto a'_i$ s $i < k$ je jasně izomorfizmus $\mathcal{A}$ a $\mathcal{A}'$.

Zbývá dokázat (2.5). Pro $a \in A$ buď p množina všech L-formulí $\varphi(x)$ takových, že $\mathcal{A} \models \varphi[a]$. Označme $D_\varphi = \{a \in A;\ \mathcal{A} \models \varphi[a]\}$; je $D_\varphi \subseteq A$. Protože je A konečná, existuje konečně formulí $\varphi_0, \dots, \varphi_{m-1}$ tak, že pro každé φ z p je D_φ některé D_{φ_i}, $i < m$, tj. $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$. Speciálně platí $\mathcal{A} \models (\exists x) \bigwedge_{i<m} \varphi_i$, díky $\mathcal{A} \equiv \mathcal{A}'$ tedy $\mathcal{A}' \models (\exists x) \bigwedge_{i<m} \varphi_i$; buď a' z A' takové, že $\mathcal{A}' \models \bigwedge_{i<m} \varphi_i[a']$. Zřejmě je a' hledané, tj. $\langle \mathcal{A}, a\rangle \equiv \langle \mathcal{A}', a'\rangle$.

2) Pro modely $\mathcal{A}$, $\mathcal{B}$ uvažované teorie je $\mathcal{A} \equiv \mathcal{B}$ a protože L je s rovností, tak $|A| = |B|$. Dle 1) je tedy $\mathcal{A} \cong \mathcal{B}$. □

Definovatelné množiny.

2.3.4. **Definovatelné množiny. Algebry** $\mathrm{Df}^n(X, \mathcal{A})$.

Buď $\mathcal{A}$ nějaká L-struktura.

1. Buď φ v $\overline{x}, \overline{y}$ a $\overline{b} \in A^{\mathrm{l}(\overline{y})}$. Množina *definovaná z parametrů* $\overline{b}$ formulí $\varphi(\overline{x}, \overline{y})$ v $\mathcal{A}$ je množina

$$\varphi(\overline{x}, \overline{y})(\mathcal{A}, \overline{b}) = \{\overline{a} \in A^{\mathrm{l}(\overline{x})};\ \mathcal{A} \models \varphi[\overline{x}\smile\overline{y}|\overline{a}\smile\overline{b}]\}.$$

Značí se též

$$\varphi(\mathcal{A}^{\mathrm{l}(\overline{x})}, \overline{b}) \quad \text{či} \quad \varphi(\mathcal{A}, \overline{b}).$$

Je-li $\overline{y}$ prázdné, je to množina *definovaná bez parametrů* formulí $\varphi(\overline{x})$ v $\mathcal{A}$. Značí se $\varphi(\overline{x})(\mathcal{A})$, $\varphi(\mathcal{A}^{\mathrm{l}(\overline{x})})$ či jen $\varphi(\mathcal{A})$. Připouštíme $\mathrm{l}(\overline{x}) = 0$; pak je definovaná množina částí $A^0 = \{\emptyset\}$. Pro názornost můžeme psát výše i $\varphi(\overline{x}, \overline{y})$ či $\varphi(\overline{x})$ místo pouhého φ.

2. Buď $X \subseteq A$ a $n \in \mathbb{N}$. Obor všech podmnožin A^n definovatelných L-formulemi tvaru $\varphi(\overline{x}, \overline{y}_\varphi)$ z parametrů z X, kde $\mathrm{l}(\overline{x}) = n$, tj. obor všech množin tvaru $\varphi(\overline{x}, \overline{y}_\varphi)(\mathcal{A}, \overline{b})$ s $\mathrm{l}(\overline{x}) = n$ a $\overline{b} \in X^{\mathrm{l}(\overline{y}_\varphi)}$, značíme

$\mathrm{Df}^n(X, \mathcal{A})$.

Snadno se zjistí, že $\mathrm{Df}^n(X, \mathcal{A})$ je podalgebra potenční algebry $\mathcal{P}(A^n)$ množin. Speciálně máme $\mathrm{Df}^0(X, \mathcal{A}) = \underline{2}$ (když chápeme 0 jako $\emptyset$, 1 jako $\{\emptyset\}$, 2 jako $\{0, 1\} = \{\emptyset, \{\emptyset\}\}$). Operace $\mathrm{Df}^n(X, \mathcal{A})$ jsou dány zřejmě takto:

- komplement do A^n negací definující formule,
- průnik resp. sjednocení konjunkcí resp. disjunkcí definujících formulí,
- $\emptyset = \varphi(\overline{x}, \overline{y})(\mathcal{A}, \overline{b})$ resp. $A^n = \varphi(\overline{x}, \overline{y})(\mathcal{A}, \overline{b})$, kde φ je sentence neplatná resp. platná v $\mathcal{A}$.

2.3.5. Funkce $\curlyvee^A_{n,i}$ existenčního a $\curlywedge^A_{n,i}$ univerzálního zúžení relace.

Pomocí prvé resp. druhé funkce můžeme sestrojit $(\exists x_i)\varphi(\overline{x})(\mathcal{A}^{n-1})$ resp. $(\forall x_i)\varphi(\overline{x})(\mathcal{A}^{n-1})$ z množiny $\varphi(\overline{x})(\mathcal{A}^n)$, kde $n = \mathrm{l}(\overline{x})$. Buď $i < n \in \mathbb{N}$. Pro $(n-1)$-tici $\overline{a}$ a prvek b buď $\overline{a}\langle i, b\rangle$ n-tice, která se získá z $\overline{a}$ vsunutím b na místo i; speciálně je $\overline{a}\langle n-1, b\rangle = \overline{a}\smile b$. Dále např. $\langle a_0, a_1, a_2, a_3\rangle\langle 1, b\rangle = \langle a_0, b, a_1, a_2, a_3\rangle$.

Buď $\curlyvee^A_{n,i}$ resp. $\curlywedge^A_{n,i}$ definováno pro každé $X \subseteq A^n$ vztahem

$$\curlyvee^A_{n,i}(X) = \{\overline{a} \in A^{n-1};\ \text{existuje } b \in A \text{ s } \overline{a}\langle i, b\rangle \in X\}, \quad \curlywedge^A_{n,i}(X) = A^{n-1} - \curlyvee^A_{n,i}(A^n - X).$$

Speciálně je $\curlyvee^A_{n,n-1}(X) = \mathrm{dom}(X)$.

TVRZENÍ 2.3.6. (Elementární vlastnosti definovatelných množin.) *Nechť $\mathcal{A}$ je L-struktura, φ je L-formule v $\overline{x}, \overline{y}$, $n = \mathrm{l}(\overline{x})$ a $\overline{b} \in A^{\mathrm{l}(\overline{y})}$. Pak:*

1) *Když žádné $\overline{x}_i$ nemá volný výskyt ve φ, tak $\varphi(\mathcal{A}^n, \overline{b})$ je $\emptyset$, když $\mathcal{A} \not\models \varphi[\overline{b}]$, a A^n jinak.*

2) *Je-li π permutace n-tice proměnných $\overline{x}$, tak*
$$\varphi(\pi\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b}) = \{\pi\overline{a};\ \overline{a} \in \varphi(\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b})\} = \pi[\varphi(\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b})].$$

3) *Když x_i nemá volný výskyt ve φ a $D = \varphi(\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b})$ je neprázdná, tak $\{\overline{a}_i;\ \overline{a} \in D\} = A$.*

4) $(\exists x_i)\varphi(\overline{x}, \overline{y})(\mathcal{A}^{n-1}, \overline{b}) = \curlyvee^A_{n,i}(\varphi(\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b}))$,
$(\forall x_i)\varphi(\overline{x}, \overline{y})(\mathcal{A}^{n-1}, \overline{b}) = \curlywedge^A_{n,i}(\varphi(\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b}))$.

5) $\mathcal{A} \models (\forall \overline{x})\varphi(\overline{x}, \overline{y})[\overline{b}] \Leftrightarrow \varphi(\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b}) = A^n$,
$\mathcal{A} \models (\exists \overline{x})\varphi(\overline{x}, \overline{y})[\overline{b}] \Leftrightarrow \varphi(\overline{x}, \overline{y})(\mathcal{A}^n, \overline{b}) \neq \emptyset$.

Důkaz. 1) Plyne to z faktu, že $\varphi(\overline{x}, \overline{y})[\overline{a}, \overline{b}]$ nezávisí na $\overline{a}$.

2) je jasné.

3) Platnost $\mathcal{A} \models \varphi[\overline{a}, \overline{b}]$ totiž nezávisí na hodnotě $\overline{a}_i$.

4) První tvrzení plyne ihned z toho, že $\langle a_0, \ldots, a_{n-2}\rangle \in (\exists x_i)\varphi(\overline{x}, \overline{y})(\mathcal{A}^{n-1}, \overline{b})$, právě když existuje $a' \in A$ s $\mathcal{A} \models \varphi(\overline{x}, \overline{y})[\langle a_0, \ldots, a_{i-1}, a', a_i, \ldots, a_{n-2}\rangle, \overline{b}]$. Druhé plyne analogicky nebo jako důsledek vztahu $\exists$ a $\forall$.

5) plyne snadno z definic. $\square$

POZNÁMKA 2.3.7. Když $\mathcal{A} \subseteq \mathcal{B}$, nemusí být $\varphi(\mathcal{A}) = \varphi(\mathcal{B}) \cap A$. Nechť např. $\varphi(x)$ je formule $(\exists y)(y \cdot y = 1 + 1)$. Pak $\varphi(\underline{\mathbb{R}}) = \mathbb{R}$, $\varphi(\underline{\mathbb{Q}}) = \emptyset$, kde $\underline{\mathbb{R}}$ resp. $\underline{\mathbb{Q}}$ je těleso reálných resp. racionálních čísel.

PŘÍKLADY 2.3.8. 1. Buď $\mathcal{A} = \langle \mathbb{N}, \mathrm{S}, <\rangle$, kde $\mathrm{S}(n) = n + 1$. Buď φ formule $(\exists y)(\mathrm{S}y < x)$, x, y, z různé proměnné. Označme $D = \mathbb{N} - \{0, 1\}$. Pak:

$$\varphi(x)(\mathcal{A}) = D, \quad \varphi(x, y)(\mathcal{A}) = D \times \mathbb{N}, \quad \varphi(y, x)(\mathcal{A}) = \mathbb{N} \times D, \quad \varphi(z, x, y)(\mathcal{A}) = \mathbb{N} \times D \times \mathbb{N}.$$

2. Buď $t(x, \overline{y})$ term jazyka okruhů $\langle +, -, \cdot, 0, 1\rangle$. Nechť $\mathcal{A}$ je těleso reálných nebo komplexních čísel, $\overline{b} \in A^{\mathrm{l}(\overline{b})}$. Pak $D = (t(x, \overline{y}) = 0)(\mathcal{A}, \overline{b})$ je množina všech řešení rovnice $t(x, \overline{b}) = 0$ v tělese $\mathcal{A}$. Term $t(x, \overline{b})$ se v $\mathcal{A}$ (přesněji v $\mathcal{A}_A$) rovná termu tvaru polynomu v jedné neurčité, tudíž D je konečné nebo $D = A$.

Homomorfizmy, vnoření, izomorfizmy.

Homomorfizmus L-struktury $\mathcal{A}$ do L-struktury $\mathcal{B}$ je zobrazení $h : A \to B$, respektující v té či oné míře relace a funkce struktur; mluvíme pak o epimorfizmu, vnoření, izomorfizmu atd. Homomorfizmy umožňují porovnávat struktury a na základě toho analyzovat obor modelů dané teorie co do izomorfnosti, existence minimálních vnořitelných modelů apod. Dále homomorfizmus dovoluje konstruovat pomocí kongruence indukované na $\mathcal{A}$ příslušnou faktorstrukturu; toho využijeme ke konstrukci Booleových algeber formulí.

2.3.9. **Homomorfizmus, vnoření. Izomorfizmus.**

Buďte $\mathcal{A}$, $\mathcal{B}$ dvě L-struktury.

1. Funkce $h : A \to B$ je *homomorfizmus* $\mathcal{A}$ do $\mathcal{B}$, píšeme $h : \mathcal{A} \to \mathcal{B}$, platí-li:

(h1) Když P je n-ární relační symbol signatury L a $\overline{a} \in A^n$, tak $P^A(\overline{a}) \Rightarrow P^B(h\overline{a})$.

(h2) Když F je n-ární funkční symbol signatury L a $\overline{a} \in A^n$, tak $h(F^A(\overline{a})) = F^B(h\overline{a})$.

Speciálně: je-li P nulární relační symbol, (h1) dává $P^A \subseteq P^B$ a je-li c konstantní symbol, (h2) dává $h(c^A) = c^B$.

Je-li v (h1) $\Leftrightarrow$ místo $\Rightarrow$, říkáme, že h je *striktní homomorfizmus* $\mathcal{A}$ do $\mathcal{B}$ a pokud je navíc prostý, je to *izomorfní vnoření*, krátce *vnoření*, $\mathcal{A}$ do $\mathcal{B}$; je-li navíc na B, je to *izomorfizmus $\mathcal{A}$ a $\mathcal{B}$ (via h)* píšeme

$$\mathcal{A} \cong \mathcal{B} \text{ (via } h).$$

Prostý (čili *injektivní*) homomorfizmus se nazývá *monomorfizmus*. Homomorfizmus na je *epimorfizmus*.

Zřejmě je $\mathcal{A} \subseteq \mathcal{B}$, právě když identita na A je izomorfní vnoření $\mathcal{A}$ do $\mathcal{B}$. Dále pro struktury $\mathcal{A}$, $\mathcal{B}$ téže signatury je zřejmě zobrazení $h : A \to B$ homomorfizmus [izomorfní vnoření] $\mathcal{A}$ do $\mathcal{B}$, právě když je h homomorfizmus [izomorfizmus] $\mathcal{A}$ na podstrukturu $\mathcal{B}\restriction h[A]$.

Pro homomorfizmus $h : \mathcal{A} \to \mathcal{B}$ označme strukturu $\mathcal{B}\restriction h[A]$ jako

$$h[\mathcal{A}]$$

a říkejme, že to je *homomorfní obraz struktury $\mathcal{A}$ via h*.

2. *Automorfizmus* $\mathcal{A}$ je izomorfizmus $\mathcal{A}$ a $\mathcal{A}$; $\mathsf{Aut}(\mathcal{A})$ značí množinu všech automorfizmů struktury $\mathcal{A}$. Struktura $\mathcal{A}$ je *strnulá*, existuje-li na ní jediný automorfizmus (totiž Id_A), čili $\mathsf{Aut}(\mathcal{A}) = \{\mathrm{Id}_A\}$. $\langle \mathsf{Aut}(\mathcal{A}), {}^{-1}, \cdot, \mathrm{Id}_A\rangle$ je *grupa automorfizmů* struktury $\mathcal{A}$; značí se $\underline{\mathsf{Aut}}(\mathcal{A})$, stručněji jen $\mathsf{Aut}(\mathcal{A})$.

PŘÍKLADY 2.3.10.

1. Nechť $\underline{\mathbb{R}}^n$ značí vektorový prostor n-tic reálných čísel nad tělesem $\underline{\mathbb{R}}$ reálných čísel.

a) Buď $h : \mathbb{R}^2 \to \mathbb{R}$ zobrazení, kde $h(\langle a, b\rangle) = b$. Pak h je homomorfizmus $\underline{\mathbb{R}}^2$ na $\underline{\mathbb{R}}^1$.

b) Buď $h : \mathbb{R}^1 \to \mathbb{R}^2$ zobrazení, kde $h(a) = \langle 0, a\rangle$. Pak h je izomorfní vnoření $\underline{\mathbb{R}}^1$ do $\underline{\mathbb{R}}^2$ na podstrukturu $\underline{R}^2\restriction(\{0\} \times \mathbb{R})$.

c) Buď $h : \mathbb{R}^1 \to \mathbb{R}^2$, kde $h(a) = \langle 1, a\rangle$. Pak h není homomorfizmus $\underline{\mathbb{R}}^1$ do $\underline{\mathbb{R}}^2$.

2. a) Buď $i \in X$ a $h : \mathcal{P}(I) \to 2$ zobrazení, kde $h(u) = 1 \Leftrightarrow i \in u$ pro $u \subseteq X$. Pak h je homomorfizmus potenční algebry $\underline{\mathcal{P}(X)}$ na algebru $\underline{2}$.

b) Buď X nekonečná množina. Pak zobrazení $h : \mathrm{FA}(X) \to 2$, kde $h(u) = 1 \Leftrightarrow u$ je nekonečná, je homomorfizmus algebry $\overline{\mathrm{FA}(X)}$ na $\underline{2}$.

3. Je-li $\langle \mathbb{Q}, \leq\rangle$ resp. $\langle \mathbb{R}, \leq\rangle$ obvyklé uspořádání racionálních resp. reálných čísel, tak

$$\langle \mathbb{Q}, \leq\rangle \cong \langle \mathbb{Q} - \{0\}, \leq\rangle, \quad \langle \mathbb{R}, \leq\rangle \ncong \langle \mathbb{R} - \{0\}, \leq\rangle.$$

4. a) Existuje jediný automorfizmus oboru integrity $\mathcal{A} = \langle \mathbb{Z}, +, -, \cdot, 0, 1\rangle$ celých čísel.

b) Buď $\mathcal{B} = \langle \mathbb{Z}, \leq\rangle$ obvyklé uspořádání celých čísel. Pak $\mathcal{B}$ má právě spočetně mnoho automorfizmů. Zobrazení $h : \mathbb{Z} \to \mathbb{Z}$ je totiž zřejmě automorfizmem $\mathcal{B}$, právě když existuje $n \in \mathbb{Z}$ tak, že $h(i) = i + n$ pro každé $i \in \mathbb{Z}$.

c) Buď $\mathcal{B}' = \langle \mathbb{Q}, \leq\rangle$ obvyklé uspořádání racionálních čísel. Pak $\mathcal{B}'$ má právě kontinuum automorfizmů. (Pro $X \subseteq \mathbb{Z}$ buď $h_X : \mathbb{Q} \to \mathbb{Q}$ identita na $\mathbb{Z} \cup \bigcup\{[d, d+1];\ d \in X\}$ a na $(d, d+1)$ neidentický automorfizmus $(d, d+1)$ pro každé $d \in \mathbb{Z} - X$; h_X je automorfizmus $\mathcal{B}'$. Zřejmě $X \neq Y \subseteq \mathbb{Z} \Rightarrow h_X \neq h_Y$ a podmnožin $\mathbb{Z}$ je kontinuum.)

TVRZENÍ 2.3.11. (O homomorfizmu struktur.) *Nechť $\mathcal{A}$, $\mathcal{B}$ jsou L-struktury. Zobrazení $h : A \to B$ je homomorfizmus resp. striktní homomorfizmus $\mathcal{A}$ do $\mathcal{B}$, právě když platí* a) *a* b)*:*

a) $h(t^A[e]) = t^B[he]$ *pro každý L-term t a ohodnocení* $e \in {}^{\mathrm{Var}}A$.

b) $\mathcal{A} \models \varphi[e] \Rightarrow \mathcal{B} \models \varphi[he]$ *resp.* $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{B} \models \varphi[he]$ *pro každou atomickou L-formuli φ a ohodnocení* $e \in {}^{\mathrm{Var}}A$.

Důkaz. Implikace $\Rightarrow$. a) Indukcí na L-termech. Je-li t proměnná x, máme $h(t^A[e]) = h(e(x)) = he(x) = t^B[he]$. Je-li t tvaru $F(t_0, \ldots, t_{n-1})$ s n-árním funkčním symbolem F a termy $t_0, \ldots, t_{n-1}$, pro které to platí, tak

$$\begin{aligned} h(t^A[e]) &= h(F^A(t_0^A[e], \ldots, t_{n-1}^A[e])) = F^B(h(t_0^A[e]), \ldots, h(t_{n-1}^A[e])) \\ &= F^B(t_0^B[he], \ldots, t_{n-1}^B[he]) = t^B[he]. \end{aligned}$$

Druhá rovnost plyne z toho, že h je homomorfizmus, třetí z indukčního předpokladu a čtvrtá z definice hodnoty termu. b) plyne ihned z a) a definic.

Implikace $\Leftarrow$. Vztah $h(F^A(a_0, \ldots, a_{n-1})) = F^B(h(a_0), \ldots, h(a_{n-1}))$ pro n-ární funkční symbol F a $a_0, \ldots, a_{n-1}$ z A plyne volbou $t(x_0, \ldots, x_{n-1})$ tvaru $F(x_0, \ldots, x_{n-1})$ a $e(x_i) = a_i$ pro $i < n$ v a). Vztah $R^A(a_0, \ldots, a_{n-1}) \Rightarrow R^B(h(a_0), \ldots, h(a_{n-1}))$ pro n-ární relační symbol R a prvky $a_0, \ldots, a_{n-1}$ z A plyne volbou $\varphi(x_0, \ldots, x_{n-1})$ tvaru $R(x_0, \ldots, x_{n-1})$ a $e(x_i) = a_i$ s $i < n$ v b); podobně pro $R^A(a_0, \ldots, a_{n-1}) \Leftrightarrow R^B(h(a_0), \ldots, h(a_{n-1}))$. □

TVRZENÍ 2.3.12. (O izomorfizmu struktur.) *Nechť $\mathcal{A}$, $\mathcal{B}$ jsou L-struktury. Prosté zobrazení h množiny A na B je izomorfizmus $\mathcal{A}$ a $\mathcal{B}$, právě když platí* a) *a* b)*:*

a) $h(t^A[e]) = t^B[he]$ *pro každý L-term t a ohodnocení* $e \in {}^{\mathrm{Var}}A$.

b) $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{B} \models \varphi[he]$ *pro každou L-formuli φ a ohodnocení* $e \in {}^{\mathrm{Var}}A$.

Důsledek: izomorfní struktury jsou elementárně ekvivalentní.

Důkaz. Implikace $\Rightarrow$. a) a b) s φ atomickou plyne z tvrzení o homomorfizmu struktur. b) pro libovolné φ plyne indukcí na formulích. Indukční krok pro $\neg$, $\to$ je patrný. Buď konečně φ tvaru $(\forall y)\psi$ a nechť pro ψ to platí. Pak

$$\begin{aligned} \mathcal{A} \models \varphi[e] \quad &\Leftrightarrow \quad \mathcal{A} \models \psi[e(y/a)] \text{ pro každé } a \in A \quad &&\Leftrightarrow \quad \mathcal{B} \models \psi[he(y/h(a))] \text{ pro každé } a \in A \\ &\Leftrightarrow \quad \mathcal{B} \models \psi[he(y/b)] \text{ pro každé } b \in B \quad &&\Leftrightarrow \quad \mathcal{B} \models (\forall y)\psi[he]. \end{aligned}$$

Druhý vztah $\Leftrightarrow$ plyne díky indukčnímu předpokladu, třetí z toho, že h je na B.

Implikace $\Leftarrow$ plyne ihned z 2.3.11 a díky tomu, že h je prosté a na B. □

TVRZENÍ 2.3.13. (O automorfním obrazu definovatelné množiny.) *Buď $X \subseteq A^n$ definovatelná v $\mathcal{A}$ z parametrů $\bar{b}$ a h buď automorfizmus $\mathcal{A}$ identický na $\bar{b}$. Pak je $h[X] = X$.*

Důkaz. Pro $X = \varphi(\mathcal{A}, \bar{b})$ je $\bar{a} \in X \Leftrightarrow \mathcal{A} \models \varphi[\bar{a}, \bar{b}] \Leftrightarrow \mathcal{A} \models \varphi[h\bar{a}, h\bar{b}] \Leftrightarrow \mathcal{A} \models \varphi[h\bar{a}, \bar{b}] \Leftrightarrow h\bar{a} \in X$. □

Pojem kategoričnosti.

2.3.14. Pojem kategoričnosti. Izomorfní spektrum.

Teorie je *κ-kategorická*, čili *kategorická v kardinalitě κ*, má-li až na izomorfizmus jediný model kardinality κ. Pro teorii T definujeme její *izomorfní spektrum* $\mathrm{I}(\kappa, T)$:

$$\mathrm{I}(\kappa, T) = \text{počet neizomorfních modelů z } \mathsf{M}_\kappa(T).$$

Je-li T prázdná L-teorie, místo $\mathrm{I}(\kappa, T)$ píšeme $\mathrm{I}(\kappa, L)$; je to počet neizomorfních modelů jazyka L, které mají kardinalitu κ. Definici $\mathrm{I}(\kappa, T)$ lze formálněji vyjádřit jako kardinalitu množiny $\mathsf{M}(\kappa, T)/\cong$, kde $\mathsf{M}(\kappa, T)/\cong$ je množina všech tříd ekvivalence $\cong$ na $\mathsf{M}(\kappa, T)$.

PŘÍKLADY 2.3.15. (V logice s rovností.)

$L=\langle U\rangle$, U je unární relační symbol.			
$\lvert \mathsf{M}(\kappa, L)\rvert$	$=$	2^κ	pro $\kappa > 0$
$\mathrm{I}(\kappa, L)$	$=$	$\kappa(\leq)$	pro $\kappa > 0$
$L=\langle R\rangle$, R je binární relační symbol.			
$\lvert \mathsf{M}(\kappa, L)\rvert$	$=$	2^κ	pro $\kappa \geq \omega$
$\mathrm{I}(\kappa, L)$	$=$	2^κ	pro $\kappa \geq \omega$
$L=\langle c_i\rangle_{i\in n}$, c_i jsou konstantní symboly, $0 < n < \omega$.			
$\lvert \mathsf{M}(\kappa, L)\rvert$	$=$	κ^n	pro $\kappa < \omega$
		κ	pro $\kappa \geq \omega$
$\mathrm{I}(\kappa, L)$	$=$	$B(n)$	$\kappa \geq \omega$
Poznámka. $B(n)$ je n-té Bellovo číslo, udávající počet rozkladů n.			
$L=\langle c_i\rangle_{i\in n}$, c_i jsou konstantní symboly, $0 < n < \omega$. $T = \{c_i \neq c_j,\ i \neq j \text{ a } i, j \in n\}$; teorie n různých konstant.			
$\lvert \mathsf{M}(\kappa, T)\rvert$	$=$	$\binom{\kappa}{n} n!$	pro $n \leq \kappa < \omega$
		κ	pro $\kappa \geq \omega$
$\mathrm{I}(\kappa, T)$	$=$	1	pro $n \leq \kappa$
Poznámka. $\binom{\kappa}{n} n!$ je počet prostých n-tic v κ.			
$L=\langle\leq\rangle$, $\leq$ je binární relační symbol. T je teorie LO lineárního uspořádání (v L).			
$\lvert \mathsf{M}(\kappa, T)\rvert$	$=$	$\kappa!$	pro $\kappa < \omega$
		2^κ	pro $\kappa \geq \omega$.
$\mathrm{I}(\kappa, T)$	$=$	1	pro $\kappa < \omega$
		2^κ	pro $\kappa \geq \omega$
$L=\langle\leq\rangle$, $\leq$ je binární relační symbol. T je teorie DeLO hustého lineárního uspořádání bez konců (v L).			
$\mathrm{I}(\kappa, T)$	$=$	1	pro $\kappa = \omega$
		2^κ	pro $\kappa > \omega$

Elementární vnoření, elementární podstruktura. Modelová kompletnost.

2.3.16. Elementární vnoření a elementární podstruktura.

Buďte $\mathcal{A}, \mathcal{B}$ dvě L-struktury.

1. Zobrazení $h : A \to B$ se nazývá *elementární vnoření* $\mathcal{A}$ do $\mathcal{B}$, je-li prosté a pro každou L-formuli $\varphi(\overline{x})$ a $\overline{a} \in A^{\mathrm{l}(\overline{x})}$ platí

$$\mathcal{A} \models \varphi[\overline{a}] \quad \Leftrightarrow \quad \mathcal{B} \models \varphi[h\overline{a}]. \tag{2.6}$$

2. $\mathcal{A}$ je *elementární podstruktura* $\mathcal{B}$, je-li Id_A elementární vnoření $\mathcal{A}$ do $\mathcal{B}$; píšeme

$$\mathcal{A} \prec \mathcal{B}.$$

To zřejmě platí, právě když $\mathcal{A} \subseteq \mathcal{B}$ a $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}]$, jakmile $\varphi(\overline{x})$ je L-formule a $\overline{a} \in A^{\mathrm{l}(\overline{x})}$.

POZNÁMKA 2.3.17. Snadno se zjistí, že jsou-li $\mathcal{A}, \mathcal{B}$ nějaké L-struktury, tak platí:

1. a) Když existuje elementární vnoření $\mathcal{A}$ do $\mathcal{B}$, tak $\mathcal{A} \equiv \mathcal{B}$.
   b) Elementární vnoření je izomorfní vnoření. Izomorfizmus $\mathcal{A}$ a $\mathcal{B}$ je právě elementární vnoření $\mathcal{A}$ na $\mathcal{B}$.
   c) Zobrazení $h : A \to B$ je elementární vnoření $\mathcal{A}$ do $\mathcal{B} \Leftrightarrow h$ je izomorfizmus struktury $\mathcal{A}$ a nějaké elementární podstruktury struktury $\mathcal{B}$.
2. a) Když $\mathcal{A}_i \prec \mathcal{B}$ s $i = 0, 1$ a $\mathcal{A}_0 \subseteq \mathcal{A}_1$, tak $\mathcal{A}_0 \prec \mathcal{A}_1$.
   b) Relace $\prec$ je částečné uspořádání na L-strukturách.

PŘÍKLADY 2.3.18.

1. Buď $\mathcal{A}$ resp. $\mathcal{B}$ těleso racionálních resp. reálných čísel. Pak $\mathcal{A} \subseteq \mathcal{B}$, avšak $\mathcal{A} \not\prec \mathcal{B}$, neboť $\mathcal{A} \not\equiv \mathcal{B}$ díky tomu, že $(\exists x)(x \cdot x = 1 + 1)$ platí v $\mathcal{B}$, nikoli však v $\mathcal{A}$.

2. Buď $\mathcal{B} = \langle \mathbb{Z}, \leq \rangle$, kde $\leq$ je obvyklé uspořádání celých čísel, $\emptyset \neq A \subseteq \mathbb{Z}$, $\mathcal{A} = \mathcal{B} \restriction A$. Pak
$$\mathcal{A} \prec \mathcal{B} \Leftrightarrow A = \mathbb{Z}.$$
Důkaz. Stačí dokázat, že když je nějaké $b \in \mathbb{Z} - A$, tak $\mathcal{A} \not\prec \mathcal{B}$. To platí, neboť když a_0 resp. a_1 je nejbližší menší resp. větší prvek k b, patřící A, tak v $\mathcal{B}$ platí „existuje prvek ostře mezi a_0, a_1", tj. $\mathcal{B} \models \varphi[a_0, a_1]$, kde $\varphi(x_0, x_1)$ je formule $(\exists y)(x_0 \leq y \leq x_1 \;\&\; x_0 \neq y \neq x_1)$, avšak $\mathcal{A} \not\models \varphi[a_0, a_1]$. □

3. Buď $\mathcal{B} = \langle \mathbb{Q}, \leq \rangle$, kde $\leq$ je obvyklé uspořádání racionálních čísel, $\emptyset \neq A \subseteq \mathbb{Q}$, $\mathcal{A} = \mathcal{B} \restriction A$. Pak
$$\mathcal{A} \prec \mathcal{B} \Leftrightarrow \mathcal{A} \models \text{DeLO}.$$
Důkaz. a) Má-li A některý konec, jasně $\mathcal{A} \not\equiv \mathcal{B}$, tím spíše $\mathcal{A} \not\prec \mathcal{B}$. Pokud neplatí axiom hustoty v $\mathcal{A}$, existují dva prvky $a < b$ z A, mezi kterými není prvek z A, je však nějaký prvek z B; tedy $\mathcal{A} \not\prec \mathcal{B}$. b) Buď $\mathcal{A} \models$ DeLO. Nechť $\varphi(\overline{x})$ je nějaká $L(\mathcal{B})$-formule s $\mathrm{l}(\overline{x}) = n$, $\overline{a} \in A^n$; máme dokázat, že $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}]$. Díky předpokladům existuje jasně izomorfizmus h struktur $\mathcal{A}$ a $\mathcal{B}$, identický na prvcích z $\overline{a}$; pak tedy $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[h\overline{a}]$ a $h\overline{a} = \overline{a}$. □

TVRZENÍ 2.3.19. *Buďte $\mathcal{A} \subseteq \mathcal{B}$ dvě L-struktury. Pak je ekvivalentní* 1) a 2)*:*

1) $\mathcal{A} \prec \mathcal{B}$.
2) (Tarski-Vaughtův test.) *Pro každou L-formuli $\varphi(\overline{x})$ a $\overline{a}$ z $A^{\mathrm{l}(\overline{x})}$ platí:*
$$\mathcal{B} \models (\exists y)\varphi[\overline{a}] \Rightarrow \textit{existuje } d \in A \textit{ tak, že } \mathcal{B} \models \varphi[\overline{a}(y/d)]. \tag{2.7}$$

Důkaz. 1) $\Rightarrow$ 2) je jasné. Dokážeme obrácenou implikaci. Indukcí podle složitosti $\varphi(\overline{x})$ dokážeme: pro $\overline{a} \in A^{\mathrm{l}(\overline{x})}$ platí $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}]$. Indukční krok pro φ atomickou a logické spojky $\neg, \to$ je jasný. Buď $\varphi(\overline{x})$ tvaru $(\forall y)\psi(\overline{x})$, pro ψ nechť dokazované platí, a nechť $\overline{a} \in A^{\mathrm{l}(\overline{x})}$. Stačí dokázat $\mathcal{A} \models \varphi[\overline{a}] \Rightarrow \mathcal{B} \models \varphi[\overline{a}]$, neboť opačná implikace je jasná. Z $\mathcal{A} \models (\forall y)\psi[\overline{a}]$ plyne užitím indukčního předpokladu: $\mathcal{B} \models \psi[\overline{a}(y/d)]$ pro každé $d \in A$. Odtud užitím (2.7) (volíme-li tamější φ jako $\neg\psi$) plyne $\mathcal{B} \models (\forall y)\psi[\overline{a}]$, tj. $\mathcal{B} \models \varphi[\overline{a}]$. □

VĚTA 2.3.20. (Löwenheim-Skolemova dolů.) *Buď L jazyk s rovností, $\mathcal{A}$ nekonečná L-struktura. Pak pro každý kardinál κ s $\|L\| \leq \kappa \leq \|\mathcal{A}\|$ a každou množinu $X \subseteq A$ velikosti nejvýše κ existuje elementární podstruktura $\mathcal{B}$ struktury $\mathcal{A}$ velikosti κ taková, že $X \subseteq B$.*

Důkaz. Lze předpokládat $|X| = \kappa$. Ke každé formuli $\varphi(x, x_1, \ldots, x_n)$ a posloupnosti $a_1, \ldots, a_n$ v X vybereme $a \in A$ tak, že $\mathcal{A} \models (\exists x)\varphi[a_1, \ldots, a_n] \to \varphi[a, a_1, \ldots, a_n]$; nechť X' je množina všech takových a. Zřejmě $X' \supseteq X$ a $|X'| = \kappa$. Buď $X_0 = X'$ a $X_{i+1} = X_i'$; položme $B = \bigcup_i X_i$. Pak $|B| = \kappa$ a B je uzavřeno na všechny funkce struktury $\mathcal{A}$ (a speciálně obsahuje všechny její konstanty); buď $\mathcal{B}$ podstruktura $\mathcal{A}$ s univerzem B. Ukážeme, že $\mathcal{B} \prec \mathcal{A}$. Dle Tarski-Vaughtova testu stačí ukázat, že pro L-formuli $\varphi(x, x_1, \ldots, x_n)$ a n-tici $b_1, \ldots, b_n$ v B plyne z $\mathcal{A} \models (\exists x)\varphi[b_1, \ldots, b_n]$ existence prvku $b \in B$ tak, že $\mathcal{A} \models \varphi[b, b_1, \ldots, b_n]$. Jsou-li $b_1, \ldots, b_n$ v X_i, je hledaný prvek díky provedené konstrukci jistě v X_{i+1} a tedy v B. □

2.3.21. **Modelová kompletnost teorie.**

Teorie T je *modelově kompletní*, jestliže po každé její dva modely $\mathcal{A}$, $\mathcal{B}$ platí:
$$\mathcal{A} \subseteq \mathcal{B} \quad\Rightarrow\quad \mathcal{A} \prec \mathcal{B}. \tag{2.8}$$

PŘÍKLADY 2.3.22. 1. Buď $\mathcal{B} = \langle \mathbb{Z}, \leq \rangle$, $\mathcal{A} = \langle \mathbb{Z} - \{1\}, \leq \rangle$ (kde $\leq$ je obvyklé uspořádání $\mathbb{Z}$). Pak:
a) $\mathcal{A} \equiv \mathcal{B}$ (neboť $\mathcal{A} \cong \mathcal{B}$), $\mathcal{A} \subseteq \mathcal{B}$, $\mathcal{A} \not\prec \mathcal{B}$.
b) Teorie $T = \mathrm{Th}(\mathcal{A})$ je kompletní, není však modelově kompletní; o tom svědčí její modely $\mathcal{A}$, $\mathcal{B}$.

2. Teorie ACF algebraicky uzavřených těles není kompletní, je však modelově kompletní.

Prvomodely.

2.3.23. Algebraický prvomodel a prvomodel.
Model teorie T je její *algebraický prvomodel* resp. *prvomodel*, lze-li jej vnořit resp. elementárně vnořit do každého modelu teorie T.

TVRZENÍ 2.3.24.
Má-li teorie T [algebraický] prvomodel $\mathcal{A}$, pro [bezkvantifikátorovou]$L(T)$-sentenci φ platí

$$T \models \varphi \Leftrightarrow \mathcal{A} \models \varphi.$$

Speciálně: Má-li teorie prvomodel, je kompletní sémanticky.

Důkaz. Buď $\mathcal{B} \models T$. Pak $\mathcal{A}$ je až na izomorfizmus [podstruktura] elementární podstruktura $\mathcal{B}$, tedy $\mathcal{B} \models \varphi \Leftrightarrow \mathcal{A} \models \varphi$. □

TVRZENÍ 2.3.25. *Nechť teorie T je modelově kompletní a má algebraický prvomodel. Pak je kompletní sémanticky a její algebraický prvomodel je její prvomodel.*

Důkaz. Pro modely $\mathcal{A}$ teorie T a její algebraický prvomodel $\mathcal{B}$ je, až na izomorfizmus, $\mathcal{B}$ podmodel $\mathcal{A}$, tedy díky modelové kompletnosti je $\mathcal{B} \prec \mathcal{A}$. Tudíž je $\mathcal{B}$ prvomodel teorie T a dle 2.3.24 je T kompletní. □

TVRZENÍ 2.3.26. (ω-kategorické kriterium kompletnosti sémanticky.) *Nechť T je teorie ve spočetném jazyce, která má jen nekonečné modely a je ω-kategorická. Pak má T prvomodel a je tedy i kompletní sémanticky.*

Důkaz. Buď $\mathcal{A}$ model T; je nekonečný. Podle Löwenheim-Skolemovy věty dolů existuje spočetný elementární podmodel $\mathcal{B}$ modelu $\mathcal{A}$. $\mathcal{B}$ je až na izomorfizmus jediný díky ω-kategoričnosti a je to tedy prvomodel uvažované teorie. □

PŘÍKLADY 2.3.27. 1. Teorie DeLO hustého lineárního uspořádání bez konců je ω-kategorická teorie ve spočetném jazyce a s jen nekonečnými modely; tedy je kompletní sémanticky.

2. Teorie PE čisté rovnosti je ω-kategorická teorie ve spočetném jazyce, není však kompletní sémanticky.

3. Buď T teorie netriviálních (tj. s axiomem $(\exists x, y)(x \neq y)$) vektorových prostorů nad nejvýše spočetným tělesem F. Pak je to ω-kategorická teorie ve spočetném jazyce. T je kompletní sémanticky, právě když F je nekonečné. Neboť jen pro F nekonečné má T jen nekonečné modely.

Jednoduché kompletní extenze.

Důležitou charakteristikou dané teorie T je, jak vypadají její modely až na elementární ekvivalenci. Protože $\mathcal{A} \models T$ představuje jakožto $\mathrm{Th}(\mathcal{A})$ jednoduchou kompletní extenzi T sémanticky, jde o otázku, jak vypadají takové extenze až na ekvivalenci teorií sémanticky.

ÚMLUVA. Frázi „jednoduchá kompletní extenze“ včetně mluvnických tvarů budeme zapisovat stručně jako

JKE.

JKE sémanticky pak znamená tento pojem v sémantické verzi.

Poznamenejme, že platí následující významné tvrzení: Je-li teorie T v rekurzivním jazyce a nějaký seznam všech jejich JKE je rekurzivní, je T rozhodnutelná, tj. množina všech teorémů T je rekurzivní.

2.3.28. Komplet modelů teorie a komplet teorie.

Buď T nějaká L-teorie s modelem.

1. *Komplet modelů teorie* T je množina K modelů teorie T taková, že pro každý model $\mathcal{A} \models T$ existuje v K právě jeden model elementárně ekvivalentní s $\mathcal{A}$.

2. *Komplet teorie* T je množina $\mathcal{K}$ nějakých JKE teorií T taková, že každá JKE teorie T je ekvivalentní s právě jednou teorií z $\mathcal{K}$.

Nahradíme-li každý pojem v uvedené definici jeho sémantickou verzí, získáme definici *kompletu T sémanticky.*

Symbol $\mathrm{Kn}(T)$ nechť značí *počet neekvivalentních* JKE *teorie T sémanticky.*

Zřejmě platí:
- Je-li K komplet modelů T, tak $\{\mathrm{Th}(\mathcal{A});\ \mathcal{A} \in \mathsf{K}\}$ je komplet teorie T a $|\mathsf{K}| = |\mathcal{K}| = \mathrm{Kn}(T)$.
- Je-li $\mathcal{K}$ komplet teorie T a $\mathsf{K} = \{\mathcal{A}_S;\ S \in \mathcal{K}\}$, kde $\mathcal{A}_S \models S$, tak K je komplet modelů teorie T.

Poznamenejme, že $\mathrm{Kn}(T)$ je počet ultrafiltrů v Lindenbaumově algebře B^0T.

PŘÍKLADY.

1. $\{\langle n\rangle;\ 0 < n \in \mathbb{N}\} \cup \{\langle\mathbb{N}\rangle\}$ je komplet modelů teorie PE čisté rovnosti. ($\langle\mathbb{N}\rangle \equiv \langle A\rangle$ pro A nekonečnou plyne např. užitím Tarski-Vaughtova testu.)

2. $\mathrm{Kn}(\mathrm{DeLO}^*) = 4$.

$\{\mathrm{DeLO}, \mathrm{DeLO}^-, \mathrm{DeLO}^+, \mathrm{DeLO}^\pm\}$ je komplet teorie DeLO^* sémanticky. (DeLO je ve spočetném jazyce, ω-kategorická a má jen nekonečné modely, tedy dle ω-kategorického kriteria kompletnosti je DeLO kompletní sémanticky. Podobně pro další tři teorie.)

$\{(0,1)_\mathbb{Q}, [0,1)_\mathbb{Q}, (0,1]_\mathbb{Q}, [0,1]_\mathbb{Q}\}$ (intervaly racionálních čísel) je komplet modelů teorie DeLO^*.

Eliminace.

Problematika eliminace se zabývá v podstatě otázkou, zda pro danou teorii T a množinu Φ jejích formulí platí, že ke každé $L(T)$-formuli φ existuje $\varphi^* \in \Phi$ s $T \vdash \varphi \leftrightarrow \varphi^*$. Je-li Φ množina otevřených čili bezkvantifikátorových formulí, mluvíme o eliminaci kvantifikátorů teorie T. Sémantickou verzi problematiky získáme nahrazením $\vdash$ symbolem $\models$. Důsledkem eliminace kvantifikátorů teorie T je, že definovatelné množiny v modelech teorie T jsou deskriptivně jednoduché, totiž definovatelné otevřenými formulemi.

Eliminaci kvantifikátorů má např. teorie DeLO hustého lineárního uspořádání bez konců a také teorie ACF algebraicky uzavřených těles; prvá teorie je kompletní, druhá nikoli. Naopak eliminaci kvantifikátorů nemá teorie DiLO diskrétního lineárního uspořádání, ani teorie PE čisté rovnosti.

2.3.29. Eliminační množina formulí. Eliminace kvantifikátorů.

1. Nejmenší množina formulí obsahující danou množinu Γ formulí a uzavřená na $\neg$, $\&$, $\vee$ se značí $\mathrm{b}(\Gamma)$; její prvky se nazývají *booleovské kombinace* formulí z Γ. Snadno se dokáže, že každá otevřená formule je ekvivalentní sémanticky booleovské kombinaci atomických formulí.

2. Buď Γ množina L-formulí a T teorie v L. Množina Γ je *eliminační pro teorii T [sémanticky]*, jestliže ke každé L-formuli $\varphi(\overline{x})$ s $\mathrm{l}(\overline{x}) > 0$ existuje booleovská kombinace $\psi(\overline{x})$ formulí z Γ tak, že

$$T \vdash \varphi(\overline{x}) \leftrightarrow \psi(\overline{x}) \quad [T \models \varphi(\overline{x}) \leftrightarrow \psi(\overline{x})].$$

Je-li Γ množina všech atomických formulí, říkáme, že T *má eliminaci kvantifikátorů [sémanticky].*

POZNÁMKA 2.3.30. Je-li Γ eliminační sémanticky pro L-teorii T a φ je L-sentence, existuje booleovská kombinace $\psi(x_0)$ formulí z Γ tak, že $T \models \varphi \leftrightarrow \psi(x_0)$. Tedy i $T \models \varphi \leftrightarrow (Qx_0)\psi(x_0)$ platí, kde Q je $\forall$ nebo $\exists$. Když navíc L obsahuje konstantní symbol c a $\psi(x/c) \in \Gamma$ jakmile $\psi \in \Gamma$, tak $T \models \varphi \leftrightarrow \psi(x_0/c)$ a poslední formule je sentence z $\mathrm{b}(\Gamma)$.

TVRZENÍ 2.3.31. (Lemma o eliminaci kvantifikátorů.)

1) *Teorie T má eliminaci kvantifikátorů sémanticky, právě když pro každou otevřenou $L(T)$-formuli $\chi(\overline{x}, y)$ s $\mathrm{l}(\overline{x}) > 0$ existuje otevřená formule $\psi(\overline{x})$ tak, že*
$$T \models (\exists y)\chi(\overline{x}, y) \leftrightarrow \psi(\overline{x}). \tag{2.9}$$

2) *Má-li teorie T eliminaci kvantifikátorů sémanticky, je modelově kompletní.*

Důkaz. 1) $\Rightarrow$ je jasná. Dokažme opačnou: Pro každou $L(T)$-formuli $\varphi(\overline{x})$ s $\mathrm{l}(\overline{x}) > 0$ existuje otevřená $\psi(\overline{x})$ tak, že $T \models \varphi \leftrightarrow \psi$. Postupujeme indukcí podle složitosti φ. Je-li otevřená, tvrzení platí. Platí-li pro φ_i s $i < 2$, platí jasně i pro φ tvaru $\neg\varphi_0$ nebo tvaru $\varphi_0 \to \varphi_1$. Je-li konečně φ tvaru $(\forall y)\varphi_0(\overline{x}, y)$ a $T \models \varphi_0 \leftrightarrow \chi(\overline{x}, y)$ s χ otevřenou, existuje $\psi(\overline{x})$ otevřená s $T \models \psi \leftrightarrow \neg(\exists y)\neg\chi$ dle (2.9). Dále $T \models \neg(\exists y)\neg\chi \leftrightarrow (\forall y)\chi \leftrightarrow (\forall y)\varphi_0$; druhá $\leftrightarrow$ plyne z tvrzení o distribuci kvantifikátorů sémanticky. Tedy nakonec $T \models \psi \leftrightarrow \varphi$.

2) Pro dva modely $\mathcal{A}, \mathcal{B}$ teorie T s $\mathcal{A} \subseteq \mathcal{B}$ má platit: Je-li $\varphi(\overline{x})$ nějaká $L(T)$-formule a $\overline{a} \in A^{\mathrm{l}(\overline{x})}$, tak $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}]$. Dokazovaná ekvivalence platí díky $\mathcal{A} \subseteq \mathcal{B}$ pro každou otevřenou $L(T)$-formuli φ a díky eliminaci kvantifikátorů pro každou $L(T)$-formuli φ. □

PŘÍKLAD. Teorie těles charakteristiky 0 není modelově kompletní a nemá tedy eliminaci kvantifikátorů, neboť těleso $\underline{\mathbb{Q}}$ není elementární podstruktura tělesa $\underline{\mathbb{R}}$ (protože $\underline{\mathbb{Q}} \not\equiv \underline{\mathbb{R}}$).

Dále směřujeme k prezentaci ekvivalentní podmínky a postačující podmínky pro eliminaci kvantifikátorů; budeme je formulovat pomocí pojmu koexistence a f-homogenity teorie.

2.3.32. **Parciální vnoření. f-homogenní teorie.**

1. Pro L-struktury $\mathcal{A}, \mathcal{B}$ je *parciální vnoření* $\mathcal{A}$ do $\mathcal{B}$ prosté zobrazení $f \subseteq A \times B$ takové, že pro každou atomickou (ekvivalentně otevřenou) L-formuli $\varphi(\overline{x})$ a $\overline{a} \in \mathrm{dom}(f)^{\mathrm{l}(\overline{x})}$ platí
$$\mathcal{A} \models \varphi(\overline{x})[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi(\overline{x})[f\overline{a}].$$

Říkáme dále, že je lze *bezprostředně prodloužit*, když pro každé $a \in A$ existuje $b \in B$ tak, že $f \cup \{\langle a, b\rangle\}$ je parciální vnoření $\mathcal{A}$ do $\mathcal{B}$.

2. Teorie T je f-*homogenní*, lze-li každé neprázdné konečné parciální vnoření mezi dvěma modely teorie T bezprostředně prodloužit.

POZNÁMKA 2.3.33. Buďte $\mathcal{A}$, $\mathcal{B}$ dvě L-struktury. Snadno se zjistí, že platí:

1. Buď h parciální vnoření $\mathcal{A}$ do $\mathcal{B}$.
   a) h^{-1} je parciální vnoření $\mathcal{B}$ do $\mathcal{A}$.
   b) V $\mathcal{A}$ a $\mathcal{B}$ platí právě tytéž atomické (ekvivalentně otevřené) L-sentence.
   c) Je-li $\mathrm{dom}(h) = A$, je h izomorfní vnoření $\mathcal{A}$ do $\mathcal{B}$.
2. Zobrazení $\emptyset$ je parciální vnoření $\mathcal{A}$ do $\mathcal{B}$, právě když v $\mathcal{A}$ a $\mathcal{B}$ platí tytéž atomické L-sentence.

2.3.34. **1-primitivní a 1-existenční formule. Koexistenční teorie.**

1. *Elementární konjunkce* je formule tvaru $\bigwedge_{i<n} \chi_i$, kde χ_i jsou atomické nebo negace atomických formulí.

2. Je-li formule φ tvaru $(\exists y)\chi$, kde χ je elementární konjunkce resp. bezkvantifikátorová formule, říkáme, že φ je 1-*primitivní* resp. 1-*existenční formule*.

Vezmeme-li $\overline{y}$ místo jednotice y, říkáme, že φ je *primitivní* resp. *existenční formule*.

3. Teorie T je [1-]*koexistenční*, když pro $\mathcal{A} \models T$, $\mathcal{B} \models T$, neprázdné konečné parciální vnoření f modelu $\mathcal{A}$ do $\mathcal{B}$ a každou [1-]primitivní formuli $\varphi(\overline{x})$ s $\mathrm{l}(\overline{x}) > 0$ a $\overline{a} \in \mathrm{dom}(f)^{\mathrm{l}(\overline{x})}$ je
$$\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[f\overline{a}]. \tag{2.10}$$

V definici můžeme ekvivalentně místo [1-]primitivních formulí vzít [1-]existenční, neboť $\psi(\overline{x}, y)$ otevřená je logicky ekvivalentní formuli $\bigvee_{i<n} \psi_i(\overline{x}, y)$, kde $\psi_i(\overline{x}, y)$ jsou elementární konjunkce. Dále lze ekvivalentně v (2.10) vzít $\Rightarrow$ místo $\Leftrightarrow$, neboť f^{-1} je parciální vnoření $\mathcal{B}$ do $\mathcal{A}$.

POZNÁMKA 2.3.35. Elementární konjunkci $\psi(\overline{x}, y)$ lze chápat jako „soustavu elementárních vztahů“, kde elementárním vztahem je nějaký literál $\chi(\overline{x}, y)$; y lze pak chápat jako řešení uvedené soustavy s parametry $\overline{x}$. Je-li $\varphi(\overline{x})$ formule $(\exists y)\psi$, vztah (2.10) vyjadřuje „ekviřešitelnost v $\mathcal{A}$ a $\mathcal{B}$ soustav $\psi(\overline{a}, y)$ a $\psi(f\overline{a}, y)$ pro neznámou y, pokud je f neprázdné konečné parciální vnoření $\mathcal{A}$ do $\mathcal{B}$ a $\overline{a} \in \mathrm{dom}(f)^{\mathrm{l}(\overline{x})}$.“

VĚTA 2.3.36. *Buď T teorie v jazyce s rovností.*

1) (Eliminační ekvivalent.) *Platí:*
   T má eliminaci kvantifikátorů sémanticky $\Leftrightarrow$ T je koexistenční $\Leftrightarrow$ T je 1-koexistenční.
2) (Eliminační kriterium.) *Když T je* f*-homogenní, má eliminaci kvantifikátorů sémanticky.*

Důkaz. 1) Má-li T eliminaci kvantifikátorů sémanticky, plyne tvrzení bezprostředně z definic. Důkaz opačné implikace neuvádíme, není však příliš obtížný. 2) T je zřejmě 1-koexistenční a tvrzení plyne z 1). $\square$

POZNÁMKA 2.3.37. Níže uvedené příklady ukazují mj. toto:
– Předpoklad o neprázdnosti parciálního vnoření v definici koexistence nelze vynechat.
– f-homogenita je silnější, než 1-koexistence; to ukazuje teorie SC_0.
– Eliminace kvantifikátorů neimplikuje otevřenou axiomatizovatelnost; to ukazuje teorie SC_0.

PŘÍKLAD 2.3.38. Buď $L = \langle U \rangle$ jazyk s rovností, přičemž U je unární relační symbol. Buďte $\mathcal{A} = \langle 1, 1 \rangle$, $\mathcal{B} = \langle 1, \emptyset \rangle$ dvě L-struktury ($U^A = A = 1 = \{0\}$, $U^B = \emptyset$).

a) Zobrazení $h = \emptyset$ je parciální vnoření $\mathcal{A}$ do $\mathcal{B}$, neboť neexistuje atomická L-sentence. Avšak h nelze bezprostředně rozšířit do (parciálního) vnoření $\mathcal{A}$ do $\mathcal{B}$.
b) Prázdná L-teorie není f-homogenní, neboť $f = \{\langle 0, 0 \rangle\}$ je parciální vnoření $\langle 2, 2 \rangle$ do $\langle 1, 1 \rangle$.
c) Nechť T je L-teorie s jediným axiomem „existuje právě jeden prvek“; $\mathcal{A}$, $\mathcal{B}$ jsou modely T. Pak T má eliminaci kvantifikátorů sémanticky, neboť je evidentně f-homogenní. Dále je $\emptyset$ parciální vnoření $\mathcal{A}$ do $\mathcal{B}$, $\mathcal{A} \models (\exists v_0)U(v_0)$, $\mathcal{B} \not\models (\exists v_0)U(v_0)$. Předpoklad o neprázdnosti parciálního vnoření v definici koexistence tedy nelze vynechat.

PŘÍKLADY 2.3.39.

1. Teorie SC následníka není modelově kompletní, tedy nemá eliminaci kvantifikátorů. Neboť $\mathcal{A} = \langle \mathbb{N}, \mathrm{S} \rangle$ je model SC, podstruktura $\mathcal{A}\restriction(\mathbb{N} - \{0\})$ je model SC, není to však elementární podstruktura $\mathcal{A}$.

2. a) Teorie SC_0 následníka s nulou má eliminaci kvantifikátorů, neboť je 1-koexistenční. Buď totiž f neprázdné konečné parciální vnoření modelu $\mathcal{A} \models \mathrm{SC}_0$ do $\mathcal{B} \models \mathrm{SC}_0$; můžeme předpokládat, že $0^A \in \mathrm{dom}(f)$. Nechť $a_0, \ldots, a_{n-1}$ je prosté očíslování $\mathrm{dom}(f)$, $\chi(x_0, \ldots, x_{n-1}, y)$ je elementární konjunkce a $\mathcal{A} \models \chi[a_0, \ldots, a_{n-1}, a]$ s jistým $a \in A$; hledáme b tak, aby platilo $\mathcal{B} \models \chi[f(a_0), \ldots, f(a_{n-1}), b]$. Konjunkty konjunkce χ jsou bez újmy na obecnosti tvaru $\mathrm{S}^n x_i = y$ či $\mathrm{S}^n y = x_i$ a jejich negace. Uvedené rovnosti pišme zkráceně jednotně jako $\mathrm{S}^n x_i = y$ s n celým. Když $a = (S^A)^n a_i$ pro nějaké n celé, buď $b = (S^B)^n f(a_i)$; pak má jasně b požadovanou vlastnost. Jinak má b být různé od konečně prvků tvaru $(S^B)^n f(a_i)$; protože je B nekonečné, takové b existuje.

b) Pro $\mathcal{A} \models \mathrm{SC}_0$ je $\langle \mathbb{N}, \mathrm{S}, 0 \rangle$ izomorfní s $\mathcal{A}\restriction A_0$, kde $A_0 = \{\mathrm{S}^n)0;\ n \in \mathbb{N}\}$. Tedy $\langle \mathbb{N}, \mathrm{S}, 0 \rangle$ je algebraický prvomodel SC_0 a z modelové kompletnosti SC_0 plyne, že SC_0 je kompletní sémanticky.

c) SC_0 není f-homogenní. Neboť zobrazení $f : \mathbb{J}_1 \to \mathbb{J}_0$ takové, že $f(\langle 0, 0 \rangle) = \langle 0, 0 \rangle$, je parciální vnoření $\underline{\mathbb{J}}_1(0)$ do $\underline{\mathbb{J}}_0(0)$. Nelze je bezprostředně rozšířit do $\langle 1, 0 \rangle$ ($\in \mathbb{J}_1$).

Přitom $\underline{\mathbb{J}}_n$ je struktura $\langle \mathbb{J}_n, \mathrm{S}_n \rangle$, kde $\mathbb{J}_n = (\{0\} \times \mathbb{N}) \cup \bigcup_{0<i\leq n}(\{i\} \times \mathbb{Z})$ pro $n \in \mathbb{N}$, $\mathrm{S}_n(\langle i, a \rangle) = \langle i, a+1 \rangle$, $\underline{\mathbb{J}}_n(0)$ je expanze struktury $\underline{\mathbb{J}}_n$ o konstantu $\langle 0, 0 \rangle$.

d) Teorie SC_0 není otevřeně axiomatizovatelná sémanticky, neboť podstruktura modelu $\langle \mathbb{N}, S, 0 \rangle$ ($\models \mathrm{SC}_0$) s univerzem $\mathbb{N} - \{1\}$ není model SC_0. (S je přičítání jedničky.)

3. Teorie DeLO je f-homogenní a tedy má eliminaci kvantifikátorů. Důsledkem je např., že pro $\mathcal{A} \models$ DeLO je velikost algebry $\mathrm{Df}^2(\emptyset, \mathcal{A})$ právě 8, neboť jde o podalgebru potenční algebry $\underline{\mathcal{P}}(A^2)$, generovanou podmnožinami A^2, definovanými v $\mathcal{A}$ atomickými formulemi $v_0 = v_1, v_0 \leq v_1$.

2.3.40. V následující tabulce symbol N* v kolonce ω-kateg. značí, že teorie není ω-kategorická, je však kompletní. Všechny uvedené teorie jsou s rovností.

Teorie	ω-kateg.	f-homog.	Koexist.	Prvomodel
DeLO*	N	N	N	Nemá. Má 4 alg. prvomod.
DeLO+	A	N	N	$\langle \mathbb{Q} \cup \{+\infty\}, \leq \rangle$
DeLOc	N*	N	A	$\langle \mathbb{Q}, \leq, n \rangle_{n \in \mathbb{N}}$
DiLO	N*	N	N	$\langle \mathbb{Z}, \leq \rangle$
DiLO°	N*	N	A	$\langle \mathbb{Z}, \leq \rangle^\circ$
Pr	N*	N	N	$\langle \mathbb{N}, \mathrm{S}, +, 0 \rangle$
SC	N*	N	N	$\langle \mathbb{N}, \mathrm{S} \rangle$
SC_0	N*	N	A	$\langle \mathbb{N}, \mathrm{S}, 0 \rangle$
$\mathrm{CE_k}(\infty)$, $2 \leq k \in \mathbb{N}$	N	A	A	Nemá

Tabulka 2.2: Eliminace kvantifikátorů (koexistence) a další charakteristiky některých teorií s rovností.

Z tabulky je např. vidět, že f-homogenita nesplývá s koexistencí a že z f-homogenity neplyne ω-kategoričnost.

Charakteristiky teorie.

Charakteristiky nějaké teorie jsou: kompletnost, JKE (počet Kn, forma JKE), izomorfní spektrum, ω-kategoričnost, konečná axiomatizovatelnost, otevřená axiomatizovatelnost, modelová kompletnost, existence algebraických prvomodelů a prvomodelů, eliminace kvantifikátorů, f-homogenita.

2.3.41. Charakteristiky teorie $\mathrm{VS}(F, \infty)$ nekonečných vektorových prostorů nad tělesem F.

Označme $\mathrm{VS}(F, \infty)$ stručně T.

• Izomorfní spektrum a algebraické prvomodely.

Užijeme těchto známých vlastností vektorových prostorů: vektorový prostor má bázi a každé dvě báze mají tutéž velikost. Dva vektorové prostory nad týmž tělesem jsou izomorfní, právě když jejich báze mají tutéž velikost.

Nechť $\mathcal{A}$ je nekonečný model T velikosti κ; je pak $\dim(\mathcal{A}) \geq 1$.

$$\text{Buď } |F| < \omega. \text{ Pak } \kappa = \dim(\mathcal{A}). \tag{2.11}$$

$$\text{Buď } |F| \geq \omega. \text{ Pak } \kappa \geq |F| \text{ a tedy } \dim(\mathcal{A}) \begin{cases} \leq \kappa & \text{když } \kappa = |F|, \\ = \kappa & \text{když } \kappa > |F|. \end{cases} \tag{2.12}$$

Z (2.11), (2.12) plyne, přičemž $\kappa(\leq)$ značí počet velikostí (kardinálních čísel) nejvýše rovných κ:

$\lvert F \rvert$	$\mathrm{I}(\kappa, T)$	ω-kategoričnost	Alg. prvomodel $\mathcal{A} \models T$
$< \omega$	1, když $\kappa \geq \omega$	A	$\dim(\mathcal{A}) = \omega$
$\geq \omega$	0, když $\omega \leq \kappa < \lvert F \rvert$ $\kappa(\leq)$, když $\kappa = \lvert F \rvert$ 1, když $\kappa > \lvert F \rvert$.	N	$\dim(\mathcal{A}) = 1$

$\mathrm{VS}(F, \infty)$ je pro $|F| < \omega$ kompletní sémanticky. Plyne to z ω-kategorického kriteria kompletnosti sémanticky, neboť jde o ω-kategorickou teorii ve spočetném jazyce a s jen nekonečnými modely.

• Konečná a otevřená axiomatizovatelnost sémanticky.

Teorie T není konečně axiomatizovatelná sémanticky. Když $|F| < \omega$, nestačí vzít konečně axiomů ze schematu „existuje nekonečně prvků“, protože VS(F) má model velikosti $|F|^n$ pro každé $n \in \mathbb{N}$. Když $|F| \geq \omega$, nestačí zřejmě vzít konečně rovností z nekonečného výčtu axiomů vektorových prostorů nad F, plus konečně axiomů ze schematu „existuje nekonečně prvků“.

Teorie T není otevřeně axiomatizovatelná sémanticky, protože každý její model má podstrukturu s univerzem $\{0\}$, což není model T.

• Eliminace kvantifikátorů sémanticky a f-homogenita.

Teorie T má eliminaci kvantifikátorů sémanticky. Dokážeme totiž, že je 1-koexistenční. Buďte $\mathcal{A}$, $\mathcal{B}$ modely T a f neprázdné konečné parciální vnoření $\mathcal{A}$ do $\mathcal{B}$. Nechť $(\exists y)\chi(x_0, \ldots, x_{n-1}, y)$ je 1-primitivní formule, kde χ je elementární konjunkce bez újmy na obecnosti tvaru

$$\bigwedge_{j<m} \sum_{i<n} r_{j,i} x_i + r_j y \diamond_j 0$$

s $r_{j,i}, r_j$ z F, $r_j \neq 0$ a $\diamond_j$ buď $=$ nebo $\neq$. Nechť $\mathcal{A} \models \chi[a_0, \ldots, a_{n-1}, d]$ pro nějaké $a_0, \ldots, a_{n-1}$ z $\mathrm{dom}(f)$ a $d \in A$; hledáme $d' \in B$ s $\mathcal{B} \models \chi[f(a_0), \ldots, f(a_{n-1}), d']$. Je-li $d = -\frac{1}{r_j} \sum_{i<n} r_{j,i} a_i$ pro nějaké $j < m$, buď $d' = -\frac{1}{r_j} \sum_{i<n} r_{j,i} f(a_i)$. Jinak za d' vyberme nějaký prvek z nekonečné množiny $A' \subseteq B$ prvků různý od všech prvků tvaru $-\frac{1}{r_j} \sum_{i<n} r_{j,i} f(a_i)$ s $j < m$. Pak má d' požadované vlastnosti.

Teorie T je f-homogenní, právě když F je konečné. Buďte totiž $\mathcal{A}$, $\mathcal{B}$ modely T. Je-li F konečné, mají $\mathcal{A}$, $\mathcal{B}$ nekonečnou dimenzi a tedy lze každé neprázdné konečné parciální vnoření $\mathcal{A}$ do $\mathcal{B}$ bezprostředně prodloužit. Je-li F nekonečné, nechť $\mathcal{A}$ má dva generátory a_0, a_1 a $\mathcal{B}$ jen jeden b_0. Zobrazení $f = \{\langle a_0, b_0 \rangle\}$ nelze prodloužit do a_1.

• Modelová kompletnost, kompletnost sémanticky, prvomodel.

Teorie T je modelově kompletní, neboť má eliminaci kvantifikátorů.

Teorie T je kompletní sémanticky, neboť je modelově kompletní a má algebraický prvomodel; ten je pak prvomodelem T.

Kon. ax.	Ot. ax.	Kompl.	Model. kompl.	Prvom.	elim. kv.	f-homog.
N	N	A	A	A	A	A $\Leftrightarrow$ $|F| < \omega$

Tabulka 2.3: Charakteristiky teorie VS(F, ∞).

2.3.42. V následující tabulce jsou uvedeny některé charakteristiky několika teorií (s rovností).

Teorie T	**Kompletní**	JKE **neekvival.**	I(κ, T)	ω-**kategorická**	**Otevřeně axiomat.**	**Konečně axiomat.**	**Modelově kompletní**
DeLO	A	1	1 pro $\kappa = \omega$, 2^κ pro $\kappa > \omega$	A	N	A	A
DeLO*	N	4 DeLO$^+$, DeLO$^-$, DeLO$^\pm$, DeLO	4 pro $\kappa = \omega$, 2^κ pro $\kappa > \omega$	N	N	A	N
DeLO$^+$	A	1	1 pro $\kappa = \omega$, 2^κ pro $\kappa > \omega$	A	N	A	N
SC$_0$	A	1	ω pro $\kappa = \omega$, 1 pro $\kappa > \omega$	N	N	N	A
SC	A	1	ω pro $\kappa = \omega$, 1 pro $\kappa > \omega$	N	N	N	N
PE	N	ω PE(n) s $0 < n < \omega$, PE(∞)	1 pro $\kappa > 0$	A	A	A	N
CE$_\mathrm{k}(\infty)$ $2 \le k < \omega$	N	$B(k)$ Extenze o: $\{c_i = [\neq]\ c_j;\ \langle i, j\rangle \in [\notin]\ E\}$, E je ekvivalence na k.	$B(k)$ pro $\kappa \ge \omega$	N	N	N	A
VS(F, ∞) $\lvert F\rvert \ge \omega$	A	1	$\kappa(\le)$ pro $\kappa = \lvert F\rvert$ 1 pro $\kappa > \lvert F\rvert$.	N	N	N	A
UFO^m $0 < m < \omega$	N	ω Extenze o: „existuje právě km prvků“ s $0 < k < \omega$, „existuje nekonečně prvků“.	1 pro $\kappa = km$ s $0 < k < \omega$ 1 pro $\kappa \ge \omega$, 0 jinak.	A	A	A	N
Q	N	2^ω	0 pro $0 < \kappa < \omega$ 2^κ pro $\kappa \ge \omega$.	N	N	A	N
P	N	2^ω	0 pro $0 < \kappa < \omega$ 2^κ pro $\kappa \ge \omega$.	N	N	N	N

Tabulka 2.4: Charakteristiky některých teorií (s rovností). Symbol $\kappa(\le)$ značí počet velikostí nejvýše rovných κ, $B(k)$ pak k-té Bellovo číslo (= počet rozkladů k).

2.4 Faktorstruktury. Algebry formulí.

Kongruence pro L-strukturu $\mathcal{A}$ je ekvivalence $\sim$ na A, respektující relace a funkce struktury $\mathcal{A}$: platnost relace resp. hodnota funkce v daných argumentech $\overline{a}$ a jim blízkých argumentech $\overline{a}'$ (tj. s $\overline{a}_i \sim \overline{a}'_i$ pro $i < \mathrm{l}(\overline{a})$) je táž. Pak lze na faktorech $a/\sim$ s $a \in A$ definovat korektně pomocí reprezentantů operace a funkce na $A/\sim$ a získat tak L-strukturu, značenou $\mathcal{A}/\sim$ a nazývanou faktorstruktura $\mathcal{A}$ dle $\sim$. V logice jsou pro danou L-teorii T s modelem důležité faktorstruktury $\underline{\mathrm{Fm}}_L/\approx_T$ struktury L-formulí dle ekvivalence $\approx_T$, kde $\varphi \approx_T \psi \Leftrightarrow T \models \varphi \leftrightarrow \psi$; taková faktorstruktura je Booleova algebra a nazývá se Lindenbaumova algebra teorie T.

Kongruence. Faktorstruktura.

2.4.1. **Kongruence. Faktorstruktura.**

Buď $\sim$ ekvivalence na $A \neq \emptyset$, $n \in \mathbb{N}$. Relaci $\sim^{[n]}$ definujeme na A^n „po složkách“, tj. tak, že pro $\overline{a}, \overline{a'}$ z A^n je $\overline{a} \sim^{[n]} \overline{a'} \Leftrightarrow \overline{a}_i \sim \overline{a'}_i$ pro každé $i < n$. Místo $\sim^{[n]}$ můžeme stručně psát jen $\sim$. Dále

$$\overline{a}/\sim \quad \text{značí} \quad \langle \overline{a}_0/\sim, \ldots, \overline{a}_{n-1}/\sim\rangle. \tag{2.13}$$

Tudíž $\overline{a}/{\sim} \in (A/{\sim})^n$. Připomeňme, že často ztotožňujeme A s A^1.

1. Ekvivalence $\sim$ je *kongruence pro relaci* $R \subseteq A^n$, když pro každé $\overline{a}, \overline{a'}$ z A^n platí: $\overline{a} \sim^{[n]} \overline{a'} \Rightarrow R(\overline{a}) \Leftrightarrow R(\overline{a'})$. *Faktorrelace* $R^\sim$ *relace* R *dle* $\sim$ je pak definována korektně *pomocí reprezentantů* jako $\{\overline{a}/{\sim};\ R(\overline{a})\}$; je $R^\sim \subseteq (A/{\sim})^n$.

2. Ekvivalence $\sim$ je *kongruence pro funkci* $F : A^n \to A$, když pro každé $\overline{a}, \overline{a'}$ z A^n platí: $\overline{a} \sim^{[n]} \overline{a'} \Rightarrow F(\overline{a}) \sim F(\overline{a'})$. *Faktorfunkce* $F^\sim$ *funkce* F *dle* $\sim$ je pak definována korektně *pomocí reprezentantů* jako $\{\langle \overline{a}/{\sim}, F(\overline{a})/{\sim}\rangle;\ \overline{a} \in A^n\}$; je $F^\sim : (A/{\sim})^n \to A/{\sim}$.

Speciálně je každá ekvivalence $\sim$ kongruence pro nulární relaci či funkci. Dále pro funkci $F = \{\langle \emptyset, c\rangle\}$ čili konstantu c zapisujeme $F^\sim$ přirozeně jako $c/{\sim}$.

3. Ekvivalence $\sim$ je *kongruence pro strukturu* $\mathcal{A}$, když to je kongruence pro každou její relaci a funkci. *Faktorstruktura struktury* $\mathcal{A}$ *podle kongruence* $\sim$ (pro $\mathcal{A}$) je struktura s univerzem $A/{\sim}$ a relacemi a funkcemi, které jsou právě faktorrelacemi a faktorfunkcemi (včetně nulárních) struktury $\mathcal{A}$; značíme ji $\mathcal{A}/{\sim}$. Zobrazení $\pi : A \to A/{\sim}$ takové, že $\pi(a) = a/{\sim}$, je *faktorprojekce* $\mathcal{A}$ *na* $\mathcal{A}/{\sim}$.

TVRZENÍ 2.4.2. (O kongruencích a homomorfizmech.)

1) *Buď $\sim$ kongruence pro $\mathcal{A}$. Pak faktorprojekce $\pi : \mathcal{A} \to \mathcal{A}/{\sim}$ je striktní homomorfizmus na.*

   Důsledek. Jsou-li $t(\overline{x}), s(\overline{x})$ termy, pro $\mathrm{l}(\overline{x})$-tici $\overline{a}$ z A platí:

   a) $t^A[\overline{a}]/{\sim} \;=\; t^{A/\sim}[\overline{a}/{\sim}]$ *a tedy* $t^A[\overline{a}] \sim s^A[\overline{a}] \Leftrightarrow \mathcal{A}/{\sim} \models (t = s)[\overline{a}/{\sim}]$.

   b) $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{A}/{\sim} \models \varphi[\overline{a}/{\sim}]$, *je-li $\varphi(\overline{x})$ atomická, neobsahující rovnost.*

   Speciálně: Atomická formule platící v $\mathcal{A}$, platí v $\mathcal{A}/{\sim}$.

2) *Buď $h : \mathcal{A} \to \mathcal{B}$ striktní homomorfizmus a $\sim$ ekvivalence na A indukovaná h, tj. definovaná vztahem $a \sim a' \Leftrightarrow h(a) = h(a')$. Pak je $\sim$ kongruence pro $\mathcal{A}$ a $\mathcal{A}/{\sim}$ je izomorfně vnořeno do $\mathcal{B}$ via $g(a/{\sim}) = h(a)$ a tedy g je izomorfizmus $\mathcal{A}/{\sim}$ a $h[\mathcal{A}]$.*

   Důsledek: Ekvivalence $\sim$ na A je kongruence pro $\mathcal{A}$, právě když je $\sim$ indukována nějakým striktním homomorfizmem $\mathcal{A}$ (na nějakou strukturu).

Důkaz. 1) Z definic ihned plyne, že π je striktní homomorfizmus. Odtud podle 2.3.11 plyne a), b).
2) Je zřejmé, že $\sim$ je kongruence pro $\mathcal{A}$ a g je homomorfizmus $\mathcal{A}$ do $\mathcal{B}$. Dále je g prosté, neboť $a/{\sim} \neq a'/{\sim}$ implikuje $a \not\sim a'$ a tedy $h(a) \neq h(a')$. Navíc užitím 1) b) a striktnosti pro relační symbol R různý od $=$ a $\overline{a}$ z A máme $R^\sim(\overline{a}/{\sim}) \Leftrightarrow R^A(\overline{a}) \Leftrightarrow R^B(h\overline{a}) \Leftrightarrow R^B(g(\overline{a}/{\sim}))$. Důsledek plyne z právě dokázaného a 1). $\square$

Lindenbaumovy algebry teorie.

2.4.3. Kongruence teorie T, T-ekvivalence sémanticky.

Nechť L-teorie T má model. *Kongruence teorie* T je ekvivalence $\approx_T$ na Fm_L definovaná vztahem

$$\varphi \approx_T \psi \quad\Leftrightarrow\quad T \models \varphi \leftrightarrow \psi. \tag{2.14}$$

Když $\varphi \approx_T \psi$, říkáme, že φ je *T-ekvivalentní sémanticky s ψ*. Je-li T prázdná teorie, vynecháme T- a místo $\approx_T$ píšeme $\approx_L$ nebo jen $\approx$.

Zřejmě platí: Je-li $\varphi \leftrightarrow \psi$ tautologie, tak $\varphi \approx_T \psi$.

TVRZENÍ 2.4.4. *Nechť L-teorie T má model. Pak*

1) $\approx_T$ *je kongruence pro strukturu* $\underline{\mathrm{Fm}}_L$.

2) $\underline{\mathrm{Fm}}_L/{\approx_T}$ *je Booleova algebra.*

3) *Buď $\Phi \subseteq \mathrm{Fm}_L$ množina uzavřená na $\neg, \vee, \&, \bot, \top$, tj. Φ je univerzum struktury $\underline{\Phi} = \underline{\mathrm{Fm}}_L \restriction \Phi$. Označme $\underline{B}$ podalgebru $\underline{\mathrm{Fm}}_L/{\approx_T}$ s univerzem $B = \{\varphi/{\approx_T};\ \varphi \in \Phi\}$. Pak platí:*

   a) $1^B = \{\varphi \in \mathrm{Fm}_L;\ T \models \varphi\}, \qquad 0^B = \{\varphi \in \mathrm{Fm}_L;\ T \models \neg\varphi\}$.

   b) $\varphi/{\approx_T} \leq^B \psi/{\approx_T} \;\Leftrightarrow\; T \models \varphi \to \psi$, *jakmile φ, ψ jsou z Φ.*

   c) *Buď T' jednoduchá extenze teorie T sémanticky, která má model. Pak*

   $$F = \{\varphi/{\approx_T};\ T' \models \varphi \text{ a } \varphi \in \Phi\} \text{ je filtr v } \underline{B}.$$

Důkaz. 1) plyne z 2.2.20.

2) Označme $\underline{\mathrm{Fm}}_L/{\approx_T}$ jako $\langle B, \neg', \vee', \wedge', \perp', \top' \rangle$. Komutativita $\vee'$ znamená, že pro L-formule φ, ψ platí $\varphi/{\approx_T} \vee' \psi/{\approx_T} = \psi/{\approx_T} \vee' \varphi/{\approx_T}$. To ale právě znamená, že platí $T \models \varphi \vee \psi \leftrightarrow \psi \vee \varphi$. Poslední ekvivalence je tautologie, tedy platí v T. Platnost ostatních axiomů Booleových algeber tvaru rovnosti termů plyne zcela stejně. Konečně $\perp' \neq \top'$ plyne z $T \models \neg(\perp \leftrightarrow \top)$ díky existenci modelu teorie T.

3) a), b) plynou bezprostředně z definic. c) Díky existenci modelu teorie T' je $\perp/{\approx_T} \notin F$. Zbývá ukázat uzavřenost F na průsek a „být větší“ v algebře $\underline{B}$. Buďte dále φ, ψ z Φ, $\varphi/{\approx_T} \in F$. Když $\psi/{\approx_T} \in F$, tak $\varphi/{\approx_T} \wedge^B \psi/{\approx_T} = (\varphi \mathbin{\&} \psi)/{\approx_T}$. Máme $T' \models \varphi$, $T' \models \psi$, tedy $T' \models \varphi \mathbin{\&} \psi$; tedy $(\varphi \mathbin{\&} \psi)/{\approx_T} \in F$. Když $\varphi/{\approx_T} \leq^B \psi/{\approx_T}$, tak $T \models \varphi \rightarrow \psi$ dle b), tím spíše $T' \models \varphi \rightarrow \psi$. Protože $T' \models \varphi$, tak $T' \models \psi$ a konečně tedy $\psi/{\approx_T} \in F$. □

2.4.5. Lindenbaumovy algebry. Algebry výroků.

Nechť L-teorie T má model. Buď $\Phi \subseteq \mathrm{Fm}_L$ univerzum struktury $\underline{\Phi} = \underline{\mathrm{Fm}}_L \restriction \Phi$.

1. Algebra $\underline{B}$ z 2.4.4, 3) se značí $\mathrm{B}^\Phi T$.

2. Když Φ je Fm_L resp. Fm_L^n s $n \in \mathbb{N}$, píšeme jen $\mathrm{B}T$ resp. $\mathrm{B}^n T$ a říkáme, že to je *Lindenbaumova algebra teorie* T resp. n*-tá Lindenbaumova algebra teorie* T. Je-li T prázdná L-teorie, píšeme $\mathrm{B}L$ resp. $\mathrm{B}^n L$. Zřejmě platí:

$$\mathrm{B}^0 T \subseteq \mathrm{B}^1 T \subseteq \cdots \subseteq \mathrm{B}^n T \subseteq \mathrm{B}^{n+1} T \subseteq \cdots \subseteq \mathrm{B}T.$$

3. Buď T výroková teorie nad $\mathbb{P}$ s modelem. *Algebra výroků teorie* T je algebra $\mathrm{B}^\Phi T$, kde Φ jsou bezkvantifikátorové $L^{\mathbb{P}}$-formule (čili výroky nad $\mathbb{P}$); značí se

$$\underline{\mathrm{AV}}(T), \text{ stručněji } \mathrm{AV}(T);$$

je-li T prázdné, píšeme jen $\underline{\mathrm{AV}}(\mathbb{P})$ či $\mathrm{AV}(\mathbb{P})$, nebo jen $\underline{\mathrm{AV}}$ či AV.

TVRZENÍ 2.4.6. (O Lindenbaumových algebrách a algebrách definovatelných množin.) *Buď T teorie s modelem $\mathcal{A}$, $n \in \mathbb{N}$. Pak zobrazení $h : \mathrm{B}^n T \rightarrow \mathrm{Df}^n(\emptyset, \mathcal{A})$, dané vztahem $h(\varphi/{\approx_T}) = \varphi(\mathcal{A}^n)$ pro φ z Fm_L^n, je homomorfizmus algebry $\mathrm{B}^n T$ na algebru $\mathrm{Df}^n(\emptyset, \mathcal{A})$.*

Je-li T kompletní sémanticky, je zobrazení h izomorfizmus uvedených algeber.

Důkaz. Je patrné, že h je homomorfizmus a na. Nechť jsou každé dva modely teorie T elementárně ekvivalentní; dokážeme, že h je prosté. Buďte $\varphi, \psi \in \mathrm{Fm}_L^n$, $\varphi/{\approx_T} \neq \psi/{\approx_T}$. Tudíž $T \not\models \varphi \leftrightarrow \psi$, tudíž v nějakém a tedy v každém modelu teorie T platí $(\exists v_0, \ldots, v_{n-1})\neg(\varphi \leftrightarrow \psi)$; speciálně pro nějaké $\overline{a} \in A^n$ je $\mathcal{A} \models \neg(\varphi \leftrightarrow \psi)[\overline{a}]$. Pak ovšem $\overline{a}$ je v symetrickém rozdílu množin $\varphi(\mathcal{A}^n), \psi(\mathcal{A}^n)$ a tedy $h(\varphi/{\approx_T}) \neq h(\psi/{\approx_T})$. □

2.4.7. Booleovské úpravy formulí.

Nechť T je L-teorie s modelem. V Booleově algebře $\mathrm{B}T$ platí řada „booleovských“ pravidel tvaru rovnosti termů, jako např. komutativita, asociativita, distributivita booleovských operací, de Morganovy vztahy atd.; mluvíme pak korelativně o komutativitě, asociativitě atd. odpovídajících spojek. Zmíněné rovnosti napsané pomocí reprezentantů faktorů z $\mathrm{B}T$ mají tvar ekvivalence dvou formulí, pravdivé v T. Tudíž „booleovská“ pravidla dovolují nalézat k dané formuli formuli s ní ekvivalentní v T.

PŘÍKLAD.

a) $(\varphi \rightarrow \psi) \mathbin{\&} \neg\varphi \approx (\neg\varphi \vee \psi) \mathbin{\&} \neg\varphi \approx \neg\varphi \vee (\neg\varphi \mathbin{\&} \psi) \approx \neg\varphi$.
1. vztah $\approx$ platí, neboť ekvivalence formulí před a za ním je tautologie. (Jiný argument: $\neg\varphi \vee \psi$ je $\neg\neg\varphi \rightarrow \psi$ dle definice zkratky $\vee$. Protože $\models \neg\neg\varphi \leftrightarrow \varphi$, plyne pravdivost dokazované ekvivalence z tvrzení o ekvivalenci sémanticky.) 2. vztah $\approx$ plyne užitím distributivity, idempotence a komutativity &, 3. užitím booleovské identity $a \vee (a \wedge b) = a$ (nebo argumentací tautologií).

b) Nechť $L = \langle \leq, 0 \rangle$ je jazyk s rovností, přičemž $\leq$ je binární relační a 0 konstantní symbol. Nechť $T = \{(\forall x)\neg(0 \leq x)\}$ je L-teorie a χ L-formule je $((\exists x)(0 \leq x) \rightarrow \psi) \mathbin{\&} (\forall x)\neg(0 \leq x)$. Máme zjistit, zda $T \models \chi$.

Označme $(\exists x)(0 \leq x)$ jako φ. Pak $\neg\varphi \approx (\forall x)\neg(0 \leq x)$. Tedy máme $\chi \approx (\varphi \rightarrow \psi) \mathbin{\&} \neg\varphi \approx \neg\varphi$ užitím tvrzení o ekvivalenci sémanticky a a). Tudíž $T \models \chi$.

2.4.8. Význam a užití Lindenbaumových algeber.

Lindenbaumovy algebry zachycují základní „booleovskou“ strukturu uvažované L-teorie T, pokud má T model. Platí např. následující:

- Lze provádět T-ekvivalentní „booleovské“ úpravy formulí, tj. až na T-ekvivalenci užívat asociativitu, komutativitu a distributivitu disjunkce a konjunkce, deMorganova pravidla atd. Vztah „φ je (sémanticky) silnější než ψ v T“, tj. $T \models \varphi \to \psi$, odpovídá uspořádání v $\mathrm{B}T$.
- „Množina pravdivých formulí teorie T je filtr v algebře $\mathrm{B}L$“. Přesněji:
  $\mathrm{Tru}(T, L) = \{\varphi/{\approx_L};\ T \models \varphi\}$ je filtr v $\mathrm{B}L$. Tudíž $\mathrm{B}T \cong \mathrm{B}L/\mathrm{Tru}(T, L)$. Podobně pro $\mathrm{B}^n T$.
  - Ultrafiltr v $\mathrm{B}^0 L$ rozšiřující $\mathrm{Tru}(T, L)$ představuje (formulemi z jeho faktorů) jednoduchou kompletní extenzi teorie T.
  - Ultrafiltr v $\mathrm{B}^0 T$ představuje právě jednu jednoduchou kompletní extenzi teorie T.
  - T je kompletní $\Leftrightarrow \mathrm{B}^0 T \cong \underline{2}$.
  - Je-li L s rovností, tak
    $\mathrm{B}T \cong \underline{2} \Leftrightarrow T$ je kompletní sémanticky a každý model teorie T je 1-prvkový.
- Kvalita Lindenbaumových algeber charakterizuje řadu vlastností teorií v jazyce L s rovností. Např. pro L-teorii T s modelem platí:
  - $\varphi/{\approx_T}$ je atom v $\mathrm{B}T \Rightarrow T, \varphi$ je kompletní teorie. Opačná implikace neplatí.
  - Je-li T spočetná 1-kategorická s alespoň dvouprvkovým modelem, tak
    $$\mathrm{B}T \cong \underline{2} \times \underline{\mathrm{C}}_\infty.$$
  - Kompletní spočetná teorie T je ω-kategorická $\Leftrightarrow$ každá algebra $\mathrm{B}^n T$ je konečná.
  - Kompletní spočetná teorie T má prvomodel $\Leftrightarrow$ každá algebra $\mathrm{B}^n T$ je atomární.

2.5 Formalistické upřesnění – designátory.

2.5.1. **Notace. Designátory.**
Obecná notace je dvojice $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$, kde $\emptyset \notin \mathcal{S}$, $Ar_{\mathcal{S}} : \mathcal{S} \to \mathbb{N}$; značíme ji stručně $\underline{\mathcal{S}}$ nebo jen $\mathcal{S}$. Dále $S \in \mathcal{S}$ je *symbol* $\underline{\mathcal{S}}$, $Ar_{\mathcal{S}}(S)$ je *četnost* S, $Ar_{\mathcal{S}}[\mathcal{S}]$ je *množina četností* $\underline{\mathcal{S}}$. Obecná notace $\underline{\emptyset}$ se nazývá *prázdná*; ztotožňujeme ji s $\emptyset$. *Notace* je obecná notace $\underline{\mathcal{S}}$, obsahující alespoň jeden nulární symbol; tedy $0 \in Ar_{\mathcal{S}}[\mathcal{S}]$.

Množina $\mathrm{D}(\mathcal{S})$ *designátorů* notace $\underline{\mathcal{S}}$ je definována induktivní definicí:

Pro $S \in \mathcal{S}$ a sekvenci s designátorů délky $Ar_{\mathcal{S}}(S)$ je $\langle S \rangle \smile \sqcup (s)$ designátor.

Je-li $S \in \mathcal{S}$ a $s = \langle s_0, \dots, s_{n-1} \rangle$ sekvence, užíváme pro grafický zápis sekvence $\langle S \rangle \smile \sqcup (s)$ „obvyklou“ prefixní nebo infixní notaci, tj.

$$\langle S \rangle \smile \sqcup (\langle s_0, \dots, s_{n-1} \rangle) \text{ značíme } S(s_0, \dots, s_{n-1}), \text{ také (infixně) } (s_0 S s_1), \text{ když } n = 2.$$

Poznamenejme, že pro $n = 0$ se často píše místo $S()$ jen S. V „obvyklé notaci“ užíváme tři delimitery), (. Zápisu $\langle S \rangle \smile \sqcup (s)$ říkáme *polská notace*; nepotřebuje delimitery, ale jen rozpoznání pozice v sekvenci a ovšem údaj o četnosti symbolů. Sekvence x je *podsekvence* sekvence y, existují-li sekvence y_0, y_1 tak, že platí $y_0 \smile x \smile y_1 = y$; říkáme pak také, že x má *výskyt v* y. *Poddesignátor* nějakého designátoru η je designátor mající výskyt v η.

Důležitá jsou následující tři tvrzení o designátorech: o jednoznačnosti, o výskytech designátorů a o substituci. Speciálně pak každý designátor má jednoznačný tvar a délku. To dovoluje *dokazovat indukcí dle délky* designátorů nějakou jejich vlastnost a dále *definovat indukcí dle délky* designátorů nějakou vlastnost designátorů či hodnotu designátorům přiřazenou (tj. konstruovat ji rekurzivně).

TVRZENÍ 2.5.2. (O jednoznačnosti designátorů.) *Designátor je jednoznačně tvaru* $\langle S \rangle \smile \sqcup (s)$ *pro jisté* $S \in \mathcal{S}$ *a jisté* $s \in \mathrm{D}(\mathcal{S})^{Ar(S)}$.

Důkaz. Je třeba dokázat jen jednoznačnost výrazu $\langle S \rangle \smile \sqcup (s)$ pro $S \in \mathcal{S}$ a $s \in \mathrm{D}(\mathcal{S})^{Ar(S)}$. Buď $\langle S \rangle \smile \sqcup (s)$ rovno $\langle S \rangle \smile \sqcup (s')$ pro jisté $s' \in \mathrm{D}(\mathcal{S})^{Ar(S)}$; máme dokázat $s = s'$. Když $s \neq s'$, tak pro nejmenší i s $(s)_i \neq (s')_i$ je $(s)_i < (s')_i$ nebo $(s')_i < (s)_i$. To je ve sporu s 2.5.3. $\square$

LEMMA 2.5.3. *Buďte* $\langle \eta_1, \ldots, \eta_n \rangle$, $\langle \eta'_1, \ldots \eta'_n \rangle$ *sekvence designátorů takové, že* $\sqcup(\langle \eta_1, \ldots, \eta_n \rangle) \lessdot \sqcup(\langle \eta'_1, \ldots \eta'_n \rangle)$. *Pak* $\eta_i = \eta'_i$ *pro* $i = 1, \ldots, n$. *Speciálně pro designátory* $\eta \lessdot \eta'$ *je* $\eta = \eta'$.

Důkaz. Indukcí dle délky $\sqcup(\langle \eta_1, \ldots, \eta_n \rangle)$. Buď $\eta_1 = \langle S \rangle \sqcup (\langle \hat{\eta}_1, \ldots, \hat{\eta}_k \rangle)$ s nějakým $S \in \mathcal{S}$ a designátory $\hat{\eta}_1, \ldots, \hat{\eta}_k$; η'_1 nutně začíná S, tedy $\eta'_1 = \langle S \rangle_\smile \sqcup (\langle \hat{\eta}'_1, \ldots, \hat{\eta}'_k \rangle)$ s nějakými designátory $\hat{\eta}'_1, \ldots, \hat{\eta}'_k$. Je-li $\eta_1 \lessdot \eta'_1$, tak $\sqcup(\langle \hat{\eta}_1, \ldots, \hat{\eta}_k \rangle) \lessdot \sqcup(\langle \hat{\eta}'_1, \ldots, \hat{\eta}'_k \rangle)$. Tudíž podle indukčního předpokladu je $\hat{\eta}_i = \hat{\eta}'_i$ pro $i = 1, \ldots, k$ (i pokud $k = 0$) a tedy $\eta_1 = \eta'_1$. Pak ale $\sqcup(\langle \eta_2, \ldots, \eta_n \rangle) \lessdot \sqcup(\langle \eta'_2, \ldots \eta'_n \rangle)$ a tudíž opět dle indukčního předpokladu je také $\eta_i = \eta'_i$ pro $i = 2, \ldots, n$. Podobně, když $\eta'_1 \lessdot \eta_1$. Speciální tvrzení plyne bezprostředně. □

TVRZENÍ 2.5.4. (O výskytech designátorů.) *Každý výskyt designátoru* η' *v designátoru* η *tvaru* $\langle S \rangle_\smile \sqcup (s)$ *s* $S \in \mathcal{S}$ *a* $s \in \mathrm{D}(\mathcal{S})^{Ar_{\mathcal{S}}(S)}$ *je buď* η *nebo je to výskyt v některém členu* $(s)_i$.

Důkaz. Nechť výskyt symbolu, jenž je první člen uvažovaného výskytu designátoru η', je první S v η; je $\eta' \lessdot \eta$, tedy dle 2.5.3 je $\eta = \eta'$.

Nechť výskyt symbolu, jenž je první člen uvažovaného výskytu designátoru η', je v některém $(s)_i$. Pak dle 2.5.5 je tento výskyt prvým členem výskytu nějakého designátoru η'' v $(s)_i$. Je nutně $\eta' \lessdot \eta''$ nebo $\eta'' \lessdot \eta'$, tedy $\eta' = \eta''$ a tedy η' se vyskytuje v $(s)_i$ jako η''. □

LEMMA 2.5.5. *Každý výskyt symbolu v nějakém designátoru* η *je prvým členem nějakého výskytu nějakého designátoru v* η.

Důkaz. Indukcí na designátorech. Máme dokázat: když $S \in \mathcal{S}$, $s \in \mathrm{D}(\mathcal{S})^{Ar_{\mathcal{S}}(S)}$ a tvrzení platí pro každé η rovno některému $(s)_i$, tak tvrzení platí pro η rovno $\langle S \rangle_\smile \sqcup (s)$. Je-li $s = \emptyset$, je to jasné. Jinak jde o prvý výskyt S nebo o výskyt v nějakém $(s)_i$. Podle indukčního předpokladu je prvým členem nějakého výskytu nějakého designátoru v $(s)_i$; ten je ovšem výskytem designátoru v $\langle S \rangle_\smile \sqcup (s)$. □

TVRZENÍ 2.5.6. (O substituci v designátorech.) *Nahradí-li se výskyt designátoru* η' *v designátoru* η *designátorem* η'', *získá se designátor.*

Důkaz. Indukcí na designátorech. Buď $\eta = \langle S \rangle_\smile \sqcup (s)$ a pro $(s)_i$ s $i < Ar_{\mathcal{S}}(S)$ nechť to platí. Pak uvažovaný výskyt η' je η a platí to, nebo je to výskyt v některém $(s)_i$; pak díky indukčnímu předpokladu to opět platí. □

2.5.7. Struktura designátorů.

Buď $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$ notace.

1. *Struktura výrazů* notace $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$ je struktura $\underline{\mathrm{D}}^*(\mathcal{S})$ tvaru $\langle \mathcal{S}^*, \mathcal{S}^\circ \rangle$, kde $\mathcal{S}^\circ$ je soubor $\langle S^\circ \rangle_{S \in \mathcal{S}}$ funkcí takových, že

$$S^\circ : (\mathcal{S}^*)^{Ar_{\mathcal{S}}(S)} \to \mathcal{S}^*, \qquad S^\circ(s) = \langle S \rangle_\smile \sqcup (s) \text{ pro } s \in (\mathcal{S}^*)^{Ar_{\mathcal{S}}(S)}. \tag{2.15}$$

Tedy $\underline{\mathrm{D}}^*(\mathcal{S})$ je $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$-struktura, kde $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$ představuje funkční signaturu.

2. *Struktura designátorů* notace $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$ je podstruktura $\underline{\mathrm{D}}(\mathcal{S})$ struktury $\underline{\mathrm{D}}^*(\mathcal{S})$ s univerzem $\mathrm{D}(\mathcal{S})$. Zřejmě je to podstruktura $\underline{\mathrm{D}}^*(\mathcal{S})$ generovaná prázdnou množinou.

3. Nechť $\mathcal{A}$ je funkční $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$-struktura. *Hodnota* $H^A(\eta)$ designátoru η z $\mathrm{D}(\mathcal{S})$ v $\mathcal{A}$ je konstruována rekurzí pro $S \in \mathcal{S}$ s $n = Ar_{\mathcal{S}}(S)$ a $\eta_0, \ldots, \eta_{n-1}$ z $\mathrm{D}(\mathcal{S})$:

$$H^A(S(\eta_0, \ldots, \eta_{n-1})) = S^A(H^A(\eta_0), \ldots, H^A(\eta_{n-1})). \tag{2.16}$$

Speciálně když η je $\langle c \rangle$ s konstantním c, je $H^A(\eta) = c^A$. Dále je H^A homomorfizmus $\underline{\mathrm{D}}(\mathcal{S})$ do $\mathcal{A}$.

TVRZENÍ 2.5.8. *Nechť* $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$ *je notace.*

1) *Když* $\mathcal{A} = \underline{\mathrm{D}}(\mathcal{S})$, *tak pro* η *z* $\mathrm{D}(\mathcal{S})$ *je* $H^A(\eta) = \eta$.

2) *Když* h *je homomorfizmus* $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$*-struktury* $\mathcal{A}$ *do* $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$*-struktury* $\mathcal{B}$, *tak pro* η *z* $\mathrm{D}(\mathcal{S})$ *je*
$$h(H^A(\eta)) = H^B(\eta).$$

Důkaz. 1) Indukcí na designátorech. Nechť $\eta = \langle S \rangle_\smile \sqcup (s)$ s n-árním S a s rovným $\langle \eta_0, \ldots, \eta_{n-1} \rangle$, přičemž pro $\eta_0, \ldots, \eta_{n-1}$ to platí. Pak $H^A(\eta) = S^A(\eta_0, \ldots, \eta_{n-1}) = S^\circ(\eta_0, \ldots, \eta_{n-1}) = \eta$. 2) plyne opět indukcí na designátorech užitím (2.16). □

2.6 Některé teorie v predikátové logice s rovností.

Teorie jsou uvedeny v rámci následujících skupin: prearitmetické teorie, aritmetické teorie, Booleovy algebry, uspořádání, grafy, algebraické teorie, demonstrační teorie.

Všechny uvedené jazyky jsou s rovností.

Prearitmetické teorie.

2.6.1. **Teorie následníka** SC**.**

Jazyk: $\langle \mathrm{S}\rangle$, S je unární funkční symbol.

Axiomy: (Q0) $(\exists x)((\forall y)(\mathrm{S}y \neq x) \mathbin{\&} (\forall z \neq x)(\exists y)(\mathrm{S}y = z))$,
(Q2) $\mathrm{S}x = \mathrm{S}y \to x = y$,
SC-schema $x \neq \mathrm{S}^n x$; $n > 0$ je přirozené.

Každý term teorie SC je ekvivalentní termu tvaru $\mathrm{S}^n x$. Každá atomická $\langle \mathrm{S}\rangle$-formule je v SC ekvivalentní formuli tvaru $\mathrm{S}^n x = y$, kde n je přirozené, x, y jsou proměnné (ev. stejné).

Teorie následníka s definovanou nulou SC° je extenze teorie SC o definici konstantního symbolu 0:

$$0 = y \leftrightarrow (\forall z)(\mathrm{S}z \neq y) \mathbin{\&} (\forall y' \neq y)(\exists z)(\mathrm{S}z = y').$$

Teorie následníka s nulou SC_0**.**

Jazyk: $\langle \mathrm{S}, 0\rangle$, S je unární funkční symbol, 0 je konstantní symbol.

Axiomy: (Q1) $0 \neq \mathrm{S}x$,
(Q2) $\mathrm{S}x = \mathrm{S}y \to x = y$,
(Q7) $x \neq 0 \to (\exists y)(\mathrm{S}y = x)$,
SC-schema: $x \neq \mathrm{S}^n x$; $n > 0$ je přirozené.

SC_0^- je $\langle \mathrm{S}, 0\rangle$-teorie s axiomy (Q1), (Q2), (Q7); SC_0 je jednoduchá extenze SC_0^- o SC-schema.

Pro n přirozené je n-tý *numerál* $\underline{n}$ konstantní term $\mathrm{S}\cdots\mathrm{S}0$, S aplikováno n-krát; $\underline{0}$ je 0.

2.6.2. **Teorie následníka s indukcí** SCI se získá tak, že v SC_0 se místo SC-schematu vezme *schema indukce pro jazyk* $\langle \mathrm{S}, 0\rangle$, tj. pro každou $\langle \mathrm{S}, 0\rangle$-formuli φ axiom indukce I_φ pro φ, což je formule

$$(\varphi(0, \overline{y}) \mathbin{\&} (\forall x)(\varphi(x, \overline{y}) \to \varphi(\mathrm{S}x, \overline{y}))) \to (\forall x)\varphi(x, \overline{y}).$$

2.6.3. Struktury $\underline{\mathbb{J}}_n$ a $\underline{\mathbb{K}}_n^m$.

Buď $0 < m \in \mathbb{N}$. S/m značí přičítání jedničky v $\mathbb{Z}_m$, tj. přičítání jedničky v celých číslech modulo m. Buď $n \in \mathbb{N}$ nebo $n = \omega$.

- $\underline{\mathbb{J}}_n$ je struktura $\langle \mathbb{J}_n, \mathrm{S}_n\rangle$, kde

  $$\mathbb{J}_n = (\{0\} \times \mathbb{N}) \cup \textstyle\bigcup_{0<i\leq n}(\{i\} \times \mathbb{Z}) \text{ pro } n \in \mathbb{N}, \qquad \mathbb{J}_\omega = (\{0\} \times \mathbb{N}) \cup \bigcup_{0<i\in\mathbb{N}}(\{i\} \times \mathbb{Z}).$$
  $$\mathrm{S}_n(\langle i, a\rangle) = \langle i, a+1\rangle.$$

  $\underline{\mathbb{J}}_n(0)$ je expanze struktury $\underline{\mathbb{J}}_n$ o konstantu $\langle 0, 0\rangle$.

  Zřejmě platí $\underline{\mathbb{J}}_0 \cong \langle \mathbb{N}, \mathrm{S}\rangle$, $\underline{\mathbb{J}}_n \restriction (\{i\} \times \mathbb{Z}) \cong \langle \mathbb{Z}, \mathrm{S}\rangle$ pro $0 < i \leq n$, $\underline{\mathbb{J}}_0(0) \cong \langle \mathbb{N}, \mathrm{S}, 0\rangle$ a dále

  $$\begin{array}{lcl} \underline{\mathbb{J}}_n & \models & \mathrm{SC}, \\ \underline{\mathbb{J}}_n(0) & \models & \mathrm{SC}_0. \end{array}$$

- $\underline{\mathbb{K}}_n^m$ je struktura $\langle \mathbb{K}_n^m, \mathrm{S}_n^m\rangle$, kde:

  $$\mathbb{K}_n^m = (\{0\} \times \mathbb{N}) \cup \textstyle\bigcup_{0<i\leq n}(\{i\} \times \mathbb{Z}_m) \text{ pro } n \in \mathbb{N}, \quad \mathbb{K}_\omega^m = (\{0\} \times \mathbb{N}) \cup \bigcup_{0<i\in\mathbb{N}}(\{i\} \times \mathbb{Z}_m),$$
  $$\mathrm{S}_n^m(\langle 0, a\rangle) = \langle 0, a+1\rangle, \qquad \mathrm{S}_n^m(\langle i, a\rangle) = \langle i, \mathrm{S}/m(a)\rangle \text{ pro } 0 < i.$$

  $\underline{\mathbb{K}}_n^m(0)$ je expanze $\underline{\mathbb{K}}_n^m$ o konstantu $\langle 0, 0\rangle$.

  Zřejmě máme pro $1 < m$, $0 < n$:

  $$\begin{array}{lcll} \underline{\mathbb{K}}_n^m & \models & (\mathrm{Q0}), (\mathrm{Q2}), & \text{SC-schema neplatí v } \underline{\mathbb{K}}_n^m. \\ \underline{\mathbb{K}}_n^m(0) & \models & (\mathrm{Q1}), (\mathrm{Q2}), (\mathrm{Q7}), & \text{SC-schema neplatí v } \underline{\mathbb{K}}_n^m(0). \end{array}$$

2.6.4. **Presburgerova aritmetika** Pr.

Jazyk: $L^a = \langle \mathrm{S}, +, 0\rangle$, S je unární funkční symbol, + je binární funkční symbol, 0 je konstantní symbol.

Axiomy:
(Q1) $0 \neq \mathrm{S}x$
(Q2) $\mathrm{S}x = \mathrm{S}y \to x = y$
(Q3) $x + 0 = x$
(Q4) $x + \mathrm{S}y = \mathrm{S}(x + y)$
schema indukce: $\{I_\varphi;\ \varphi$ je $\langle \mathrm{S}, +, 0\rangle$-formule$\}$. I_φ je axiom indukce pro φ, tj.

$$(\varphi(0,\overline{y})\ \&\ (\forall x)(\varphi(x,\overline{y}) \to \varphi(\mathrm{S}x,\overline{y}))) \to (\forall x)\varphi(x,\overline{y}).$$

Aritmetické teorie.

2.6.5. **Robinsonova aritmetika** Q.

Jazyk: $L^A = \langle \mathrm{S}, +, \cdot, 0, \leq\rangle$, S je unární funkční symbol, $+, \cdot$ jsou binární funkční symboly, 0 je konstantní symbol, $\leq$ je binární relační symbol.

Axiomy:

(Q1)	$0 \neq \mathrm{S}x$	(Q5)	$x \cdot 0 = 0$
(Q2)	$\mathrm{S}x = \mathrm{S}y \to x = y$	(Q6)	$x \cdot \mathrm{S}y = x \cdot y + x$
(Q3)	$x + 0 = x$	(Q7)	$x \neq 0 \to (\exists y)(x = \mathrm{S}y)$
(Q4)	$x + \mathrm{S}y = \mathrm{S}(x + y)$	(Q8)	$x \leq y \leftrightarrow (\exists z)(z + x = y)$

Pro n přirozené je n-tý *numerál* $\underline{n}$ konstantní term $\mathrm{S}\cdots\mathrm{S}0$, S aplikováno n-krát; $\underline{0}$ je 0.

2.6.6. **Peanova aritmetika** P.

Jazyk: $L^A = \langle \mathrm{S}, +, \cdot, 0, \leq\rangle$.

Axiomy: Robinsonova aritmetika Q
schema indukce: $\{I_\varphi;\ \varphi$ je L^A-formule$\}$. I_φ je axiom indukce pro φ, tj.

$$(\varphi(0,\overline{y})\ \&\ (\forall x)(\varphi(x,\overline{y}) \to \varphi(\mathrm{S}x,\overline{y}))) \to (\forall x)\varphi(x,\overline{y}).$$

2.6.7. *Standardní model aritmetiky* je struktura $\langle \mathbb{N}, \mathrm{S}, +, \cdot, 0, \leq\rangle$, kde $\mathrm{S}(n) = n + 1$ pro $n \in \mathbb{N}$ a $+, \cdot, 0, \leq$ mají obvyklý význam (v oboru přirozených čísel). Standardní model aritmetiky značíme $\mathcal{N}$ nebo $\underline{\mathbb{N}}$; je to zřejmě model Peanovy aritmetiky:

$$\underline{\mathbb{N}} \models \mathrm{P}.$$

Booleovy algebry.

2.6.8. **Teorie Booleových algeber.**

Jazyk: $L^{Ba} = \langle -, \vee, \wedge, 0, 1\rangle$, $\vee, \wedge$ jsou binární funkční symboly, $-$ unární funkční symbol, $0, 1$ jsou konstantní symboly.

Axiomy:

$x \diamond (y \diamond z) = (x \diamond y) \diamond z$	$\diamond$ je $\vee$ nebo $\wedge$	(asociativita)
$x \diamond y = y \diamond x$	$\diamond$ je $\vee$ nebo $\wedge$	(komutativita)
$x \diamond (y \diamond' z) = (x \diamond y) \diamond' (x \diamond z)$	$\diamond$ [$\diamond'$] je $\vee$ [$\wedge$] nebo $\wedge$ [$\vee$]	(distributivita)
$x \vee (x \wedge y) = x = x \wedge (x \vee y)$		(absorbce)
$x \vee (-x) = 1, \quad x \wedge (-x) = 0$		(komplementace)
$0 \neq 1$		(netrivialita)

2.6.9. **Teorie (bez)atomárních Booleových algeber.**

Teorie bBA *bezatomárních Booleových algeber* je obohacení teorie BA o axiom

$$\neg(\exists x)(\text{„}x \text{ je atom“}).$$

Teorie aBA *atomárních Booleových algeber* je obohacení teorie BA o axiom

$$x \neq 0 \to (\exists y)(\text{„}y \text{ je atom“}\ \ \&\ \ \text{„}y \text{ je pod } x\text{“}).$$

Přitom vlastnost „x je atom značí“, že x je nenulový a pod x je jen 0 nebo x a „y je pod x“ je vyjádřeno formulí $y \wedge x = y$. Tedy „x je atom“ vyjadřuje formule

$$x \neq 0\ \&\ (\forall y)(y = y \wedge x \to (y = 0 \vee y = x)).$$

Uspořádání.

2.6.10. **Teorie uspořádání.**
Jazyk: $L^o = \langle \leq \rangle$, $\leq$ je binární relační symbol.
Axiomy: $x \leq x$, $x \leq y \,\&\, y \leq x \to x = y$, $x \leq y \,\&\, y \leq z \to x \leq z$.

2.6.11. **Teorie lineárního uspořádání** LO je extenze teorie uspořádání o *axiom dichotomie*

$$x \leq y \vee y \leq x.$$

2.6.12. **Teorie hustého lineárního uspořádání** DeLO* **a její extenze.**
Přidáme-li k teorii LO *axiom hustoty*

$$(\exists x, y)(x \neq y) \,\&\, ((x \leq y \,\&\, x \neq y) \to (\exists z)(x \leq z \leq y \,\&\, x \neq z \neq y)),$$

získáme *teorii hustého lineárního uspořádání* DeLO*. *Teorie hustého lineárního uspořádání s nejmenším [a bez největšího]* resp. *s největším [a bez nejmenšího]* resp. *nejmenším i největším prvkem* je extenze teorie DeLO* hustého lineárního uspořádání o axiom „existuje nejmenší [a neexistuje největší] prvek“ resp. „existuje největší [a neexistuje nejmenší] prvek“ resp. „existuje nejmenší i největší prvek“. Značíme ji

$$\mathrm{DeLO}^{\overset{-}{*}}\ [\mathrm{DeLO}^-] \qquad \text{resp.} \qquad \mathrm{DeLO}^{\overset{+}{*}}\ [\mathrm{DeLO}^+] \qquad \text{resp.} \qquad \mathrm{DeLO}^{\pm}.$$

Označme dále $\langle \mathbb{Q}, \leq \rangle^\diamond$ extenzi $\langle \mathbb{Q}, \leq \rangle$ do modelu DeLO$^\diamond$, kde $\diamond$ je $-, +, \pm$, která vznikne přidáním nejmenšího resp. největšího resp. nejmenšího i největšího prvku. Připomeňme, že DeLO je extenze DeLO* o axiom „neexistuje ani nejmenší ani největší prvek“.

Teorie DeLOc je extenze teorie DeLO o rekurzivní množinu spočetně konstantních symbolů c_n a axiomy

$$\{c_n \leq c_{n+1} \,\&\, c_n \neq c_{n+1};\ n \in \mathbb{N}\}.$$

2.6.13. **Teorie diskrétního lineárního uspořádání** DiLO**,** DiLO$^\circ$**.**
Teorie *diskrétního lineárního uspořádání* DiLO je extenze LO o axiomy existence *bezprostředního předchůdce* a *bezprostředního následníka*, též *axiom diskrétnosti* uspořádání:

$$(\forall x)(\exists y)(y \leq x \,\&\, y \neq x \,\&\, (\forall z)((y \leq z \leq x) \to (z = y \vee z = x))),$$
$$(\forall x)(\exists y)(x \leq y \,\&\, y \neq x \,\&\, (\forall z)((x \leq z \leq y) \to (z = y \vee z = x))).$$

Teorie DiLO$^\circ$ je rozšíření DiLO o binární predikátové symboly $<_n$ s $n \in \mathbb{N}$, definované takto:

$$x <_n y \ \leftrightarrow\ x \leq y \,\&\, \text{"mezi } x \text{ a } y \text{ existuje právě } n \text{ prvků"}.$$

Tedy $x <_0 y$ znamená, že "x je bezprostřední předchůdce y". Dále značíme $\langle \mathbb{Z}, \leq \rangle^\circ$ jednoznačnou expanzi $\langle \mathbb{Z}, \leq \rangle$ do modelu DiLO$^\circ$.

Grafy.

2.6.14. **Teorie** Gh **grafů (obyčejných neorientovaných bez smyček).**
Jazyk: $L^{gh} = \langle E \rangle$, E je binární relační symbol.
Axiomy: $xEy \to yEx$, $\neg(xEx)$

2.6.15. **Teorie** RGh **náhodného grafu.** Teorie RGh náhodného grafu je teorie grafů obohacená o axiom $(\exists x, y)(x \neq y)$ a schema $\{\psi_n;\ 0 < n \in \mathbb{N}\}$, kde ψ_n je uzávěr formule

$$\bigwedge_{i,j<n} x_i \neq y_j \to (\exists z) \bigwedge_{i<n} (E(x_i, z) \,\&\, \neg E(y_i, z)). \tag{2.17}$$

Modelem teorie RGh je nekonečný graf takový, že pro každé dvě konečné disjunktní množiny X, Y jeho nějakých vrcholů existuje vrchol z spojený s každým vrcholem z X hranou a nespojený s žádným vrcholem z Y hranou. Takový spočetný graf se také nazývá *náhodný*.

Algebraické teorie.

2.6.16. **Teorie grup. Teorie Abelových grup** AG**, teorie** AG_0**,** DAG_0**.**

Jazyk: $L^g = \langle +, -, 0\rangle$, $+$ je binární funkční symbol, $-$ unární funkční symbol, 0 je konstantní symbol.

Axiomy: $x + (y + z) = (x + y) + z$ (asociativita $+$)
$0 + x = x = x + 0$ (0 je (oboustranně) neutrální prvek)
$x + (-x) = 0 = (-x) + x$ ($-x$ je (oboustranně) inverzní prvek k x)

Pro term t a $n = 0$ resp. $n = 1$ resp. $1 < n \in \mathbb{N}$ značí nt term

$$0, \text{ resp. } t \text{ resp. } (\cdots((t + t) + t) + \cdots + t) \text{ s } + \text{ aplikovaným } (n - 1)\text{-krát.}$$

Teorie grup se často bere v *multiplikativním* jazyce $L^{\dot g} = \langle \cdot, ^{-1}, 1\rangle$ izomorfním s L^g.

Přidáme-li k teorii grup *axiom komutativity* $x + y = y + x$, získáme *teorii Abelových grup* AG.

Teorie AG_0 *Abelových grup bez torze* je rozšíření teorie AG Abelových grup o *schema beztorznosti*:

$$mx = 0 \to x = 0, \qquad 0 < m \in \mathbb{N}.$$

Teorie DAG_0 *netriviálních divisibilních Abelových grup bez torze* je rozšíření AG_0 o axiom netriviálnosti $(\exists x)(x \neq 0)$ a *schema divisibility*:

$$(\exists y)(my = x), \qquad 0 < m \in \mathbb{N}.$$

Poznamenejme, že teorie v jazyce $\langle + \rangle$, kde $+$ je binární funkční symbol, s axiomem $x+(y+z) = (x + y) + z$ (asociativita $+$), se nazývá **teorie pologrup**, a teorie v jazyce $\langle +, 0\rangle$, kde $+$ je binární funkční symbol, 0 konstantní symbol, s axiomy $x + (y + z) = (x + y) + z$ (asociativita $+$), $0 + x = x = x + 0$ (0 je (oboustranný) neutrální prvek), se nazývá **teorie monoidů**.

2.6.17. **Teorie** OAG **uspořádaných Abelových grup** je teorie v jazyce grup rozšířeném o binární predikátový symbol $<$; její axiomatika je rozšíření teorie Abelových grup o následující axiomy ostrého lineárního uspořádání a izotonie:

$$< \text{ je ostré lineární uspořádání}, \qquad x < y \to x + z < y + z \text{ (izotonie).}$$

2.6.18. **Teorie okruhů.**

Jazyk: $L^r = \langle +, -, \cdot, 0, 1\rangle$, $+, \cdot$ jsou binární funkční symboly, $-$ je unární funkční symbol, $0, 1$ jsou konstantní symboly.

Axiomy: teorie Abelových grup v jazyce $\langle +, -, 0\rangle$,
$1 \cdot x = x \;\&\; x \cdot 1 = x$ (1 je jednotka)
$x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (asociativita $\cdot$)
$x \cdot (y + z) = x \cdot y + x \cdot z$, $(x + y) \cdot z = x \cdot z + y \cdot z$ (distributivita).

Přidáme-li k teorii okruhů axiom komutativity pro $\cdot$, získáme *teorii komutativních okruhů*.

V teorii okruhů platí $-(xy) = (-x)y$, $(-1)x = -x$. Modely teorie okruhů jsou okruhy. Podstruktura okruhu je okruh.

2.6.19. **Teorie oborů integrity** je teorie komutativních okruhů, rozšířená o axiomy

$$0 \neq 1,\ (x \neq 0 \;\&\; y \neq 0) \to x \cdot y \neq 0 \text{ (neexistence dělitelů nuly).}$$

Místo axiomu neexistence dělitelů nuly je možné ekvivalentně vzít axiom krácení:

$$(xy = xz \;\&\; x \neq 0) \to y = z.$$

Nenulové prvky komutativního okruhu, jejichž součin je nula, se nazývají *dělitelé nuly*. Netriviální komutativní okruh je tedy oborem integrity, právě když neobsahuje dělitelé nuly.

Obor integrity celých čísel $\mathbb{Z}$ je množina celých čísel s kanonickými operacemi sčítání, opačnosti a násobení a s 0 a 1 jakožto jejich neutrálními elementy. Komutativní okruh $\mathbb{Z} \times \mathbb{Z}$ (operace na dvojicích se berou po složkách) není obor integrity, neboť $\langle 0, 1\rangle, \langle 1, 0\rangle$ jsou v něm dělitele nuly $\langle 0, 0\rangle$. Komutativní okruh ${}^{\mathbb{R}}\mathbb{R}$ s operacemi definovanými po složkách není obor integrity, neboť jeho prvky $f(x) = |x| + x, g(x) = |x| - x$ jsou v něm dělitelé nuly.

2.6.20. **Teorie uspořádaných oborů integrity** má jazyk uspořádaných okruhů $\langle +, -, \cdot, 0, 1, < \rangle$ a je rozšířením teorie oborů integrity o $0 < 1$ a axiomy ostrého lineárního uspořádání a izotonie:

$$< \text{ je ostré lineární uspořádání}, \quad x < y \to x + z < y + z, \quad x < y \,\&\, 0 < z \to x \cdot z < y \cdot z. \quad (2.18)$$

Když $x < 0$ resp. $0 < x$, říkáme, že x je *záporné* resp. *kladné*. Dále definujeme

$$|x| = z \quad \leftrightarrow \quad (z = x \,\&\, 0 \leq x) \vee (z = -x \,\&\, x < 0).$$

2.6.21. **Teorie těles** FL**,** FL_p**,** FL_0**.**
Teorii těles FL získáme tak, že přidáme k teorii komutativních okruhů axiomy

$0 \neq 1$ (netrivialita),
$x \neq 0 \to (\exists y)(x \cdot y = 1)$ (existence inverzního prvku vůči $\cdot$).

Buď p prvočíslo. Extenze teorie těles o axiom $p1 = 0$ je teorie FL_p *těles charakteristiky* p.
Extenze teorie těles o schema $\{p1 \neq 0;\ p$ je prvočíslo$\}$ je teorie FL_0 *těles charakteristiky* 0.

2.6.22. **Teorie algebraicky uzavřených těles** ACF**,** ACF_p**.** Přidáme-li k teorii těles FL resp. FL_p s p rovným nule nebo prvočíslu axiomy

$$(\forall x_0, \ldots, x_{n-1})(\exists y)(x_0 + x_1 \cdot y + \cdots x_{n-1} \cdot y^{n-1} + y^n = 0), \quad n \geq 1 \text{ přirozené}, \qquad (2.19)$$

získáme teorii ACF resp. ACF_p *algebraicky uzavřených těles* resp. *algebraicky uzavřených těles charakteristiky* p. Axiomy (2.19) zaručují, že každý normovaný polynomiální term, stručně polynom, stupně $n \geq 1$ má kořen.

2.6.23. **Teorie uspořádaných těles** OFL je teorie v jazyce těles rozšířeném o binární predikátový symbol $<$ s axiomatikou rozšiřující teorii těles o $0 < 1$, axiomy ostrého uspořádání a izotonie (2.18). Teorie uspořádaných těles dokazuje, jsou-li $m < n$ přirozená nenulová,

$$0 < n1, \qquad m1 < n1 \to m = n, \quad x < y \leftrightarrow 0 < y + (-x).$$

Tedy OFL rozšiřuje FL_0.

Prvek a uspořádaného tělesa F je *kladný* resp. *záporný*, platí-li $0 <^F a$ resp $a <^F 0$. Uspořádané těleso F se nazývá **archimedovské** nebo **archimedovsky uspořádané**, jestliže pro každé dva jeho kladné prvky a, b existuje přirozené číslo n tak, že $na > b$.

Buď F uspořádané těleso. Pak platí: $F_0 = \{m1/n1;\ m \text{ je celé}, 0 < n \text{ přirozené}\}$ je nejmenší podtěleso F a je izomorfní s uspořádaným tělesem racionálních čísel. Je-li navíc F archimedovské, je množina F_0 hustá v uspořádání F a pro $a \in F$ je $a = \sup\{b \in F_0;\ b \leq a\}$. Dále pro archimedovské těleso F a $a, b \in F$ platí

$$0 < a \to (\exists n \in \mathbb{N} - \{0\})(1/n1 < a), \qquad a \neq b \to (\exists n \in \mathbb{N} - \{0\})(1/n1 < |a - b|).$$

2.6.24. **Teorie (levých)** R**-modulů nad okruhem** R**.**

Jazyk: $L^{m,R} = \langle +, -, 0, \underline{r} \rangle_{r \in R}$, $+$ je binární funkční symbol, $-$ unární funkční symbol, 0 je konstantní symbol, $\underline{r}$ je unární funkční symbol.

Axiomy: axiomy teorie Abelových grup v aditivním jazyce $\langle +, -, 0 \rangle$,
$\underline{r}(x + y) = \underline{r}(x) + \underline{r}(y)$, $\underline{(r +^R s)}(x) = \underline{r}(x) + \underline{s}(x)$, kde $r, s \in R$,
$\underline{(r \cdot^R s)}(x) = \underline{r}(\underline{s}(x))$, $\underline{1^R}(x) = x$, kde $r, s \in R$.

Term $\underline{r}(x)$ symbolicky reprezentuje násobek skalárem r a zapisuje se zpravidla jako rx. Index ^{R} se často vynechává. V teorii R-modulů platí:

$$0x = 0, \quad (-1)x = -x.$$

Prvá rovnost plyne takto: $x = 1x = (1 + 0)x = x + 0x$; jediné y splňuje $x + y = x$, tedy $0x = 0$. Druhá takto: $x + (-1)x = 1x + (-1)x = 0x = 0$ a odtud $(-1)x = -x$.

Modely teorie levých R-modulů jsou levé R-moduly. R-modul obsahující jediný prvek 0 je *triviální*; jinak je *netriviální*.

2.6.25. **Teorie vektorových prostorů nad tělesem** F je teorie F-modulů nad tělesem F. Modely teorie vektorových prostorů nad tělesem F jsou vektorové prostory nad F.

VS(F) značí teorii vektorových prostorů nad tělesem F, VS(F,∞) navíc nekonečných.

Demonstrační teorie.

2.6.26. **Čistá teorie** CE_κ **konstant.**
Jazyk: $L^{\mathrm{CE}_\kappa} = \langle c_i \rangle_{i\in\kappa}$ s rovností, c_i jsou konstantní symboly.
Axiomy: $\emptyset$
Speciálně CE_0 je teorie PE čisté rovnosti.

Teorie $\mathrm{CE}_\kappa(\infty)$ **konstant s nekonečně prvky.**
Jazyk: $L^{\mathrm{CE}_\kappa} = \langle c_i \rangle_{i\in\kappa}$ s rovností, c_i jsou konstantní symboly.
Axiomy: Existuje nekonečně prvků.

Teorie $\mathrm{C'E}_\kappa$ **různých konstant.**
Jazyk: $L^{\mathrm{C'E}_\kappa} = \langle c_i \rangle_{i\in\kappa}$ s rovností, c_i jsou konstantní symboly.
Axiomy: $c_i \neq c_j$, $i \neq j$ a $i,j \in \kappa$

2.6.27. **Čistá teorie** UE **jedné unární relace.**
Jazyk: $L^{\mathrm{UE}} = \langle U \rangle$ s rovností, U je unární relační symbol.
Axiomy: $\emptyset$
Teorie $\mathrm{UE}(m,n)$ **jedné unární relace pro** $m,n \in \mathbb{N}\cup\{\infty\}$**,** $m+n \neq 0$**.**
Jazyk: $L^{\mathrm{UE}} = \langle U \rangle$ s rovností, U je unární relační symbol.
Axiomy: Existuje právě m prvků splňujících U a
existuje právě n prvků splňujících $\neg U$

2.6.28. **Teorie** UFO^m **a** UFO_m**.**

Teorie UFO^m **jedné unární funkce s** m**-cykly,** $0 < m \in \mathbb{N}$**.**
Jazyk: $L^{\mathrm{UFO}} = \langle F \rangle$ s rovností, F je unární funkční symbol.
Pro $m \in \mathbb{N}$ je $F^m(x)$ term $F\cdots F(x)$, F aplikováno m-krát; $F^0(x)$ je x.
Axiomy: $F^m(x) = x$, $F^i(x) \neq x$ pro $0 < i < m$.
UFO^1 má tedy axiomatiku $F(x) = x$.

Teorie UFO_m
Jazyk: $L^{\mathrm{UFO}} = \langle F \rangle$ s rovností, F je unární funkční symbol.
Pro $m \in \mathbb{N}$ je $F^m(x)$ term $F\cdots F(x)$, F aplikováno m-krát; $F^0(x)$ je x.
Axiomy: $F^m(x) = x$.

2.6.29. Suma $\sum_I \langle A_i, \mathcal{F}_i \rangle$. Cykly.

1. Buď $\langle \mathcal{A}_i \rangle_{i\in I}$ neprázdný soubor struktur pro jazyk $L = \langle \mathcal{F} \rangle$, kde $\mathcal{F}$ je množina unárních funkčních symbolů, $\mathcal{A}_i = \langle A_i, \mathcal{F}_i \rangle$. Suma $\sum_I \mathcal{A}_i$ je struktura $\langle A, \mathcal{F}^A \rangle$, kde

$$A = \bigcup_I (\{i\} \times A_i), \qquad F(\langle i,a \rangle) = \langle i, F^{A_i}(a) \rangle \text{ pro } F \in \mathcal{F},\ i \in I,\ a \in A_i.$$

Místo $\sum_{\{i,j\}} \langle \mathcal{A}_i, \mathcal{A}_j \rangle$ se píše také $\mathcal{A}_i + \mathcal{A}_j$.

2. Buď $0 < m \in \mathbb{N}$, I neprázdná množina. Struktura m-*cyklus* resp. (m,I)-*cykly* je struktura

$$\underline{\mathbb{O}}^m = \langle \mathbb{Z}_m, \mathrm{S}/m \rangle \quad \text{resp.} \quad \underline{\mathbb{O}}^m_I = \textstyle\sum_I \underline{\mathbb{O}}^m.$$

Přitom S/m značí přičítání jedničky modulo m; připouštíme i $m = 1$. Dále $\mathbb{O}^m$ resp. $\mathbb{O}^m_I$ je univerzum $\underline{\mathbb{O}}^m$ resp. $\underline{\mathbb{O}}^m_I$.

Speciálně:

$$\underline{\mathbb{O}}^1 \cong \langle 1, \mathrm{Id}_1 \rangle, \qquad \underline{\mathbb{K}}^m_n = \langle \mathbb{N}, \mathrm{S} \rangle + \underline{\mathbb{O}}^m_{\{1,\dots,n\}}, \qquad \underline{\mathbb{K}}^m_\omega = \langle \mathbb{N}, \mathrm{S} \rangle + \underline{\mathbb{O}}^m_{\mathbb{N}-\{0\}}.$$

TVRZENÍ 2.6.30. (O modelech UFO^m.)

1) *Pro* $0 < m \in \mathbb{N}$ *je každý model* $\mathcal{A} = \langle A, F\rangle$ *teorie* UFO^m *izomorfní s* $\underline{\mathbb{O}}^m_I$, *kde* $I = A/E$ *a* E *je ekvivalence na* A *s* m*-prvkovými faktory* $\{F^i(a);\ i < m\}$, $a \in A$.

   Je-li A *konečné, je* $|A| = km$ *pro nějaké nenulové* $k \in \mathbb{N}$.
2) $\underline{\mathbb{O}}^m \models$ UFO^m.

Důkaz. Pro faktor u ekvivalence E je $\mathcal{A}{\restriction} u \cong \underline{\mathbb{O}}^m$ via jisté h_u; izomorfizmus $\mathcal{A}$ a $\underline{\mathbb{O}}^m_I$ získáme „spojením“ izomorfizmů h_u. Zbytek tvrzení je jasný. □

Teorie bijekcí.

2.6.31. **Teorie** BI **parciální bijekce.**

Jazyk: $L^{\mathrm{BI}} = \langle U, P\rangle$ s rovností, U resp. P je unární resp. binární relační symbol.

Axiomy: $P(x,y)\ \&\ P(x',y) \to x = x'$, $\quad P(x,y)\ \&\ P(x',y')\ \&\ x \neq x' \to y \neq y'$,

$P(x,y) \to U(x)\ \&\ \neg U(y)$, $\quad U(x) \to (\exists y)P(x,y)$, $\quad U(y) \to (\exists x)P(x,y)$.

Pro $0 < n \in \mathbb{N}$ označme

$$\mathrm{BI}(n) \quad \text{resp.} \quad \mathrm{BI}(\infty)$$

extenzi BI o axiom „existuje právě n prvků“ resp. o schema „existuje nekonečně prvků“.

Zřejmě L^{BI}-struktura $\langle A, U, P\rangle$ je model BI, právě když je P bijekce U na $A - U$. Dále teorie BI nemá model konečné liché velikosti a pro ostatní velikosti má až na izomorfizmus právě jeden model této velikosti.

2.7 Poznámky.

Kapitola 3

Výroková logika

Na výrokovou logiku můžeme hledět jako na fragment predikátové logiky s jazykem $L^{\mathbb{P}}$ bez rovnosti, který má jako mimologické symboly jen nulární relační symboly, tvořící neprázdnou množinu $\mathbb{P}$ tzv. prvovýroků či výrokových proměnných – viz 2.2.16.

Konvence.
Znamená-li značka Z nějakou predikci, operaci, množinu či třídu, vztahující se k výrokovému jazyku $\mathbb{P}$, můžeme psát místo ní obšírněji $Z_{\mathbb{P}}$, abychom zachytili souvislost s $\mathbb{P}$. Např. VF značí množinu všech výroků, $\mathrm{VF}_{\mathbb{P}}$ obšírněji množinu všech výroků jazyka $\mathbb{P}$. Naopak pro zjednodušení zápisů index $\mathbb{P}$ vynecháváme, nevede-li to ovšem k nedorozumění.

3.1 Základní syntax.

Pojem výrokového jazyka, výroku čili výrokové formule, teorie a dedukce je uveden v 2.2.16.

ZNAČENÍ. Symbol $\mathrm{var}(\varphi)$ značí množinu všech prvovýroků vyskytujících se ve výroku φ.

3.1.1. Zrekapitulujme stručně některé základní pojmy syntaxe jazyka $\mathbb{P}$; jsou identické s „predikátovými“ pro jazyk $L^{\mathbb{P}}$. Buď dále T nějaká $\mathbb{P}$-teorie.

- Spojky $\neg, \vee, \&, \leftrightarrow$ případně další se zavádějí jako zkratky stejně jako v predikátové logice.
- $\mathrm{Thm}_{\mathbb{P}}(T)$, stručněji $\mathrm{Thm}(T)$, je množina všech v T dokazatelných výroků. T je sporná, když $\mathrm{Thm}_{\mathbb{P}}(T) = \mathrm{VF}_{\mathbb{P}}$; jinak je bezesporná. Pojem vyvratitelné a nezávislé výrokové formule je týž, jako v predikátové logice pro formule. T je kompletní, je-li bezesporná a každý její výrok je v ní dokazatelný či vyvratitelný (protože jde o sentence $L^{\mathbb{P}}$).
- Teorie T' je extenze $\mathbb{P}$-teorie T [jednoduchá/konzervativní], když $L(T) \subseteq L(T')$ a $\mathrm{Thm}(T) \subseteq \mathrm{Thm}(T')$ [a $L(T') = L(T)/\mathrm{Thm}(T) = \mathrm{Thm}(T') \cap \mathrm{VF}_{\mathbb{P}}$]. T' je ekvivalentní s T, je-li T' extenzí T a naopak.

3.1.2. **Výroky $\top$, $\bot$. Klauzule a elementární konjunkce.** DNF, CNF. **Struktura výroků.**
1. *Pravdivý* výrok $\top$ specifikujeme jako $p \to p$, *lživý* výrok $\bot$ jako $\neg(p \to p)$; na konkrétní volbě p nezáleží. Mluvíme o nich též jako o nulárních logických spojkách či výrokových konstantách.
 – *Literál* je prvovýrok nebo negace prvovýroku.
 – Disjunkce literálů se nazývá *klauzule*, konjunkce literálů též *elementární konjunkce*.
 – Výrok je v *disjunktivně* resp. *konjunktivně normálním tvaru*, stručněji v DNF resp. v CNF, je-li to disjunkce konjunkcí literálů resp. konjunkce disjunkcí literálů.

2. *Struktura výroků* nad $\mathbb{P}$ je struktura $\underline{\mathrm{VF}}_{\mathbb{P}} = \langle \mathrm{VF}_{\mathbb{P}}, \neg, \vee, \&, \bot, \top \rangle$ pro jazyk Booleových algeber; logické spojky chápeme jako operace, $\bot$ a $\top$ jako konstantu 0 a 1. Operace $\vee$ není komutativní, neboť výrok $p_0 \vee p_1$ není jako výraz (tice) roven $p_1 \vee p_0$; podobně je tomu s operací $\&$.

ZNAČENÍ 3.1.3. Pro výrok φ, n-tici výroků $s = \langle \varphi_0, \ldots, \varphi_{n-1} \rangle$ a $\sigma : n \to 2$ symbol s^σ značí $\langle \varphi_0^{\sigma(0)}, \ldots, \varphi_{n-1}^{\sigma(n-1)} \rangle$ a dále

$$\varphi^1 \text{ je } \varphi, \qquad \varphi^0 \text{ je } \neg\varphi,$$

$$\bigwedge s \text{ je } \varphi_0 \,\&\, \cdots \,\&\, \varphi_{n-1}, \qquad \bigwedge \emptyset \text{ je } \top, \qquad \bigvee s \text{ je } \varphi_0 \vee \cdots \vee \varphi_{n-1}, \qquad \bigvee \emptyset \text{ je } \bot.$$

Je-li s konečná množina výroků, je $\bigwedge s$ rovno $\bigwedge s'$ a $\bigvee s$ rovno $\bigvee s'$ pro nějaké prosté očíslování s' množiny s.

Elementární teorie dokazování.

TVRZENÍ 3.1.4. *Buďte φ, ψ formule výrokové teorie T. Pak platí:*

1) $\vdash \varphi \to \varphi$.

2) (Věta o dedukci.) $\quad T, \psi \vdash \varphi \Leftrightarrow T \vdash \psi \to \varphi$.

Důkaz. 1) Nechť ψ je $\varphi \to \varphi$; pak jsou výrokovými axiomy formule $\varphi \to \psi$, $\varphi \to (\psi \to \varphi)$, $\varphi \to (\psi \to \varphi) \to ((\varphi \to \psi) \to (\varphi \to \varphi))$. Užitím modus ponens tedy $\vdash (\varphi \to \psi) \to (\varphi \to \varphi)$ a opět dle modus ponens $\vdash \varphi \to \varphi$.

2) Implikace $\Leftarrow$ plyne ihned užitím modus ponens. Buď nyní $T, \psi \vdash \varphi$; dokážeme $T \vdash \psi \to \varphi$, a to indukcí na teorémech teorie T, ψ. Buď φ axiom teorie T, ψ. Je-li φ rovno ψ, je $T \vdash \psi \to \varphi$ dle 1). Pro $\varphi \in T \cup \mathrm{LAx}$ plyne z (PL1) užitím modus ponens žádané $T \vdash \psi \to \varphi$. Buď konečně φ odvozeno pomocí modus ponens z χ, $\chi \to \varphi$ a pro teorémy χ, $\chi \to \varphi$ teorie T, ψ nechť to platí. Odtud a z výrokového axiomu $(\psi \to (\chi \to \varphi)) \to ((\psi \to \chi) \to (\psi \to \varphi))$ užitím modus ponens získáme $T \vdash \psi \to \varphi$. $\square$

LEMMA 3.1.5. *Pro výroky φ, ψ platí:*

a)	$\vdash \neg\varphi \to (\varphi \to \psi)$,	$\{\varphi, \neg\varphi\} \vdash \psi$	c)	$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$
	$\vdash \varphi \to (\neg\varphi \to \psi)$		d)	$\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$
b)	$\vdash \neg\neg\varphi \to \varphi$,	$\vdash \varphi \to \neg\neg\varphi$	e)	$\vdash (\neg\varphi \to \varphi) \to \varphi$

Důkaz. a) $\vdash \neg\varphi \to (\neg\psi \to \neg\varphi)$ dle (PL1), z věty o dedukci $\neg\varphi \vdash \neg\psi \to \neg\varphi$. Odtud, užitím (PL3) a modus ponens získáme $\neg\varphi \vdash \varphi \to \psi$ a užitím věty o dedukci prvý dokazovaný vztah a zbývající dva z něj užitím věty o dedukci.

b) $\neg\neg\varphi \vdash \neg\varphi \to \neg\neg\neg\varphi$ dle a) a věty o dedukci, tedy $\neg\neg\varphi \vdash \neg\neg\varphi \to \varphi$ užitím (PL3), tedy $\neg\neg\varphi \vdash \varphi$ a konečně $\vdash \neg\neg\varphi \to \varphi$. Odtud a užitím (PL3) plyne i $\vdash \varphi \to \neg\neg\varphi$.

c) $\neg\neg\varphi, \varphi \to \psi \vdash \psi, \neg\neg\psi$ dle b) a modus ponens, tedy dle věty o dedukci $\varphi \to \psi \vdash \neg\neg\varphi \to \neg\neg\psi$, dle (PL3), modus ponens a díky větě o dedukci $\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$.

d) Je $\varphi \vdash (\varphi \to \psi) \to \psi$, dle c) $\varphi \vdash \neg\psi \to \neg(\varphi \to \psi)$ a věta o dedukci dá žádaný vztah.

e) $\vdash \neg\varphi \to (\neg\varphi \to \neg(\neg\varphi \to \varphi))$ dle d), $\neg\varphi \vdash \neg(\neg\varphi \to \varphi)$ pomocí věty o dedukci, odtud $\vdash (\neg\varphi \to \varphi) \to \varphi$ užitím (PL3) a modus ponens. $\square$

TVRZENÍ 3.1.6. *Buďte φ, ψ formule teorie T.*

1) *Teorie T je sporná, právě když je v ní dokazatelný spor.*

2) (Důkaz sporem.) *$T, \neg\varphi$ je sporná $\Leftrightarrow$ $T \vdash \varphi$.*

Důkaz. 1) Je-li φ spor, tj. $\vdash \neg\varphi$, a $T \vdash \varphi$, plyne z 3.1.5, a), že $T \vdash \psi$ pro jakýkoli výrok ψ.

2) Implikace $\Rightarrow$: $T, \neg\varphi$ sporná implikuje $T \vdash \neg\varphi \to \varphi$ užitím věty o dedukci. Pak $T \vdash \varphi$ užitím 3.1.5, e). Implikace $\Leftarrow$ plyne z 3.1.5, a). $\square$

3.2 Základní sémantika.

Modely a pravdivost. Korektnost.

Základní sémantika je exponována v 2.2.16, algebry výroků pak v 2.4.5.

3.2.1. Zrekapitulujme některé základní pojmy sémantiky. Buď T nějaká výroková $\mathbb{P}$-teorie, φ výrok nad $\mathbb{P}$, $v \in {}^{\mathbb{P}}2$ (ohodnocení prvovýroků čili model jazyka $\mathbb{P}$).

- $\mathsf{M}_{\mathbb{P}} = {}^{\mathbb{P}}2\,(= \{v;\, v : \mathbb{P} \to 2\})$ je množina všech modelů jazyka $\mathbb{P}$, $v \models \varphi \Leftrightarrow \overline{v}(\varphi) = 1$.
- – $v \models T \Leftrightarrow v \models \chi$ pro každé $\chi \in T$, $T \models \varphi \Leftrightarrow v \models \varphi$ pro každé $v \models T$; $\models \varphi$ značí $\emptyset \models \varphi$.
  – $\mathsf{M}_{\mathbb{P}}(T) = \{v \in {}^{\mathbb{P}}2;\, v \models T\}$, $\mathrm{Tru}_{\mathbb{P}}(T) = \{\varphi;\, T \models \varphi\}$.
  – φ je tautologie, když $v \models \varphi$ pro každé $v \in {}^{\mathbb{P}}2$, čili když $\models \varphi$.
- Sémantická varianta syntakticky definovaného pojmu se získá nahrazením $\vdash$ symbolem $\models$ v příslušné definici. Jde především o pojmy: nezávislá formule, (beze)sporná teorie, kompletní teorie, extenze (jednoduchá, kompletní) a ekvivalence teorií.
- Algebra výroků teorie T je Booleova algebra $\underline{\mathrm{AV}}_{\mathbb{P}}(T) = \underline{\mathrm{VF}}_{\mathbb{P}}/{\approx_T}$, kde $\varphi \approx_T \psi \Leftrightarrow T \models \varphi \leftrightarrow \psi$.

ZNAČENÍ. $\mathsf{M}_{\mathbb{P}}(T \cup \{\varphi_0, \dots, \varphi_{k-1}\})$ značíme $\mathsf{M}_{\mathbb{P}}(T, \varphi_0, \dots, \varphi_{k-1})$; nepíšeme T, když je prázdné. $-\mathsf{M}_{\mathbb{P}}(T)$ značí ${}^{\mathbb{P}}2 - \mathsf{M}_{\mathbb{P}}(T)$; je to *komplement* třídy $\mathsf{M}_{\mathbb{P}}(T)$.

TVRZENÍ 3.2.2.

1) (O korektnosti.) *$T \vdash \varphi \Rightarrow T \models \varphi$ pro každou formuli φ teorie T.*
2) *Má-li teorie model, je bezesporná.*
3) *Teorie je kompletní sémanticky, právě když má právě jeden model.*

Důkaz. 1) Indukcí na teorémech. Logický a mimologický axiom teorie T je v T pravdivý. Jsou-li φ, $\varphi \to \psi$ pravdivé v T, je takové i ψ. 2) φ a $\neg\varphi$ nejsou zároveň platné v žádném modelu. 3) Má-li teorie T dva modely, lišící se v prvovýroku p, je p nezávislý výrok T sémanticky. Má-li teorie T právě jeden model, je evidentně kompletní sémanticky. □

Níže dokážeme i opačnou implikaci z tvrzení o korektnosti a získáme tak zásadní větu o kompletnosti čili úplnosti výrokové logiky: $T \vdash \varphi \Leftrightarrow T \models \varphi$ pro každý výrok teorie T. Její důkaz se opírá o větu o existenci modelu bezesporné teorie. Vše je formulováno v 3.3.2.

Vlastnosti pravdivosti.

Pro výrokovou teorii T v jazyce $\mathbb{P}$, její modely a formule, platí tvrzení 2.2.19 o vlastnostech $\mathrm{Tru}(T)$ a tvrzení 2.2.13 a 2.2.14 o sémantice logických spojek. Protože výroky nad $\mathbb{P}$ jsou sentence jazyka $L^{\mathbb{P}}$, lze některé implikace $\Rightarrow$ v tvrzení o sémantice spojek z 2.2.13 obrátit. Speciálně pro teorii T a její výroky φ, ψ máme:

$$T \models \varphi \to \psi \Leftrightarrow \mathsf{M}_{\mathbb{P}}(T, \varphi) \subseteq \mathsf{M}_{\mathbb{P}}(T, \psi), \qquad T \models \varphi \leftrightarrow \psi \Leftrightarrow \mathsf{M}_{\mathbb{P}}(T, \varphi) = \mathsf{M}_{\mathbb{P}}(T, \psi). \tag{3.1}$$

Dále platí tvrzení 2.2.20 o ekvivalenci sémanticky.

Normální tvary. Množinová reprezentace. CNF-algoritmus.

TVRZENÍ 3.2.3. (Vlastnosti ohodnocení výroků. Normální tvary.) *Buďte $v \in {}^{\mathbb{P}}2$, $\varphi, \psi \in \mathrm{VF}_{\mathbb{P}}$.*

1) a) *Pro $v \in {}^{\mathbb{P}}2$ závisí $v(\varphi)$ jen na hodnotách v na množině* $\mathrm{var}(\varphi)$.
   b) *$v(\varphi \diamond \psi) = v(\varphi) \diamond_1 v(\psi)$ pro $\diamond$ rovno $\vee, \wedge, \leftrightarrow$. ($\diamond_1$ je příslušná operace v algebře $\underline{2}$.)*
2) *Buď $\mathbb{P}$ konečné, $K \subseteq {}^{\mathbb{P}}2$; označme $-K = {}^{\mathbb{P}}2 - K$. Pak*
$$\mathsf{M}_{\mathbb{P}}(\textstyle\bigvee_{w \in K} \bigwedge_{p \in \mathbb{P}} p^{w(p)}) = K = \mathsf{M}_{\mathbb{P}}(\bigwedge_{w \in -K} \bigvee_{p \in \mathbb{P}} p^{-_1 w(p)}).$$
3) *Formule φ je ekvivalentní sémanticky formuli jak v disjunktivně normálním tvaru, tak formuli v konjunktivně normálním tvaru.*

Důkaz. 1) a) se dokáže snadno indukcí na výrocích. b) plyne ihned z definic.

2) Pro $v, w \in {}^{\mathbb{P}}2$ máme $v(p^{w(p)}) = 1 \Leftrightarrow v(p) = w(p)$. Tedy $v(\bigwedge_{p \in \mathbb{P}} p^{w(p)}) = 1 \Leftrightarrow v = w$. Odtud a užitím 1) b): $v(\bigvee_{\dots} \bigwedge_{\dots} p^{w(p)}) = 1 \Leftrightarrow v \in K$. Podobně $v(\bigvee_{p \in \mathbb{P}} p^{-_1 w(p)}) = 1 \Leftrightarrow v \neq w$ a tedy $v(\bigwedge_{\dots} \bigvee_{\dots} p^{-_1 w(p)}) = 1 \Leftrightarrow v \notin -K \Leftrightarrow v \in K$.

3) Pro $\mathbb{P}$ konečné to dává 2) s $K = \mathsf{M}_{\mathbb{P}}(\varphi)$. Díky 1) a) to platí pro každé $\mathbb{P}$. $\square$

3.2.4. Množinová reprezentace formulí v normálních tvarech.

Pro klauzuli χ a ohodnocení prvovýroků v nezávisí $v(\chi)$ na tom, kolikrát se v χ nějaký literál λ jako disjunkt vyskytuje. Proto můžeme chápat χ v *množinové reprezentaci* $^\circ\chi$, což je množina všech disjunktů z χ. Formální disjunkci $\bigvee\emptyset$ chápeme jako spor a značíme $\bot$. Formálně $\bigvee\emptyset$ nemá model, což přesně souhlasí s tím, že $\bot$ nemá model. Pro $\bot$ je množinová reprezentace $^\circ\bot = \emptyset$. Pro formuli φ v CNF buď její množinová reprezentace $^\circ\varphi = \{^\circ\chi;\ \chi \text{ je konjunkt } \varphi\}$. Zcela analogicky můžeme mluvit o množinové reprezentaci elementárních konjunkcí a formulí v DNF.

PŘÍKLAD. Klauzuli $\neg p \vee q \vee \neg r \vee \neg p$ zapíšeme v množinové reprezentaci jako $\{\neg p, q, \neg r\}$, podobně $(\neg p \vee r) \mathbin{\&} \neg r \mathbin{\&} (p \vee \neg r)$ jako $\{\{\neg p, r\}, \{\neg r\}, \{p, \neg r\}\}$.

3.2.5. CNF-algoritmus.

CNF1 Měň, dokud to jde, podformuli tvaru $(\varphi \to \psi)$ na $(\neg\varphi \vee \psi)$,

$$\varphi \leftrightarrow \psi \text{ na } (\neg\varphi \vee \psi) \mathbin{\&} (\neg\psi \vee \varphi), \qquad \varphi \mathbin{\dot-} \psi \text{ na } (\neg\varphi \mathbin{\&} \psi) \vee (\neg\psi \mathbin{\&} \varphi);$$

pak proveď CNF2.

CNF2 Měň, dokud to jde, podformuli

$$\neg\neg\varphi \text{ na } \varphi, \qquad \neg(\varphi \mathbin{\&} \psi) \text{ na } (\neg\varphi \vee \neg\psi), \qquad \neg(\varphi \vee \psi) \text{ na } (\neg\varphi \mathbin{\&} \neg\psi);$$

pak proveď CNF3.

CNF3 Měň, dokud to jde, podformuli tvaru

$$(\varphi \vee (\psi \mathbin{\&} \chi)) \text{ či } ((\psi \mathbin{\&} \chi) \vee \varphi) \quad \text{na} \quad ((\varphi \vee \psi) \mathbin{\&} (\varphi \vee \chi)).$$

TVRZENÍ 3.2.6. CNF-*algoritmus aplikovaný na výrok* φ *dává výrok v* CNF *a ekvivalentní s* φ *sémanticky.*

Důkaz. Algoritmus dává výrok φ' ekvivalentní s φ sémanticky, neboť dochází jen k nahrazování podformulí sémanticky ekvivalentními, a dále φ' obsahuje jen spojky $\neg, \vee, \&$. Indukcí dle délky formule φ' vzniklé CNF-algoritmem se dokáže, že to je formule v CNF. Pro délku 1 a 2 to platí. Proveďme indukční krok z n na $n+1$ s $n \geq 2$. Pak dle CNF2 není φ' tvaru $\neg(\psi)$ a je tedy tvaru $(\varphi_0 \diamond \varphi_1)$, kde $\diamond$ je buď $\&$ či $\vee$, φ_0, φ_1 vznikly CNF-algoritmem a mají délky nejvýše n, tedy jsou dle indukčního předpokladu v CNF. Je-li $\diamond$ spojka $\&$, φ' je v CNF. Je-li $\diamond$ spojka $\vee$, není ve φ_0, φ_1 spojka $\&$, neboť pak by díky CNF3 formule φ' byla konjunkce; tedy φ' je klauzule. $\square$

PŘÍKLAD 3.2.7. Pro formule $(p \vee q) \to (\neg q \mathbin{\&} r)$ dává CNF-algoritmus postupně:

$\neg(p \vee q) \vee (\neg q \mathbin{\&} r)$	dle CNF1
$(\neg p \mathbin{\&} \neg q) \vee (\neg q \mathbin{\&} r)$	dle CNF2
$((\neg p \mathbin{\&} \neg q) \vee \neg q) \mathbin{\&} ((\neg p \mathbin{\&} \neg q) \vee r)$	dle CNF3
$(\neg p \vee \neg q) \mathbin{\&} (\neg q \vee \neg q) \mathbin{\&} (\neg p \vee r) \mathbin{\&} (\neg q \vee r)$	dle CNF3

Algebra výroků a modelů výroků. Booleovské funkce.

3.2.8. Algebra výroků $\underline{\mathrm{AV}}_{\mathbb{P}}(T)$ teorie T v jazyce $\mathbb{P}$ je definována v 2.4.5.

Počítání v algebře výroků pomocí reprezentantů lze užít k nalézání sémantických ekvivalentů. Např.:

$$(p \to q) \mathbin{\&} q \approx (\neg p \vee q) \mathbin{\&} q \approx (\neg p \mathbin{\&} q) \vee (q \mathbin{\&} q) \approx (\neg p \mathbin{\&} q) \vee q \approx q.$$

1. $\approx$ plyne užitím tvrzení o sémantické ekvivalenci a díky $p \to q \approx \neg p \vee q$, 2. $\approx$ dává distributivní zákon, 3. $\approx$ idempotence, 4. $\approx$ absorbce. Získali jsme zároveň k formuli $(p \to q) \mathbin{\&} q$ sémantické ekvivalenty v konjunktivně normálním tvaru i v disjunktivně normálním tvaru.

Zřejmě platí:

$$\mathbb{P}\text{-teorie } T \text{ s modelem je kompletní sémanticky, právě když } \underline{\mathrm{AV}}_{\mathbb{P}}(T) \cong \underline{2}.$$

3.2.9. Algebra modelů výrokové teorie. Cantorova algebra.

Nechť T je $\mathbb{P}$-teorie s modelem. Podalgebra $\underline{\mathcal{P}}(\mathsf{M}_{\mathbb{P}}(T))$ s univerzem $\{\mathsf{M}_{\mathbb{P}}(T, \varphi);\ \varphi \in \mathrm{VF}_{\mathbb{P}}\}$ se nazývá *algebra modelů výroků teorie* T a značí se

$$\underline{\mathrm{AM}}_{\mathbb{P}}(T).$$

Je-li T prázdné, píšeme jen $\underline{\mathrm{AM}}_{\mathbb{P}}$. Tato algebra se také značí $\mathrm{CA}(\mathbb{P})$ a nazývá se *zobecněná Cantorova algebra nad* $\mathbb{P}$, je-li $\mathbb{P}$ spočetné, tak *Cantorova algebra nad* $\mathbb{P}$.

TVRZENÍ 3.2.10. (O algebře výroků a modelů výroků teorie.) *Nechť T je $\mathbb{P}$-teorie s modelem.*

1) $\underline{\mathrm{AV}}_{\mathbb{P}}(T) \cong \underline{\mathrm{AM}}_{\mathbb{P}}(T)$ *via* $h(\varphi/\approx_T) = \mathsf{M}_{\mathbb{P}}(T,\varphi)$ *s* $\varphi \in \mathrm{VF}_{\mathbb{P}}$.
Speciálně: $\underline{\mathrm{AV}}_{\mathbb{P}} \cong \mathrm{CA}(\mathbb{P})$.
2) *Buď* $\mathsf{M}_{\mathbb{P}}(T)$ *konečná m-prvková množina. Pak* $\underline{\mathrm{AM}}_{\mathbb{P}}(T) = \underline{\mathcal{P}}(\mathsf{M}_{\mathbb{P}}(T))$ *je* 2^m*-prvková algebra.*
Speciálně: Je-li $\mathbb{P}$ konečné, algebra $\underline{\mathrm{AM}}_{\mathbb{P}}$ je $2^{2^{|\mathbb{P}|}}$-prvková.
3) *Pro $\mathbb{P}$ nekonečné je $\mathrm{CA}(\mathbb{P})$ bezatomární Booleova algebra, mající velikost $|\mathbb{P}|$.*
4) *Buď $\mathbb{P}$ konečné. Nechť χ_v s $v \in \mathsf{M}_{\mathbb{P}}(T)$ je elementární konjunkce tvaru*

$$\bigwedge_{p\in\mathbb{P}} p^{v(p)}, \tag{3.2}$$

Pak $\mathsf{M}_{\mathbb{P}}(\chi_v)$ s $v \in \mathsf{M}_{\mathbb{P}}(T)$ jsou právě všechny atomy algebry $\underline{\mathrm{AM}}_{\mathbb{P}}(T)$.

Důsledek: Každý výrok φ nad $\mathbb{P}$ je v T ekvivalentní sémanticky disjunkci nějakých výroků z (3.2). Explicitně platí: $T \models \varphi \leftrightarrow \bigvee\{\chi_v;\, v \in \mathsf{M}_{\mathbb{P}}(T,\varphi)\}$; vpravo je formule v DNF.

Důkaz. 1) Je $\varphi \approx_T \psi \Leftrightarrow \mathsf{M}_{\mathbb{P}}(T,\varphi) = \mathsf{M}_{\mathbb{P}}(T,\psi)$, tedy je h izomorfizmus $\underline{\mathrm{AV}}_{\mathbb{P}}(T)$ a $\underline{\mathrm{AM}}_{\mathbb{P}}(T)$.

2) Platí, jak dokážeme níže: Buď $K \subseteq {}^{\mathbb{P}}2$ konečné. Pak pro každé $w \in K$ existuje φ_w tak, že

$$K \cap \mathsf{M}(\varphi_w) = \{w\}. \tag{3.3}$$

(Index $\mathbb{P}$ nepíšeme.) Odtud plyne: je-li $K \subseteq \mathsf{M}(T)$, tak pro $w \in K$ máme $K \cap \mathsf{M}(\varphi_w) = \{w\}$. Tudíž $\mathsf{M}(T, \bigwedge_{w\in K}\varphi_w) = \bigcup_{w\in K}\mathsf{M}(T,\varphi_w) = K$. Tedy každé $K \subseteq \mathsf{M}(T)$ je v algebře $\underline{\mathrm{AM}}(T)$.

Zbývá k $w \in K$ najít φ_w splňující (3.3). Pro $v \in K - \{w\}$ buď $p_v \in \mathbb{P}$ s $v(p_v) \neq w(p_v)$. Buď φ_w formule $\bigwedge_{v\in K-\{w\}} p_v^{-1v(p_v)}$. Máme pro $v \in K - \{w\}$:

$$0 = \overline{v}(p_v^{-1v(p_v)}) \neq \overline{w}(p_v^{-1v(p_v)}) = 1.$$

Tudíž pro $v \in K$ je $v \in \mathsf{M}(\varphi_w) \Leftrightarrow v = w$ a jsme hotovi.

Speciální tvrzení je důsledkem pro $T = \emptyset$, kdy máme $|\mathsf{M}_{\mathbb{P}}(T)| = 2^{|\mathbb{P}|}$.

3) Buď $\mathsf{M}_{\mathbb{P}}(\varphi) \neq \emptyset$ nenulový prvek v $\mathrm{CA}(\mathbb{P})$. Buď $p \in \mathbb{P} - \mathrm{var}(\varphi)$ pak $\emptyset \neq \mathsf{M}_{\mathbb{P}}(\varphi \,\&\, p) \subsetneq \mathsf{M}_{\mathbb{P}}(\varphi)$; tedy $\mathsf{M}_{\mathbb{P}}(\varphi)$ není atom. Protože výroků nad $\mathbb{P}$ je právě $|\mathbb{P}|$, je velikost $\mathrm{CA}(\mathbb{P})$ nejvýše $|\mathbb{P}|$. $\mathsf{M}_{\mathbb{P}}(p)$ s $p \in \mathbb{P}$ je $|\mathbb{P}|$ různých prvků algebry $\mathrm{CA}(\mathbb{P})$; tudíž $\mathrm{CA}(\mathbb{P})$ má právě $|\mathbb{P}|$ prvků.

4) Je $\mathsf{M}_{\mathbb{P}}(T,\chi_v) = \mathsf{M}_{\mathbb{P}}(\chi_v) = \{v\}$ a $\underline{\mathrm{AM}}_{\mathbb{P}}(T) = \underline{\mathcal{P}}(\mathsf{M}_{\mathbb{P}}(T))$. Tudíž $\mathsf{M}_{\mathbb{P}}(\chi_v)$ s $v \in \mathsf{M}_{\mathbb{P}}(T)$ jsou právě všechny atomy $\underline{\mathrm{AM}}_{\mathbb{P}}(T)$. Prvky $\underline{\mathcal{P}}(\mathsf{M}_{\mathbb{P}}(T))$ jsou sumy atomů, platí tedy i zbytek tvrzení. Explicitní tvrzení je důsledkem, neboť $\mathsf{M}_{\mathbb{P}}(\chi_v)$ s $v \in \mathsf{M}_{\mathbb{P}}(T,\varphi)$ jsou právě všechny atomy pod $\mathsf{M}_{\mathbb{P}}(T,\varphi)$. □

PŘÍKLADY 3.2.11.

1. Buď $\mathbb{P}$ konečná množina velikosti l, T buď $\mathbb{P}$-teorie, m počet modelů T.
   a) Teorie T má právě $2^m - 2$ nezávislých výroků až na ekvivalenci v T, vše sémanticky.
   b) Buď $p \in \mathbb{P}$, $T = \{p\}$ Pak $m = 2^{l-1}$, tudíž $|\mathrm{AM}_{\mathbb{P}}(T)| = 2^{2^{l-1}}$.
   c) Buď $l \geq 2$, $p, q \in \mathbb{P}$ různé, $T = \{p \to q\}$. Pak $m = 3 \cdot 2^{l-2}$, tudíž $|\mathrm{AM}_{\mathbb{P}}(T)| = 2^{3\cdot 2^{l-2}}$.
2. Buď $\mathbb{P}$ spočetná množina, $T = \{\chi\}$ buď $\mathbb{P}$-teorie s modelem. Pak $\underline{\mathrm{AM}}_{\mathbb{P}}(T) \cong \mathrm{CA}(\mathbb{P}) \cong \mathrm{CA}$.

Algebra $\underline{\mathrm{AM}}_{\mathbb{P}}(T)$ je bezatomární, protože když $\mathsf{M}_{\mathbb{P}}(T,\varphi) \neq \emptyset$ a $p \in \mathbb{P} - \mathrm{var}(\varphi)$, tak je $\emptyset \neq \mathsf{M}_{\mathbb{P}}(T,\varphi \,\&\, p) \subsetneq \mathsf{M}_{\mathbb{P}}(T,\varphi)$ (neboť existuje $v \models \varphi$ s $v(p) = 0$ a pak $v \notin \mathsf{M}_{\mathbb{P}}(T,\varphi \,\&\, p)$). Dále protože algebra $\underline{\mathrm{AM}}_{\mathbb{P}}(T)$ je nejvýše spočetná, je díky bezatomárnosti spočetná. Platí tvrzení: až na izomorfizmus existuje právě jedna spočetná bezatomární algebra. Protože CA je spočetná bezatomární algebra, máme $\underline{\mathrm{AM}}_{\mathbb{P}}(T) \cong \mathrm{CA}(\mathbb{P}) \cong \mathrm{CA}$.

3.2.12. **Booleovské funkce.**

Booleovská funkce n proměnných s $n > 0$ je funkce $f : {}^{n}2 \to 2$ (čili prvek množiny ${}^{{}^n 2}2$). Booleova algebra $\underline{{}^{{}^n 2}2}$ je *(Booleova) algebra booleovských funkcí* n proměnných (operace se berou po složkách v algebře $\underline{2}$); značíme ji též $\underline{\mathrm{BF}}_n$, stručně jen BF_n.

Booleovská funkce $f : {}^{n}2 \to 2$ symbolicky reprezentuje zařízení, které vstupu danému n-ticí nul a jedniček přiřadí hodnotu 0 nebo 1.

TVRZENÍ 3.2.13. (O algebře booleovských funkcí.) *Pro n-prvkovou* $\mathbb{P} = \{p_0, \dots, p_{n-1}\}$ *platí:*

1) $\underline{\mathrm{AM}}_{\mathbb{P}} \cong \underline{\mathrm{BF}}_n$ *via* $g : \mathcal{P}({}^{\mathbb{P}}2) \to {}^{^n2}2$, *kde pro* $K \subseteq {}^{\mathbb{P}}2$ *je* $g(K)$ *charakteristická funkce množiny* $\{v^* : n \to 2;\ v \in K\}$ *s* $v^*(i) = v(p_i)$ *pro* $i < n$.
2) *Pro booleovskou funkci* $f \in {}^{^n2}2$ *je* $\mathsf{M}_{\mathbb{P}}(\varphi_f) = g^{-1}(f)$, *kde* φ_f *je* $\bigvee_{f(\sigma)=1} \bigwedge_{i<n} p_i^{\sigma(i)}$.

Důkaz. 1) Je $\underline{\mathrm{AM}}_{\mathbb{P}} = \underline{\mathcal{P}}({}^{\mathbb{P}}2)$. Tvrzení tedy plyne z toho, že zobrazení $u \mapsto$ charakteristická funkce u, kde $u \subseteq I$, je izomorfizmus potenční algebry $\underline{\mathcal{P}}(I)$ a algebry ${}^{I}\underline{2}$.

2) Pro $v \in {}^{\mathbb{P}}2$ je zřejmě $v \models \varphi_f \Leftrightarrow v \in g^{-1}(f)$. Tedy $\mathsf{M}_{\mathbb{P}}(\varphi_f) = g^{-1}(f)$ platí. □

Počty neekvivalentních výroků a teorií nad konečně prvovýroky.

TVRZENÍ 3.2.14. (O počtu neekvivalentních výroků a teorií nad konečně prvovýroky sémanticky.) *Buď* $\mathbb{P}$ *výrokový jazyk s* $|\mathbb{P}| = l \in \mathbb{N}$. *Pak platí sémanticky:*

1) $\mathbb{P}$*-teorie* T *má právě* $2^{2^l - |\mathsf{M}(T)|}$ *neekvivalentních pravdivých a také tolik lživých výroků. Speciálně je* 2^{2^l} *neekvivalentních výroků nad* $\mathbb{P}$.
2) $\mathbb{P}$*-teorie* T *má právě* $2^{2^l} - 2 \cdot 2^{2^l - |\mathsf{M}(T)|}$ *neekvivalentních nezávislých výroků.*
3) $\mathbb{P}$*-teorie* T *má právě* $2^{|\mathsf{M}(T)|}$ *resp.* $|\mathsf{M}(T)|$ *neekvivalentních jednoduchých extenzí resp. navíc kompletních.*
   Speciálně je právě 2^{2^l} *neekvivalentních* $\mathbb{P}$*-teorií a právě* 2^l *neekvivalentních kompletních* $\mathbb{P}$*-teorií.*

Důkaz. 1) Pro $\varphi \in \mathrm{VF}_{\mathbb{P}}$ je $T \models \varphi \Leftrightarrow \mathsf{M}(T) \subseteq \mathsf{M}(\varphi)$. Tudíž je právě tolik pravdivých výroků teorie T neekvivalentních sémanticky, kolik je podmnožin množiny ${}^{\mathbb{P}}2 - \mathsf{M}(T)$ a těch je $2^{2^l - |\mathsf{M}(T)|}$. Lživé výroky jsou negace pravdivých, tedy jich je stejně. Speciální tvrzení plyne, volíme-li T spornou sémanticky; pak $\mathrm{Tru}_{\mathbb{P}}(T) = \mathrm{VF}_{\mathbb{P}}$ a $\mathsf{M}(T) = \emptyset$.

2) je důsledkem 1) a definice nezávislých výroků.

3) $\mathbb{P}$-teorie S je jednoduchá extenze T, právě když $\mathsf{M}(S) \subseteq \mathsf{M}(T)$. Tudíž jednoduchých extenzí T až na ekvivalenci teorií sémanticky je právě tolik, kolik je podmnožin $\mathsf{M}(T)$ (protože každá podmnožina ${}^{\mathbb{P}}2$ díky konečnosti $\mathbb{P}$ je axiomatizovatelná); je jich tedy $|\mathcal{P}(\mathsf{M}(T))| = 2^{|\mathsf{M}(T)|}$. Má-li být S navíc kompletní sémanticky, musí mít právě jediný model a tedy takových S je $|\mathsf{M}(T)|$. Speciální tvrzení plyne volbou $T = \emptyset$; pak $|\mathsf{M}(T)| = 2^l$. □

PŘÍKLADY 3.2.15. Buď $\mathbb{P}$ výrokový jazyk s $|\mathbb{P}| = l \in \mathbb{N}$.

1. a) Neexistuje $\mathbb{P}$-teorie T tak, že až na ekvivalenci sémanticky T má právě 21 pravdivých výroků, neboť až na ekvivalenci sémanticky T má právě $2^{2^l - |\mathsf{M}(T)|}$ pravdivých výroků, což není dělitelné třemi.

b) Neexistuje $\mathbb{P}$-teorie T tak, že až na ekvivalenci sémanticky má T právě tolik pravdivých výroků, kolik má nezávislých výroků sémanticky. Jinak by totiž muselo platit $2^{2^l} - 2 \cdot 2^{2^l - |\mathsf{M}(T)|} = 2^{2^l - |\mathsf{M}(T)|}$, tj. $2^{2^l} = 3 \cdot 2^{2^l - |\mathsf{M}(T)|}$, což není možné.

2. Buď $k \leq 2^l$. Pak existuje právě $\binom{2^{2^l}}{2^l - k}$ neekvivalentních sémanticky $\mathbb{P}$-teorií T, z nichž každá až na ekvivalenci sémanticky má pravdivých právě 2^k výroků. Pro uvažované T je totiž právě $2^k = 2^{2^l - |\mathsf{M}(T)|}$, tedy právě $|\mathsf{M}(T)| = 2^l - k$. Takových T neekvivalentních sémanticky je tudíž právě tolik, kolik je různých $(2^l - k)$-prvkových podmnožin ${}^{\mathbb{P}}2$ a těch je právě $\binom{2^{2^l}}{2^l - k}$.

3.3 Existence modelu, kompletnost a kompaktnost.

VĚTA 3.3.1. (O maximální bezesporné teorii a o existenci modelu.)

1) *Buď* T *maximální bezesporná teorie,* φ, ψ *její formule. Pak platí:*
   a) $T \vdash \varphi \ \Leftrightarrow\ \varphi \in T \ \Leftrightarrow\ T, \varphi$ *je bezesporná.*
   b) $\varphi \in T \ \Leftrightarrow\ \neg\varphi \notin T, \quad \varphi \to \psi \in T \Leftrightarrow \neg\varphi \in T$ *nebo* $\psi \in T$.
   c) *Ohodnocení* v *takové, že* $v(p) = 1 \Leftrightarrow p \in T$ *pro každý prvovýrok* p, *je jediný model* T.

2) *Bezesporná teorie T má maximální bezespornou jednoduchou extenzi (tj. v jazyce $\mathbb{P}(T)$).*

3) (O existenci modelu.) *Teorie má model, právě když je bezesporná.*

Důkaz. 1) a) $\Rightarrow$ v prvé $\Leftrightarrow$ plyne z toho, že rozšíření bezesporné teorie o její teorém je bezesporné, $\Leftarrow$ je jasná. Druhá $\Leftrightarrow$ je zřejmá z definice maximální bezesporné teorie. b) $\neg\varphi \notin T \Leftrightarrow T, \neg\varphi$ je sporná $\Leftrightarrow T \vdash \varphi \Leftrightarrow \varphi \in T$ dle 2) a) a důkazu sporem. Tvrzení o implikaci: Když $\varphi \to \psi \in T$, tak z $\neg\varphi \notin T$ plyne $\varphi \in T$; pak $T \vdash \psi$ a díky a) je $\psi \in T$. Když $\neg\varphi \in T$, tak $T \vdash \varphi \to \psi$ díky 3.1.5, a), tedy $\varphi \to \psi \in T$ díky a). Podobně když $\psi \in T$, tak $T, \varphi \vdash \psi$, tudíž $T \vdash \varphi \to \psi$. c) Platí $\varphi \in T \Leftrightarrow v(\varphi) = 1$, což plyne indukcí dle složitosti φ ihned užitím b); tedy $v \models T$. Konečně pro $w \models T$ máme $w(p) = 1 \Leftrightarrow p \in T$ pro každý prvovýrok p, tedy $w = v$.

2) plyne z principu maximality (ekvivalentního s axiomem výběru), aplikujeme-li jej na množinu všech bezesporných teorií S s $S \supseteq T$, na níž uvažujeme uspořádání inkluzí; každý řetězec R v popsaném uspořádání má majorantu, kterou je jeho sjednocení $\bigcup R$, neboť to je teorie, rozšiřující T, která je bezesporná, protože spor v ní je sporem v nějaké teorii z R.

3) Má-li teorie model, je dle 3.2.2 bezesporná. Nechť je T bezesporná teorie. Dle 2) existuje její maximální bezesporná jednoduchá extenze T' a dle 1), c) existuje model teorie T', což je ovšem i model T. □

VĚTA 3.3.2.

1) (O kompletnosti.) $T \vdash \varphi \;\Leftrightarrow\; T \models \varphi$ *platí pro každou teorii T a její formuli φ.*

2) (O kompaktnosti.) *Teorie má model, právě když každá její konečná část má model.*

Důkaz. 1) $T \vdash \varphi \Rightarrow T \models \varphi$ je tvrzení o korektnosti. Buď obráceně $T \models \varphi$. Pak je $T, \neg\varphi$ sporná dle tvrzení o existenci modelu, tedy $T \vdash \varphi$ dle důkazu sporem.

2) plyne ihned z věty o existenci modelu, neboť teorie je bezesporná, právě když je bezesporná každá její konečná část. □

POZNÁMKA 3.3.3. Je-li T v jazyce s nejvýše spočetně prvovýroky, maximální bezesporné rozšíření se sestrojí indukcí takto. Buď $\{\varphi_n;\, 0 < n \in \omega\}$ očíslování formulí, T_0 teorie T a T_{n+1} rovna teorii $T_n \cup \{\varphi_{n+1}\}$, je-li tato bezesporná, a rovna teorii $T_n \cup \{\neg\varphi_{n+1}\}$ jinak. Pak $\bigcup_{n\in\omega} T_n$ je hledané maximální rozšíření.

3.3.4. Uveďme několik důsledků věty o kompletnosti.

• Je $\mathrm{Thm}(T) = \mathrm{Tru}(T)$. Sémantické verze pojmů jako nezávislá formule, [beze]sporná teorie, kompletní teorie, extenze a ekvivalence teorií jsou ekvivalentní syntaktickým.

• V 2.2.14 lze zaměnit $\models$ za $\vdash$; získaná tvrzení jsou užitečné deduktivní obraty výrokové logiky.

• Z 2.2.20 získáme následující syntaktickou verzi tvrzení o ekvivalenci:

Vznikne-li výrok φ' z φ nahrazením některých výskytů podvýroku ψ formulí ψ', tak

$$T \vdash \psi \leftrightarrow \psi' \quad \Rightarrow \quad T \vdash \varphi \leftrightarrow \varphi'.$$

• Nechť T je $\mathbb{P}$-teorie, T' pak $\mathbb{P}'$-teorie. Buď $\mathsf{M}(T')\restriction\mathbb{P} = \{v\restriction\mathbb{P};\, v \in \mathsf{M}(T')\}$. Pak

a) T' je extenze T $\quad\Leftrightarrow\quad \mathbb{P} \subseteq \mathbb{P}'$ a $\mathsf{M}(T')\restriction\mathbb{P} \subseteq \mathsf{M}(T)$.

b) T' je ekvivalentní s T $\quad\Leftrightarrow\quad \mathbb{P} = \mathbb{P}'$ a $\quad \mathsf{M}(T') = \mathsf{M}(T)$.

Důkaz. 1) Když T' je extenze T, tak $\mathbb{P} \subseteq \mathbb{P}'$ a $T \subseteq \mathrm{Thm}(T')$. Tedy pro $\varphi \in T$ a $v \in \mathsf{M}(T')$ je $v \models \varphi$, tudíž i $v\restriction\mathbb{P} \models \varphi$. To znamená, že $\mathsf{M}(T')\restriction\mathbb{P} \subseteq \mathsf{M}(T)$. Nechť naopak $\mathbb{P} \subseteq \mathbb{P}'$ a $\mathsf{M}(T')\restriction\mathbb{P} \subseteq \mathsf{M}(T)$. Pak pro $\mathbb{P}$-formuli φ máme $T \vdash \varphi \Rightarrow T \models \varphi \Rightarrow T' \models \varphi \Rightarrow T' \vdash \varphi$; poslední $\Rightarrow$ plyne z věty o kompletnosti. Tudíž T' je extenze T.

• Výroková teorie T je kompletní, právě když má právě jeden model.

Důkaz plyne z toho, že T je kompletní sémanticky, právě když má právě jeden model.

• Tvrzení 3.2.14 o počtu neekvivalentních výroků a teorií nad konečně prvovýroky platí nyní i „syntakticky“; místo pravdivého a lživého výroku teď máme ovšem dokazatelný a vyvratitelný výrok.

3.4 Aplikace kompaktnosti. Axiomatizovatelnost.

Aplikace kompaktnosti.

3.4.1. **Obarvitelnost nekonečných grafů.**
Buď $0 < k \in \mathbb{N}$. Obyčejný graf $\langle V, E\rangle$ je k-obarvitelný, existuje-li jeho k-obarvení, tj. soubor $\langle C_i\rangle_{i<k}$ takový, že

$$\begin{array}{c} \text{a) } \bigcup_{i<k} C_i = V, \qquad \text{b) } C_i \cap C_j = \emptyset \text{ pro } i \neq j,\ i,j<k, \\ \text{c) není } \{a,b\} \subseteq C_i, \text{ pokud } \langle a,b\rangle \in E. \end{array} \tag{3.4}$$

Připouští se $C_i = \emptyset$, k-obarvení je tedy obarvení nejvýše k-barvami.

TVRZENÍ. *Buď $0 < k \in \mathbb{N}$. Obyčejný graf je k-obarvitelný, právě když je každý jeho konečný podgraf k-obarvitelný.*

Důkaz. Stačí zřejmě dokázat implikaci $\Leftarrow$. Buď $\langle V, E\rangle$ obyčejný graf, jehož každý konečný podgraf je k-obarvitelný. Buď $\mathbb{P}$ množina prvovýroků $p_{a,i}$, $a \in V$, $i < k$ a T výroková $\mathbb{P}$-teorie s axiomy:

$$\begin{array}{c} \text{(a) } p_{a,0} \vee \cdots \vee p_{a,k-1}, \ \text{ kde } \ a \in V, \\ \text{(b) } \neg(p_{a,i} \mathbin{\&} p_{a,j}), \ \text{ kde } \ a \in V,\ i \neq j, i,j < k \quad \text{(c) } \neg(p_{a,i} \mathbin{\&} p_{b,i}), \ \text{ kde } \ \langle a,b\rangle \in E,\ i<k. \end{array}$$

Položky (a), (b), (c) odpovídají a), b), c) z (3.4). Každá konečná neprázdná část $T' \subseteq T$ má model v. Buď totiž k-obarvení $\langle C'_i\rangle_{i<k}$ podgrafu uvažovaného grafu, s konečnou množinou V' vrcholů tvořenou a takovými, že nějaké $p_{a,i}$ je v některé formuli z T'. Pak je modelem T' funkce $v' : \mathbb{P} \to 2$ definované vztahem

$$v'(p_{a,i}) = 1 \Leftrightarrow a \in C'_i. \tag{3.5}$$

Z kompaktnosti plyne existence modelu v teorie T. Definujme C_i podle (3.5). Pak $\langle C_i\rangle_{i<k}$ je k-obarvení $\langle V, E\rangle$. □

3.4.2. **Prostý selektor.**
(Prostý) selektor neprázdné množiny S neprázdných množin je (prostá) funkce $f : S \to \bigcup S$ taková, že $f(u) \in u$ pro každé $u \in S$.

TVRZENÍ. (O existence prostého selektoru.)

1) *Neprázdná množina S neprázdných konečných množin má prostý selektor, právě když každá její neprázdná konečná podmnožina má prostý selektor.*
2) (Hallova věta.) *Prostý selektor konečné neprázdné množiny S konečných neprázdných množin existuje, právě když platí Hallova podmínka: pro každou $S' \subseteq S$ je $|S'| \leq |\bigcup S'|$.*

Důkaz. 1) Stačí dokázat implikaci $\Leftarrow$, neboť opačná platí triviálně. Buď $\mathbb{P} = \{p_{u,a};\ u \in U, a \in \bigcup S\}$ množina prvovýroků a T výroková $\mathbb{P}$-teorie s axiomy:

$$\begin{array}{ll} p_{u,a_1} \vee \cdots \vee p_{u,a_n}, & \text{kde } \ u \in S \text{ a } a_1, \ldots, a_n \text{ je prosté očíslování } u, \\ \neg(p_{u,a} \mathbin{\&} p_{u',a}), & \text{kde } \ u \neq u' \text{ jsou z } S,\ a \in u \cap u'. \end{array} \tag{3.6}$$

Každá neprázdná konečná část $T' \subseteq T$ má model, neboť je-li S' množina všech $u \in S$ takových, že některé $p_{u,a}$ je v nějakém výroku z T', má S' prostý selektor f' a pak $v' : \mathbb{P} \to 2$ splňující $v'(p_{u,a}) = 1 \Leftrightarrow f'(u) = a$, je jasně model T'. Z kompaktnosti plyne, že T má nějaký model v. Definujme $f : S \to \bigcup S$ tak, že $f(u) = a$ pro nějaké $a \in u$ s $v(p_{u,a}) = 1$; takové a jistě existuje dle prvého řádku z (3.6). Dále je f prostá funkce dle druhého řádku z (3.6).

2) Dokažme $\Leftarrow$ indukcí dle $n = |S|$, tj. že pro každou S nenulové velikosti nejvýše n platí $\Leftarrow$. Pro $n = 1$ to platí. Nechť to platí pro nějaké nenulové n; dokážeme platnost pro $n + 1$. Buď $|S| = n + 1$.

Případ (A): Existuje S_0 tak, že $\emptyset \neq S_0 \subsetneq S$ a $|S_0| = |\bigcup S_0|$. Dle indukčního předpokladu existuje prostý selektor g množiny S_0. Označme $S_1 = \{u - \bigcup S_0;\ u \in S - S_0\}$, Je $0 < |S_1| < |S|$ a S_1 splňuje Hallovu podmínku, neboť pro $S' \subseteq S_1$ máme

$$|\bigcup S'| = |\bigcup S' \cup \bigcup S_0 - \bigcup S_0| = |\bigcup S' \cup \bigcup S_0| - |\bigcup S_0|$$
$$\geq |S' \cup S_0| - |S_0| = |S'| + |S_0| - |S_0| = |S'|.$$

Tedy dle indukčního předpokladu existuje prostý selektor h množiny S_1; pak rozšíření g o prostou funkci $\{\langle u, h(u - \bigcup S_0)\rangle;\ u \in S - S_0\}$ je prostý selektor pro S.

Případ (B): neplatí (A). Pak pro každé S' splňující $\emptyset \neq S' \subsetneq S$ máme $|S'| < |\bigcup S'|$. Vyberme $a_0 \in u_0 \in S$. Pak dle indukčního předpokladu máme prostý selektor g množiny $\{u - \{a_0\};\ u \in S - \{u_0\}\}$. Pak funkce $f : S \to \bigcup S$ definovaná tak, že $f(u) = g(u - \{a_0\})$ pro $u \in S - \{u_0\}$ a $f(u_0) = a_0$, je prostý selektor množiny S. □

3.4.3. **Linearizace uspořádání.**

TVRZENÍ. *Je-li $\langle A, <\rangle$ ostré uspořádání, existuje $R \subseteq A^2$ rozšiřující $<$ tak, že $\langle A, R\rangle$ je ostré lineární uspořádání.*

Důkaz. A) Tvrzení platí pro A konečné. To plyne indukcí podle počtu prvků A; v indukčním kroku odstraníme minimální prvek, dle indukčního předpokladu „zlinearizujeme“ zbytek a z odstraněného prvku uděláme nejmenší.

B) Buď $\mathbb{P}$ množina prvovýroků právě tvaru $p_{a,b}$, $a, b \in A$. T buď $\mathbb{P}$-teorie s axiomy (a) – (c):

(a) $p_{a,b} \,\&\, p_{b,c} \to p_{a,c}$, $\neg p_{a,a}$, $p_{a,b} \to \neg p_{b,a}$ pro každé $a, b \in A$,

(b) $p_{a,b} \vee p_{b,a}$ pro každé $a \neq b$, $a, b \in A$,

(c) $p_{a,b}$ pro každé $a < b$.

Podle části A) důkazu má každá konečná část T model, tedy dle kompaktnosti má T nějaký model v. Definujme $R = \{\langle a, b\rangle \in A^2;\ v(p_{a,b}) = 1\}$. Dle (a) je R uspořádání A, dle (b) je navíc lineární a dle (c) rozšiřuje $<$. □

Axiomatizovatelnost tříd modelů.

VĚTA 3.4.4. (O konečné axiomatizovatelnosti.) *Množina $\mathsf{K} \subseteq {}^{\mathbb{P}}2$ je konečně axiomatizovatelná, právě když ona i její komplement jsou axiomatizovatelné.*

Důkaz. Implikace $\Rightarrow$ je jasná. Dokážeme opačnou. Nechť T, S jsou takové teorie, že $\mathsf{K} = \mathsf{M}(T) = -\mathsf{M}(S)$. Pak $\mathsf{M}(T \cup S) = \mathsf{M}(T) \cap \mathsf{M}(S) = \emptyset$, tedy díky kompaktnosti existují $T' \subseteq T$, $S' \subseteq S$ konečné tak, že $T' \cup S'$ nemá model; pak $\emptyset = \mathsf{M}(T' \cup S') = \mathsf{M}(T') \cap \mathsf{M}(S')$. Konečně $\mathsf{M}(T) \subseteq \mathsf{M}(T') \subseteq -\mathsf{M}(S') \subseteq -\mathsf{M}(S) \subseteq \mathsf{M}(T)$, tedy $\mathsf{M}(T) = \mathsf{M}(T')$. □

3.4.5. **Uzavřené, otevřené a obojetné třídy modelů.**

Buď $\mathbb{P}$ množina prvovýroků, $\mathsf{K} \subseteq {}^{\mathbb{P}}2$ třída modelů jazyka nad $\mathbb{P}$. Pak $w \in {}^{\mathbb{P}}2$ je *oddělitelné od* K, existuje-li klauzule χ *oddělující w od* K, tj. taková, že $w \notin \mathsf{M}(\chi) \supseteq K$; jinak je *$w$ neoddělitelné od* K. Třída K je *uzavřená*, je-li každé $w \in {}^{\mathbb{P}}2 - \mathsf{K}$ oddělitelné od K. Třída K je *otevřená*, je-li ${}^{\mathbb{P}}2 - \mathsf{K}$ uzavřená. Třída K je *obojetná*, je-li uzavřená i otevřená. Zřejmě platí:

Třída $\mathsf{K} \subseteq {}^{\mathbb{P}}2$ je otevřená $\Leftrightarrow$ pro každé $v \in K$ existuje klauzule χ s $v \in \mathsf{M}(\neg\chi) \subseteq \mathsf{K}$.

VĚTA 3.4.6. *Buď K třída modelů jazyka nad $\mathbb{P}$.*

1) *K je axiomatizovatelná, právě když je uzavřená.*

2) *K je konečně axiomatizovatelná, právě když je obojetná.*

3) a) *Obor obojetných tříd modelů jazyka nad $\mathbb{P}$ tvoří právě algebru* $\mathrm{AM}_{\mathbb{P}}$ *(viz* 3.2.10.*)*

b) *Třída K je uzavřená resp. otevřená, právě když je průnikem resp. sjednocením neprázdné množiny obojetných množin. Obor uzavřených resp. otevřených tříd modelů jazyka nad $\mathbb{P}$ je uzavřený na $\bigcap, \cup$ resp. $\bigcup, \cap$. Jednoprvkové třídy, tj. tvaru $\{v\}$ s $v \in {}^{\mathbb{P}}2$, jsou uzavřené.*

c) *$\bigcap \mathcal{K} \neq \emptyset$, je-li $\mathcal{K}$ centrovaná množina uzavřených množin.*

Důkaz. Poznamenejme nejprve, že každá teorie je ekvivalentní teorii s axiomatikou tvořenou klauzulemi.

1) a) Buď $K = \mathsf{M}(T)$ a T z klauzulí; je $\mathsf{K} = \bigcap_{\chi \in T} \mathsf{M}(\chi)$. Pak w neoddělitelné od K leží v každém $\mathsf{M}(\chi)$ pro $\chi \in T$ a tedy $w \in \mathsf{K}$. b) Buď K uzavřená. Buď $T = \{\chi;\ \chi \text{ je klauzule a } \mathsf{K} \subseteq \mathsf{M}(\chi)\}$;

dokážeme $\mathsf{K} = \mathsf{M}(T) = \bigcap_{\chi\in T} \mathsf{M}(\chi)$. Jasně $\mathsf{K} \subseteq \mathsf{M}(T)$. Pro $w \in {}^{\mathbb{P}}2 - \mathsf{K}$ je w odděleno od K nějakou klauzulí χ, tj. $w \notin \mathsf{M}(\chi) \supseteq \mathsf{K}$. Je $\chi \in T$ a tedy $w \notin \mathsf{M}(T)$, což jsme měli dokázat.

2) Protože třída K je konečně axiomatizovatelná, právě když ona i její komplement jsou axiomatizovatelné, plyne dokazované z 1).

3) a) Podle 2) jsou jsou obojetné třídy právě tvaru $\mathsf{M}(\varphi)$, kde φ je výrok nad $\mathbb{P}$. To jsou právě prvky algebry $\mathrm{AM}^{\mathbb{P}}$. b) Zřejmě uzavřené třídy jsou právě tvaru $\bigcap_{\varphi\in T} \mathsf{M}(\varphi)$, kde T je nějaká neprázdná $\mathbb{P}$-teorie, a každé $\mathsf{M}(\varphi)$ je obojetná. Tvrzení pro otevřené třídy plyne přechodem ke komplementu. Jednoprvková třída je axiomatizovatelná. c) Pro $\mathsf{K} \in \mathcal{K}$ buď T_{K} teorie s $\mathsf{M}(T_{\mathsf{K}}) = \mathsf{K}$. $\bigcap \mathcal{K} = \mathsf{M}(\bigcup_{\mathcal{K}} T_{\mathsf{K}})$ a teorie $\bigcup_{\mathcal{K}} T_{\mathsf{K}}$ má model, neboť každý její konečný fragment má model. □

3.5 Syntaktické důkazové metody.

3.5.1. Syntaktické důkazové metody prokazují dokazatelnost formulí (v nějaké dané teorii T, to jest vztah $T \vdash \varphi$) jen pomocí syntaktických pojmů, tj. bez užití pojmu modelu, pravdivosti a věty o kompletnosti. Typicky se užívají:

– Již syntakticky prokázaná dokazatelnost nějakých formulí (speciálně pak axiomů).
– Pravidlo MP, věta o dedukci, důkaz sporem a indukce na teorémech či dle délky formule.
– Obraty následujícího tvaru, jsou-li zdůvodněny syntaktickou argumentací:

$$T \vdash \varphi_1, \dots, T \vdash \varphi_n \Rightarrow T \vdash \varphi, \quad \text{pokud } \varphi_1, \dots, \varphi_n, \varphi \text{ splňují } ---, \tag{3.7}$$

Obratům tvaru (3.7) říkejme neformálně (syntaktická) důkazová pravidla; pojem zavádíme jen k jistému zpřehlednění vyjadřování. Uveďme např., že z $T \vdash \varphi \to \psi$ plyne triviálně důkazové pravidlo $T \vdash \varphi \Rightarrow T \vdash \psi$. Můžeme tedy užívat jako důkazové pravidlo $T \vdash \varphi \Rightarrow T \vdash \neg\neg\varphi$ dle b) z 3.1.5. Dále také důkazové pravidlo $T \vdash \varphi \Rightarrow T \vdash \psi \to \varphi$ plynoucí z (PL1) apod. Další taková pravidla jsou obsažená např. v 3.5.2 3). Jiné důkazové pravidlo je obsaženo v 3.5.5 ve formulaci b). Syntakticky prokázané jsou zatím

$$\vdash \varphi \to \varphi \text{ (viz 3.1.4)}, \qquad \text{a) – e) z 3.1.5.}$$

Na a) – e) z 3.1.5 se budeme dále odvolávat jako na [a] – [e].

Abychom se mohli úsporně vyjadřovat, označme pro dvě množiny formulí T, S vlastnost, že každá formule z S je dokazatelná v T, symbolem

$$T \vdash S.$$

Znamená to právě, že $\mathrm{Thm}(S) \subseteq \mathrm{Thm}(T)$, neboť $T \vdash S \Leftrightarrow S \subseteq \mathrm{Thm}(T) \Leftrightarrow \mathrm{Thm}(S) \subseteq \mathrm{Thm}(T)$; to plyne díky známým vlastnostem uzávěru Thm. Zřejmě dále $T \vdash S$ a $S \vdash S' \Rightarrow T \vdash S'$; tomuto tvrzení říkejme *tranzitivita dedukce*. Speciálním případem je *tranzitivita* $\to$: $T \vdash \varphi \to \psi$ a $T \vdash \psi \to \psi' \Rightarrow T \vdash \varphi \to \psi'$. Místo $T \vdash S$ a $S \vdash S'$ můžeme psát stručně $T \vdash S \vdash S'$.

TVRZENÍ 3.5.2.

1) a) $\varphi \,\&\, \psi \vdash \varphi, \psi$ b) $\varphi, \psi \vdash \varphi \,\&\, \psi$

2) a) $\varphi \leftrightarrow \psi \vdash \{\varphi \to \psi, \psi \to \varphi\}$ b) $\{\varphi \to \psi, \psi \to \varphi\} \vdash \varphi \leftrightarrow \psi$

3) $T \vdash \varphi \,\&\, \psi \quad \Leftrightarrow \quad T \vdash \varphi$ *a* $T \vdash \psi$

$T \vdash \varphi \leftrightarrow \psi \quad \Leftrightarrow \quad T \vdash \varphi \to \psi$ *a* $T \vdash \psi \to \varphi$

Pravidlo tranzitivity $\leftrightarrow$: $T \vdash \varphi \leftrightarrow \psi$ *a* $T \vdash \psi \leftrightarrow \chi \Rightarrow T \vdash \varphi \leftrightarrow \chi$

Důkaz. Hlavní kroky důkazu píšeme do sloupce vlevo, vpravo pak argumentaci pro platnost kroku (opírající se o platnost předešlých kroků); přitom $[x]$ je odvolání na položku x) z 3.1.5.

1) Připomeňme, že $\varphi \,\&\, \psi$ je $\neg(\varphi \to \neg\psi)$.

a)

$\varphi \,\&\, \psi \vdash \varphi$.		$\varphi \,\&\, \psi \vdash \psi$	
$\vdash \neg\varphi \to (\varphi \to \neg\psi)$	[a]	$\vdash \neg\psi \to (\varphi \to \neg\psi)$	(PL1)
$\vdash \neg(\varphi \to \neg\psi) \to \neg\neg\varphi$	[c], MP	$\vdash \neg(\varphi \to \neg\psi) \to \neg\neg\psi$	[c], MP
$\vdash \neg(\varphi \to \neg\psi) \to \varphi$	[b], tranzitivita $\to$	$\vdash \neg(\varphi \to \neg\psi) \to \psi$	[b], tranzitivita $\to$
$\varphi \,\&\, \psi \vdash \varphi$	věta o dedukci	$\varphi \,\&\, \psi \vdash \psi$	věta o dedukci

b)

$\vdash \varphi \to (\neg\neg\psi \to \neg(\varphi \to \neg\psi))$	[d]
$\varphi \vdash (\neg\neg\psi \to \neg(\varphi \to \neg\psi))$	věta o dedukci
$\varphi, \psi \vdash \neg(\varphi \to \neg\psi)$	[b], věta o dedukci

2) Protože $\varphi \leftrightarrow \psi$ je $\varphi \to \psi \,\&\, \psi \to \varphi$, plyne tvrzení ihned z 1).

3) Ekvivalence o &. Z $T \vdash \varphi \,\&\, \psi$ plyne pomocí 1) a) $T \vdash \{\varphi, \psi\}$, tj. $\Rightarrow$ platí. Obdobně pomocí 1) b) plyne $\Leftarrow$. Ekvivalence o $\leftrightarrow$ se dokáže stejně pomocí 2). Pravidlo tranzitivity $\leftrightarrow$ plyne z předešlé $\Leftrightarrow$ a z 1), 2). □

TVRZENÍ 3.5.3. *Následující ekvivalence jsou dokazatelné:*

1)	φ	$\leftrightarrow$	$(\varphi \,\&\, \varphi)$	*idempotence &*
2)	$\varphi \,\&\, \psi$	$\leftrightarrow$	$\psi \,\&\, \varphi$	*komutativita &*
3)	$(\varphi \,\&\, \psi) \,\&\, \chi$	$\leftrightarrow$	$\varphi \,\&\, (\psi \,\&\, \chi)$	*asociativita &*
4)	φ	$\leftrightarrow$	φ	*reflexivita* $\leftrightarrow$
5)	$(\varphi \leftrightarrow \psi)$	$\leftrightarrow$	$(\psi \leftrightarrow \varphi)$	*symetrie* $\leftrightarrow$
6)	φ	$\leftrightarrow$	$\neg\neg\varphi$	*idempotence* $\neg$

Důkaz. 1) Z 3.5.2 1) a věty o dedukci máme $\vdash \varphi \to (\varphi \,\&\, \varphi)$, $\vdash (\varphi \,\&\, \varphi) \to \varphi$, dle 3.5.2 2) tedy $\vdash \varphi \leftrightarrow (\varphi \,\&\, \varphi)$. 2) Dle 3.5.2 1) je $\varphi \,\&\, \psi \vdash \{\varphi, \psi\} \vdash \{\psi, \varphi\} \vdash \psi \,\&\, \varphi$, tj. $\vdash (\varphi \,\&\, \psi) \to (\psi \,\&\, \varphi)$. Tudíž i $\vdash (\psi \,\&\, \varphi) \to (\varphi \,\&\, \psi)$ a dokazovaná ekvivalence plyne z 3.5.2 2). 3) se dokáže zcela obdobně.

4) Je $\vdash \varphi \to \varphi$, dle 3.5.2 3) tedy i $\vdash \varphi \leftrightarrow \varphi$.

5) $\varphi \leftrightarrow \psi \vdash \varphi \to \psi \,\&\, \psi \to \varphi \vdash \psi \to \varphi \,\&\, \varphi \to \psi \vdash \psi \leftrightarrow \varphi$ užitím definice $\leftrightarrow$ a komutativity &.

6) Je $\vdash \varphi \to \neg\neg\varphi$, $\vdash \neg\neg\varphi \to \varphi$ dle [b], dle 3.5.2 3) tedy i $\vdash \varphi \leftrightarrow \neg\neg\varphi$. □

TVRZENÍ 3.5.4. *Následující ekvivalence jsou dokazatelné:*

1)	$(\varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots)))$	$\leftrightarrow$	$((\varphi_1 \,\&\, \varphi_2 \,\&\, \cdots \,\&\, \varphi_n) \to \psi)$
2)	$(\varphi \leftrightarrow \psi)$	$\leftrightarrow$	$((\varphi \to \psi) \,\&\, (\psi \to \varphi))$
3)	$(\varphi \leftrightarrow \psi)$	$\leftrightarrow$	$(\neg\varphi \leftrightarrow \neg\psi)$

Důkaz. 1) Stačí ukázat dokazatelnost $\to$ a $\leftarrow$; tvrzení pak plyne z 3.5.2 2) b). Dokažme $\to$ indukcí dle n. Užitím 3.5.2 1), MP a indukčního předpokladu máme

$$\begin{aligned}\{\varphi_1 \,\&\, (\varphi_2 \,\&\, \cdots \,\&\, \varphi_n), (\varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots)))\} &\vdash \\ \{\varphi_2 \,\&\, \cdots \,\&\, \varphi_n, \varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots)\} &\vdash \quad \psi.\end{aligned}$$

Zcela stejně plyne $\leftarrow$.

2) Stačí ukázat dokazatelnost $\to$ a $\leftarrow$; tvrzení pak plyne z 3.5.2 2) b). Implikace $\to$ plyne z 3.5.2 2) a), 1) b) a tranzitivity dedukce, implikace $\leftarrow$ z 3.5.2 1) a), 2) b) a tranzitivity dedukce.

3) Stačí ukázat dokazatelnost $\to$ a $\leftarrow$; tvrzení pak plyne z 3.5.2 2) b). Implikace $\to$. $\varphi \leftrightarrow \psi, \neg\varphi \vdash \{\psi \to \varphi, \neg\varphi\} \vdash \{\neg\varphi \to \neg\psi, \neg\varphi\} \vdash \neg\psi$ užitím 3.5.2, [c], MP; tedy $\varphi \leftrightarrow \psi \vdash \neg\varphi \to \neg\psi$. Zcela stejně plyne $\varphi \leftrightarrow \psi \vdash \neg\psi \to \neg\varphi$. Dle 3.5.2 2) b) tedy $\varphi \leftrightarrow \psi \vdash \neg\varphi \leftrightarrow \neg\psi$ a dle věty o dedukci i $\vdash (\varphi \leftrightarrow \psi) \to (\neg\varphi \leftrightarrow \neg\psi)$. Implikace $\leftarrow$ plyne zcela analogicky. □

TVRZENÍ 3.5.5. (O ekvivalenci.) *Vznikne-li formule φ' z φ nahrazením některého výskytu podformule ψ formulí ψ', tak*

$$\text{a) } \vdash \psi \leftrightarrow \psi' \to \varphi \leftrightarrow \varphi', \qquad \text{b) } T \vdash \psi \leftrightarrow \psi' \Rightarrow T \vdash \varphi \leftrightarrow \varphi'.$$

Důkaz. Jasně je b) důsledkem a). Dokazujeme a). Je-li nahrazovaný výskyt ψ celá formule φ, je φ rovno ψ a φ' rovno ψ' a dokazované má tvar $\vdash (\psi \leftrightarrow \psi') \to (\psi \leftrightarrow \psi')$, což platí díky $\vdash \chi \to \chi$. Dále nechť nahrazovaný výskyt ψ není celá formule φ. Dokazujme indukcí na výrocích. Je-li φ prvovýrok, je φ' rovno φ a jasně to platí.

Buď φ tvaru $\neg\varphi_0$. Máme

$$\psi \leftrightarrow \psi' \vdash \varphi_0 \leftrightarrow \varphi_0' \vdash \neg\varphi_0 \leftrightarrow \neg\varphi_0' \vdash \varphi \leftrightarrow \varphi';$$

prvé $\vdash$ plyne z indukčního předpokladu a z věty o dedukci, druhé $\vdash$ z 3.5.4 3). Věta o dedukci dá $\vdash \psi \leftrightarrow \psi' \to \varphi \leftrightarrow \varphi'$.

Buď φ tvaru $\varphi_0 \to \varphi_1$. Pak φ' je $\varphi_0' \to \varphi_1'$ s tím, že v některém φ_i nahrazení neprovádíme; pak je φ_i' rovno φ_i. Stačí dokázat: $\psi \leftrightarrow \psi' \vdash \varphi \leftrightarrow \varphi'$. Indukční předpoklad je $\psi \leftrightarrow \psi' \vdash \{\varphi_0 \leftrightarrow \varphi_0', \varphi_1 \leftrightarrow \varphi_1'\}$. Pak $\psi \leftrightarrow \psi', \varphi_0 \to \varphi_1, \varphi_0' \vdash \varphi_1'$ a věta o dedukci dá $\psi \leftrightarrow \psi' \vdash ((\varphi_0 \to \varphi_1) \to (\varphi_0' \to \varphi_1'))$, tj. $\psi \leftrightarrow \psi' \vdash \varphi \to \varphi'$. Zcela analogicky $\psi \leftrightarrow \psi' \vdash \varphi' \to \varphi$. Celkem díky 3.5.2 3) pak $\psi \leftrightarrow \psi' \vdash \varphi \leftrightarrow \varphi'$. □

TVRZENÍ 3.5.6. *Následující ekvivalence jsou dokazatelné:*

1)	$\neg(\varphi \,\&\, \psi)$	$\leftrightarrow$	$(\neg\varphi \vee \neg\psi)$	*de Morganův vztah*
2)	$\neg(\varphi \vee \psi)$	$\leftrightarrow$	$(\neg\varphi \,\&\, \neg\psi)$	*de Morganův vztah*
3)	φ	$\leftrightarrow$	$\varphi \vee \varphi$	*idempotence* $\vee$
4)	$\varphi \vee \psi$	$\leftrightarrow$	$\psi \vee \varphi$	*komutativita* $\vee$
5)	$(\varphi \vee \psi) \vee \chi$	$\leftrightarrow$	$\varphi \vee (\psi \vee \chi)$	*asociativita* $\vee$

Důkaz. 1) Následující ekvivalence jsou dokazatelné; vpravo je uveden argument:

$$\begin{array}{rcll} \neg(\varphi \,\&\, \psi) & \leftrightarrow & \neg\neg(\varphi \to \neg\psi) & \text{zavedení } \& \\ & \leftrightarrow & \varphi \to \neg\psi & \vdash \neg\neg\chi \leftrightarrow \chi \\ & \leftrightarrow & \neg\neg\varphi \to \neg\psi & \text{věta o ekvivalenci}, \vdash \chi \leftrightarrow \neg\neg\chi \\ & \leftrightarrow & \neg\varphi \vee \neg\psi & \text{zavedení } \vee. \end{array}$$

Z pravidla tranzitivity $\leftrightarrow$ plyne $\neg(\varphi \,\&\, \psi) \leftrightarrow (\neg\varphi \vee \neg\psi)$.

2) plyne stejně, jako 1).

3) – 5) plynou snadno z odpovídajících vlastností &, de Morganových vztahů a již dokázaných vlastností $\leftrightarrow$. □

Podobně lze dále syntakticky dokázat pravidlo rozbor případů:

$$T \vdash (\varphi \vee \psi) \to \chi \;\Leftrightarrow\; (T \vdash \varphi \to \chi \;\text{ a }\; T \vdash \psi \to \chi).$$

Pomocí něj pak distributivnost konjunkce a disjunkce a další a další tvrzení. Speciálně tak syntakticky dokážeme výrokovou variantu ($\wedge$ změněno na &, $=$ na $\leftrightarrow$) booleovských axiomů, což je asociativita, komutativita, distributivita $\vee, \wedge$, absorbce $x \vee (x \wedge y) = x = x \wedge (x \vee y)$, komplementace $x \vee (-x) = 1, x \wedge (-x) = 0$, a základních booleovských identit, což je idempotence $x \vee x = x$, $x \wedge x = x$, $-(-x) = x$, extremalita $x \vee 1 = 1$, $x \wedge 0 = 0$, neutralita $x \vee 0 = x$, $x \wedge 1 = x$, De Morgan $x \wedge y = -(-x \vee -y)$, $x \vee y = -(-x \wedge -y)$.

3.6 Problém splnitelnosti. Rezoluce.

Základní úlohou problému splnitelnosti je najít odpověď na otázku, zda daný výrok φ je splnitelný čili zda má model a objasnit, do jaké míry je tato odpověď dána efektivně. Mluvíme pak o úloze SAT pro φ. Úloha je jistě řešitelná algoritmicky tak, že se počítá $v(\varphi)$ pro $v \in {}^{\mathrm{var}(\varphi)}2$. Důležité je zjistit časovou složitost tohoto algoritmu, kterou můžeme chápat jako počet kroků vedoucí k výsledku v závislosti na velikosti vstupu. Říká se, že algoritmus pracuje v čase $f(n)$, kde $f : \mathbb{N} \to \mathbb{N}$, když pro každý vstup x potřebuje algoritmus $f(\textit{velikost}(x))$ kroků k poskytnutí výsledku. Říká se dále, že f roste nejvýše jako g, pokud existují $n_0, c \in \mathbb{N}$ tak, že pro každé $n \geq n_0$ je $f(n) \leq c \cdot g(n)$; píše se pak $f \in \mathcal{O}(g)$. Pokud algoritmus pracuje v čase $f(n)$ s f z $\mathcal{O}(g)$, říká se, že pracuje v čase $\mathcal{O}(g(n))$. Za efektivní řešitelnost se považuje algoritmická řešitelnost v polynomiálním čase, tj. v $\mathcal{O}(n^k)$ pro nějaké $k \in \mathbb{N}$. Třída úloh řešitelných v polynomiálním čase se značí P. Není obtížné zjistit, že algoritmus počítající $v(\varphi)$ je v $\mathcal{O}(n^2)$, v důsledku čehož úloha SAT pro každou formuli je řešitelná algoritmem pracujícím v čase $\mathcal{O}(n^2 \cdot 2^n)$ čili v exponenciálním čase. Lze však ukázat, že SAT je ve třídě NP všech úloh řešitelných nedeterministicky, tj. nedeterministickým Turingovým strojem, v polynomiálním čase. Navíc lze každou úlohu A z NP převést na SAT polynomiálním algoritmem; píšeme $A \leq_p$ SAT. Obě zmíněné vlastnosti SAT pak znamenají, že SAT je NP-kompletní; toto tvrzení se jmenuje Cookova věta. Zásadním problémem je, zda P $=$ NP; přitom inkluze $\subseteq$ platí. Pokud by platila rovnost, dostali bychom, že SAT je v P. Úloha najít model daného výroku φ v CNF se nazývá CNFSAT.

Rezoluce.

Ukážeme tzv. metodu rezoluce, pomocí které lze zjistit, právě kdy je daná množina T výrokových klauzulí splnitelná (čili má model).

3.6.1. **Množinová reprezentace množiny klauzulí. Rezoluční operace a uzávěr.**
Pro literál λ tvaru p resp. $\neg p$ buď $\overline{\lambda}$ literál $\neg p$ resp. p.

1. Je-li χ klauzule, je $^\circ\chi$ její množinová reprezentace – viz 3.2.4. Je-li T množina klauzulí, buď

$$^\circ T = \{^\circ\chi;\, \chi \in T\}$$

množinová reprezentace teorie T. Takové $^\circ T$ je množina konečných množin literálů.

2. Buď v ohodnocení prvovýroků. Pro konečnou množinu K literálů a množinu $\mathcal{K}$ konečných množin literálů definujeme:

$$\mathring{v}(K) = \sup\{v(\lambda);\, \lambda \in K\}, \qquad v \mathrel{\mathring{\models}} \mathcal{K} \Leftrightarrow \mathring{v}(K) = 1 \text{ pro každé } K \in \mathcal{K}.$$

Zřejmě platí: $\mathring{v}(K)$ je 1 resp. 0, právě když existuje resp. neexistuje $\lambda \in K$ s $v(\lambda) = 1$; speciálně je $\mathring{v}(\emptyset) = 0$ a není $v \mathrel{\mathring{\models}} \{\emptyset\}$. Přitom je $v \mathrel{\mathring{\models}} \emptyset$. Dále pro klauzuli χ platí $v(\chi) = \mathring{v}(^\circ\chi)$.

3. *Rezoluční operace* R je zobrazení, které každým konečným množinám literálů K, K' a literálu λ přiřadí konečnou množinu literálů takto:

$$\mathrm{R}(K, K', \lambda) = (K - \{\lambda\}) \cup (K' - \{\overline{\lambda}\}), \text{ pokud } \lambda \in K - K' \text{ a } \overline{\lambda} \in K' - K. \tag{3.8}$$

Poskytuje *rezolventu* $(K - \{\lambda\}) \cup (K' - \{\overline{\lambda}\})$ nebo není definována. Říkáme dále, že $\lambda \in K - K'$ a $\overline{\lambda} \in K' - K$ je *podmínka rezoluce* a značíme ji stručně (K, K', λ).

4. *Rezoluční uzávěr* množiny $\mathcal{K}$ konečných množin literálů je nejmenší nadmnožina $\mathcal{K}$, uzavřená na všechny operace $\mathrm{R}(*, *, \lambda)$, kde λ je literál; značíme ji $\mathrm{Rcl}(\mathcal{K})$.

VĚTA 3.6.2. (O výrokové rezoluci.) *Množina T klauzulí má model, právě když $\emptyset \notin \mathrm{Rcl}(^\circ T)$.*

Důkaz. $\Rightarrow$. Pro konečné množiny literálů K, K', literál λ, množinu $\mathcal{K}$ konečných množin literálů, ohodnocení v prvovýroků a množinu T klauzulí máme

$$\text{a) } v \mathrel{\mathring{\models}} \{K', K\} \Rightarrow v \mathrel{\mathring{\models}} \mathrm{R}(K, K', \lambda) \text{ (pokud } (K, K', \lambda)\text{)}, \qquad \text{b) } v \mathrel{\mathring{\models}} \mathcal{K} \Rightarrow v \mathrel{\mathring{\models}} \mathrm{Rcl}(\mathcal{K}),$$
$$\text{c) } T \text{ má model} \Rightarrow \emptyset \notin \mathrm{Rcl}(^\circ T).$$

a) platí, neboť když $v \mathrel{\mathring{\models}} \{K', K\}$, z $v(\lambda) = 0$ plyne $\mathring{v}(K - \{\lambda\}) = 1$ a z $v(\lambda) = 1$ plyne $\mathring{v}(K' - \{\overline{\lambda}\}) = 1$, což dává $v \mathrel{\mathring{\models}} \mathrm{R}(K, K', \lambda)$. b) je přímý důsledek a) a c) důsledek b), neboť $\mathring{v}(\emptyset) = 0$ pro každé ohodnocení v prvovýroků.

$\Leftarrow$. Nechť $\emptyset \notin \mathrm{Rcl}(^\circ T)$. Najdeme model v teorie T. Stačí najít model pro každý konečný fragment teorie T; můžeme tedy předpokládat, že T je nad nějakými konečně prvovýroky $p_0, \ldots, p_{m-1}$. Najdeme $v_m : \{p_0, \ldots, p_{m-1}\} \to 2$ s $v_m \mathrel{\mathring{\models}} {}^\circ T$; pak ovšem $v_m \models T$.

Označme $\mathcal{K} = \mathrm{Rcl}(^\circ T)$ a buď pro $n \leq m$

$$\mathcal{K}_n = \{K \in \mathcal{K};\, K \subseteq \{p_0, \ldots, p_{n-1}\} \cup \{\neg p_0, \ldots, \neg p_{n-1}\} \text{ a } p_{n-1} \in K \text{ nebo } \neg p_{n-1} \in K\}.$$

Díky $\emptyset \notin \mathcal{K}$ máme $\mathcal{K}_0 = \emptyset$, $\mathcal{K} = \bigcup_{0<n\leq m} \mathcal{K}_n$.

Pro $0 < n \leq m$ a $w : \{p_0, \ldots, p_{n-2}\} \to 2$ řekneme, že $K \in \mathcal{K}_n$ je w-senzitivní, když

$$\text{(a) pro každé } \lambda \in K - \{p_{n-1}, \neg p_{n-1}\} \text{ je } w(\lambda) = 0, \qquad \text{(b) } \{p_{n-1}, \neg p_{n-1}\} \not\subseteq K.$$

Pro $n < m$ a $w : \{p_0, \ldots, p_{n-1}\} \to 2$ s $w \overset{\circ}{\models} \bigcup_{i \le n} \mathcal{K}_i$ platí právě jedna z následujících alternativ:

$$(*)_w \qquad p_n \text{ je v každém } w\text{-senzitivním } K \in \mathcal{K}_{n+1},$$
$$(**)_w \qquad \neg p_n \text{ je v každém } w\text{-senzitivním } K \in \mathcal{K}_{n+1}.$$

Dokažme to sporem. Předpokládejme, že pro $n\,(< m)$ to neplatí. Pak existují w-senzitivní K, K' z $\mathcal{K}_{n+1}$ s $p_n \in K$, $\neg p_n \in K'$. Díky (b) platí (K, K', p_n). Označme $K_0 = \mathrm{R}(K, K', p_n)$; je $K_0 \in \mathcal{K}_i$ pro nějaké $0 < i \le n$. Speciálně máme $w \overset{\circ}{\models} \mathcal{K}_i$, tedy i $w \overset{\circ}{\models} K_0$ a pak pro nějaké $\lambda \in K_0$ je $w(\lambda) = 1$. Je ovšem $\lambda \in K \cup K'$, díky w-senzitivitě K, K' tedy $w(\lambda) = 0$ – spor.

Pro $n \le m$ sestrojíme indukcí $v_n : \{p_0, \ldots, p_{n-1}\} \to 2$ tak, že $v_0 = \emptyset$ a pro $0 < n$ platí:

$$\mathrm{i})_n \qquad v_{n-1} \subseteq v_n,$$
$$\mathrm{ii})_n \qquad v_n \overset{\circ}{\models} \bigcup_{i \le n} \mathcal{K}_i.$$

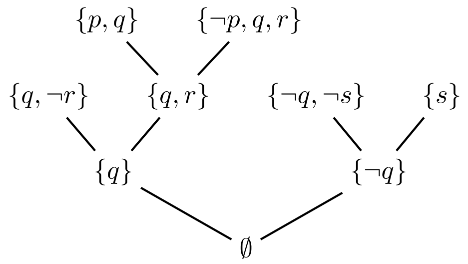
Nechť v_n s nějakým $n < m$ již máme; najdeme v_{n+1} jako $v_n \cup \{\langle p_n, k\rangle\}$ s vhodným $k < 2$ tak, aby platilo $\mathrm{ii})_{n+1}$. Když neexistuje v_n-senzitivní $K \in \mathcal{K}_{n+1}$, buď $k < 2$ libovolné. Pak platí $\mathrm{ii})_{n+1}$. Když existuje v_n-senzitivní $K \in \mathcal{K}_{n+1}$, buď $k = 1$, platí-li $(*)_{v_n}$ a $k = 0$ jinak. Pak platí $\mathrm{ii})_{n+1}$. □

Rezoluční strom.

3.6.3. Rezoluční strom.
Buď T množina klauzulí. „Vznik“ K z $\mathrm{Rcl}(^\circ T)$ znázorňuje tzv. *rezoluční strom* pro K v T. Je to konečný strom s kořenem, u jehož každého vrcholu je uveden nějaký prvek z $\mathrm{Rcl}(^\circ T)$, K je u kořene, do každého vrcholu nevstupuje buď žádná hrana (tj. jde o list) a pak je u něj prvek z $^\circ T$, nebo do něj vstupují právě dvě hrany a pak je u něj rezolventa z formulí u vrcholů, z nichž hrany vstupují.

PŘÍKLAD 3.6.4.

$\{p, q, r, s\}$-teorie T:	$\{q \vee p \vee q, \neg p \vee q \vee r, q \vee \neg r, \neg q \vee \neg s, s\}$.
Množinová reprezentace T:	$\{\{p, q\}, \{\neg p, q, r\}, \{q, \neg r\}, \{\neg q, \neg s\}, \{s\}\}$.
Rezoluční strom pro $\emptyset$ v T:	



Teorie T nemá model dle věty o výrokové rezoluci, neboť $\emptyset \in \mathrm{Rcl}(^\circ T)$.

3.7 Vícehodnotová logika.

Ukážeme jisté abstraktní zobecnění výrokové sémantiky. Pomocí ní prokážeme nevyvoditelnost některých axiomů výrokové logiky z jiných.

3.7.1. Výroková evaluace a sémantika nad ní.

1. *Výroková evaluace* je struktura $\underline{\mathsf{V}} = \langle \mathsf{V}, \neg^{\mathsf{V}}, \rightarrow^{\mathsf{V}} \rangle$, kde

$$\{0,1\} \subseteq \mathsf{V}, \quad \neg^{\mathsf{V}} \text{ je unární funkce}, \quad \rightarrow^{\mathsf{V}} \text{ je binární funkce}.$$

2. Pro *ohodnocení* $v : \mathbb{P} \rightarrow \mathsf{V}$ výrokových proměnných ve V je *hodnota* $v^{\mathsf{V}}(\varphi)$ výroku φ je sestrojená rekurzí pravidly:

$$v^{\mathsf{V}}(p) = v(p) \text{ je-li } p \text{ z } \mathbb{P}, \quad v^{\mathsf{V}}(\neg\varphi) = \neg^{\mathsf{V}}(v^{\mathsf{V}}(\varphi)), \quad v^{\mathsf{V}}(\varphi \rightarrow \psi) = v^{\mathsf{V}}(\varphi) \rightarrow^{\mathsf{V}} v^{\mathsf{V}}(\psi).$$

Říkáme, že $\underline{\mathsf{V}}$ je MP-*korektní*, pokud platí: $(v^{\mathsf{V}}(\varphi) = 1$ a $v^{\mathsf{V}}(\varphi \rightarrow \psi) = 1) \Rightarrow v^{\mathsf{V}}(\psi) = 1$.

Speciálním případem je výroková evaluace $\langle 2, -_1, \rightarrow_1 \rangle$, o které mluvíme jako o klasické dvouhodnotové výrokové evaluaci. Nad ní je sestrojena klasická dvouhodnotová sémantika výroků. Sestrojíme analogicky sémantiku nad $\underline{\mathsf{V}}$. Buď $\varphi \in \mathrm{VF}_{\mathbb{P}}$, $T, S \subseteq \mathrm{VF}_{\mathbb{P}}$, $v : \mathbb{P} \rightarrow \mathsf{V}$.

- $v \models^{\mathsf{V}} \varphi$ značí, že $v^{\mathsf{V}}(\varphi) = 1$.
- $v \models^{\mathsf{V}} T$ značí, že $v \models^{\mathsf{V}} \varphi$ pro každé φ z T. Tedy $v \models^{\mathsf{V}} \emptyset$ pro každé $v : \mathbb{P} \rightarrow \mathsf{V}$.
- $T \models^{\mathsf{V}} \varphi$ resp. $T \models^{\mathsf{V}} S$ značí, že $v \models^{\mathsf{V}} T \Rightarrow v \models^{\mathsf{V}} \varphi$ resp. $v \models^{\mathsf{V}} S$. Je-li $T = \emptyset$, nepíšeme je.
- φ je ${}^{\mathsf{V}}$-*tautologie*, když $\models^{\mathsf{V}} \varphi$.

TVRZENÍ 3.7.2. (O korektnosti.) *Nechť* $\underline{\mathsf{V}}$ *je* MP-*korektní výroková evaluace a* $T \subseteq \mathrm{VF}_{\mathbb{P}}$. *Když* φ *je* $\{\mathrm{MP}\}$-*odvozeno z* T, *tak* $T \models^{\mathsf{V}} \varphi$.

Důkaz. Indukcí na prvcích z $\{\mathrm{MP}\}\langle T \rangle$. Pro φ z T to platí a indukční krok plyne z MP-korektnosti $\underline{\mathsf{V}}$. □

3.7.3. Buď T tvořeno právě schematy (PL1), (PL2). Výrokové evaluace $\underline{\mathsf{V}} = \langle 3, \neg', \rightarrow' \rangle$ a $\underline{\mathsf{W}} = \langle 3, \neg'', \rightarrow'' \rangle$ jsou dány takto:

$\neg'$	
0	1
1	0
2	0

$\rightarrow'$	0	1	2
0	1	1	1
1	0	1	2
2	0	1	1

$\neg''$	
0	1
1	0
2	2

$\rightarrow''$ je $\rightarrow'$

A) Platí:

a) $\underline{\mathsf{V}}$ je MP-korektní a $\models^{\mathsf{V}} T \cup \{\varphi \rightarrow (\neg\varphi \rightarrow \psi)\}$. Speciálně $T \models^{\mathsf{V}} \varphi \rightarrow (\neg\varphi \rightarrow \psi)$.

b) Pro různé prvovýroky p, q platí: Není $\models^{\mathsf{V}} (\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$.
Axiom $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$ není $\{\mathrm{MP}\}$-odvozený z T.

Důkaz. a) MP-korektnost je zřejmá. $v^{\mathsf{V}}(\chi) = 1$ pro χ z $T \cup \{\varphi \rightarrow (\neg\varphi \rightarrow \psi)\}$ se zjistí propočtem. b) Buď $v(p) = 2$, $v(q) = 1$. Pak $v^{\mathsf{V}}((\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)) = (0 \rightarrow' 0) \rightarrow' (1 \rightarrow' 2) = 1 \rightarrow' 2 = 2$. □

B) Platí:

a) $\underline{\mathsf{W}}$ je MP-korektní a $\models^{\mathsf{W}} T$.

b) Pro různé prvovýroky p, q platí: Není $\models^{\mathsf{W}} p \rightarrow (\neg p \rightarrow q)$.
Formule $p \rightarrow (\neg p \rightarrow q)$ není $\{\mathrm{MP}\}$-odvozená z T.
Je však $T \models^{\mathsf{V}} p \rightarrow (\neg p \rightarrow q)$.

Důkaz. a) MP-korektnost je zřejmá a $v^{\mathsf{W}}(\chi) = 1$ pro χ z T se zjistí propočtem. b) Buď $v(p) = 2$, $v(q) = 0$. Pak $v^{\mathsf{W}}(p \rightarrow (\neg p \rightarrow q)) = 2 \rightarrow'' (\neg'' 2 \rightarrow'' 0) = 2 \rightarrow'' 0 = 0$. Odtud a z 3.7.2 plyne, že formule $p \rightarrow (\neg p \rightarrow q)$ není $\{\mathrm{MP}\}$-odvozená z T. Konečně $T \models^{\mathsf{V}} p \rightarrow (\neg p \rightarrow q)$ víme z A), a). □

3.8 Poznámky.

Kapitola 4

Kompletnost predikátové logiky

4.1 Elementární teorie dokazování. Prenexní tvar formulí.

Základní vlastnosti dedukce.

Připomeňme, že formule jazyka L predikátové logiky jsou výroky nad prvovýroky $\mathbb{P}_L$, kterými jsou právě všechny atomické a kvantifikátorem začínající L-formule. V tomto smyslu dedukce predikátové logiky obsahuje dedukci výrokové logiky. Speciálně je každá tautologie dokazatelná v predikátové logice. Protože všechny vztahy z 2.2.14, píšeme-li tam $\vdash$ místo $\models$, plynou z jistých tautologií a užitím pravidla modus ponens, platí i v predikátové logice. Shrňme to:

TVRZENÍ 4.1.1. (Základní deduktivní obraty.)

1) *Každá tautologie je dokazatelná v predikátové logice.*
2) *Platí tvrzení z* 2.2.14, *kde píšeme* $\vdash$ *místo* $\models$. *Speciálně platí následující pravidla.*

Rozbor případů:	$T \vdash (\varphi \vee \psi) \to \chi$	$\Leftrightarrow$	$(T \vdash \varphi \to \chi \text{ a } T \vdash \psi \to \chi)$.
Konjunkce:	$T \vdash \varphi \text{ a } T \vdash \psi$	$\Leftrightarrow$	$T \vdash \varphi \,\&\, \psi$.
Tranzitivita implikace:	$T \vdash \varphi \to \psi \text{ a } T \vdash \psi \to \chi$	$\Rightarrow$	$T \vdash \varphi \to \chi$.

TVRZENÍ 4.1.2. *Buď φ nějaká L-formule a T buď L-teorie.*

1) (O uzávěru.) $T \vdash \varphi \Leftrightarrow T \vdash \varphi'$, *je-li φ' uzávěr φ.*
2) (O instanci.) $T \vdash \varphi \Rightarrow T \vdash \varphi'$, *je-li φ' instance φ. Implikaci nelze obrátit.*

Důkaz. 1) Implikace $\Rightarrow$ plyne ihned z pravidla generalizace, opačná užitím axiomu substituce a pravidla modus ponens. 2) Nechť $T \vdash \varphi$. Je-li φ' tvaru $\varphi(x_1/t_1, x_2, \ldots, x_n)$, platí to na základě generalizace, axiomu substituce a pravidla modus ponens. Nechť φ' je formule $\varphi(x_1/t_1, \ldots, x_n/t_n)$; $y_1, \ldots, y_n$ buďte různé proměnné nepatřící ani φ ani φ'. Podle již dokázaného platí $T \vdash \varphi_0$, kde φ_0 je $\varphi(x_1/y_1, \ldots, x_n/y_n)$, neboť zde simultánní substituování vede k témuž, jako postupné. Touž argumentací dostaneme $T \vdash \varphi_0(y_1/t_1, \ldots, y_n/t_n)$ a poslední formule je jasně φ'. Implikaci nelze obrátit, neboť pro φ rovno $x = 0$ je $T \vdash \varphi(x/0)$, nemusí ale být $T \vdash \varphi$. □

Sémantická, jasně platná, verze tvrzení o uzávěru říká: je-li φ' uzávěr φ, tak

$$\mathcal{A} \models \varphi \Leftrightarrow \mathcal{A} \models \varphi'. \tag{4.1}$$

TVRZENÍ 4.1.3. *Pro teorii T platí:*

a)	$T \vdash \bot$	$\Leftrightarrow$	*T je sporná.*
b)	$T \vdash \bot \leftrightarrow \varphi$	$\Leftrightarrow$	*φ je vyvratitelná v T.*
c)	$T \vdash \top \leftrightarrow \varphi$	$\Leftrightarrow$	*φ je dokazatelná v T.*
d)	*T je ekvivalentní s $L(T)$-teorií $T' = \{\text{g.c.}(\varphi);\ \varphi \in T\}$, kde g.c.($\varphi$) je uzávěr φ.*		

Důkaz. Formule $\top$ je $\varphi_0 \to \varphi_0$ pro jisté φ_0 a $\bot$ je $\neg\top$. a) Implikace $\Leftarrow$ je jasná, dokazujeme $\Rightarrow$. Když $T \vdash \bot$, díky $\vdash \varphi \to \varphi$, $\vdash \neg\psi \to (\psi \to \chi)$ a modus ponens máme $T \vdash \chi$ pro každou $L(T)$-formuli χ. b) i) Buď $T \vdash \neg\varphi$. Jelikož $\neg\varphi \to (\varphi \to \bot)$ je tautologie, modus ponens dá $T \vdash \varphi \to \bot$. Jelikož $\bot \to \varphi$ je tautologie, máme $T \vdash \bot \to \varphi$. Podle základních deduktivních obratů – viz 4.1.1 – je $T \vdash \psi \leftrightarrow \chi \Leftrightarrow T \vdash \psi \to \chi$ a $T \vdash \chi \to \psi$, tedy $T \vdash \bot \leftrightarrow \varphi$ platí. ii) Buď $T \vdash \bot \leftrightarrow \varphi$. Pak $T \vdash \neg\bot \leftrightarrow \neg\varphi$ díky tautologii $(\bot \leftrightarrow \varphi) \leftrightarrow (\neg\bot \leftrightarrow \neg\varphi)$ a užitím modus ponens. Protože $T \vdash \neg\bot$ máme konečně $T \vdash \neg\varphi$. c) jako b). d) Z tvrzení o uzávěru plyne, že každý axiom T je dokazatelný v T' a naopak, tudíž je T ekvivalentní s T'. $\square$

Teorémy logiky a pravidla dokazování.

TVRZENÍ 4.1.4. *Buďte φ, ψ formule teorie T.*

1) $\vdash \varphi(x/t) \to (\exists x)\varphi$.
2) (Pravidlo $\forall$-zavedení.) $T \vdash \varphi \to \psi \Rightarrow T \vdash \varphi \to (\forall x)\psi$, *pokud x není volná proměnná φ.*
3) (Pravidlo $\exists$-zavedení.) $T \vdash \varphi \to \psi \Rightarrow T \vdash (\exists x)\varphi \to \psi$, *pokud x není volná proměnná ψ.*

Důkaz. 1) Je $\vdash (\forall x)\neg\varphi \to \neg\varphi(x/t)$, tedy pomocí tautologie a modus ponens také $\vdash \varphi(x/t) \to \neg(\forall x)\neg\varphi$ a tvrzení plyne z definice $\exists$.

2) Pravidlo generalizace dá $T \vdash (\forall x)(\varphi \to \psi)$, $(\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$ je axiom $\forall$-zavedení, užitím modus ponens pak plyne $T \vdash \varphi \to (\forall x)\psi$.

3) Je $T \vdash \neg\psi \to \neg\varphi$ pomocí modus ponens z $\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$ a $T \vdash \varphi \to \psi$, dále je $T \vdash \neg\psi \to (\forall x)\neg\varphi$ dle pravidla $\forall$-zavedení; $T \vdash (\exists x)\varphi \to \psi$ plyne pomocí zřejmých tautologií a z definice $\exists$. $\square$

VĚTA 4.1.5. *Buďte φ, ψ nějaké L-formule, T buď L-teorie.*

1) (O konstantách.) $T \vdash \varphi \Leftrightarrow T' \vdash \varphi(x_1/c_1, \dots, x_n/c_n)$, *pokud je T' extenze T o nové konstantní symboly $c_1, \dots, c_n$ (a žádný nový mimologický axiom).*
2) (O dedukci.) *Když ψ je sentence, tak* $T \vdash \psi \to \varphi \Leftrightarrow T, \psi \vdash \varphi$.
3) (Důkaz sporem.) *Když φ je sentence, tak* $(T, \neg\varphi \vdash \bot) \Rightarrow T \vdash \varphi$.

Důkaz. 1) Zřejmě $T \vdash \varphi \Rightarrow T' \vdash \varphi \Rightarrow T' \vdash \varphi(x_1/c_1, \dots, x_n/c_n)$. Nechť naopak platí vztah $T' \vdash \varphi(x_1/c_1, \dots, x_n/c_n)$; buď D příslušný důkaz a $y_1, \dots, y_n$ různé proměnné, nepatřící žádné formuli z D. Nahradíme-li v D každý výskyt c_i proměnnou y_i, $i = 1, \dots, n$, získáme tak důkaz v T formule φ_0 tvaru $\varphi(x_1/y_1, \dots, x_n/y_n)$, neboť z každého logického axiomu získáme uvedeným nahrazením logický axiom, mimologické se nových konstant netýkají a z aplikace pravidla se opět stane aplikace pravidla. Jelikož φ je $\varphi_0(y_1/x_1, \dots, y_n/x_n)$, máme $T \vdash \varphi$ podle tvrzení o instanci.

2) Implikace $\Rightarrow$ plyne ihned užitím modus ponens, dokonce bez předpokladu, že ψ je sentence. Buď nyní $T, \psi \vdash \varphi$; dokážeme $T \vdash \psi \to \varphi$, a to indukcí na teorémech teorie T, ψ.

Buď φ axiom teorie T, ψ. Je-li φ rovno ψ, je $\psi \to \varphi$ tautologie, tedy je dokazatelná v T. Je-li φ axiom T, plyne z axiomu $\varphi \to (\psi \to \varphi)$ užitím modus ponens žádané $T \vdash \psi \to \varphi$.

Buď φ odvozeno pomocí modus ponens z χ, $\chi \to \varphi$ a pro χ, $\chi \to \varphi$ nechť to platí. Odtud a z axiomu $\psi \to (\chi \to \varphi) \to ((\psi \to \chi) \to (\psi \to \varphi))$ užitím modus ponens získáme $T \vdash \psi \to \varphi$.

Buď φ odvozeno generalizací z χ a pro χ nechť tvrzení platí; φ je $(\forall x)\chi$. Pak $T \vdash \psi \to \chi$ dá indukční předpoklad a pravidlo $\forall$-zavedení dá $T \vdash \psi \to \varphi$.

3) Z $T, \neg\varphi \vdash \bot$ plyne $T \vdash \neg\varphi \to \bot$ užitím věty o dedukci. Pomocí tautologií $(\neg\varphi \to \bot) \to (\top \to \varphi)$, $(\top \to \varphi) \to \varphi$ a modus ponens pak $T \vdash \varphi$. $\square$

VĚTA 4.1.6.

1) (Pravidlo distribuce kvantifikátoru.) *Když Q je $\forall$ nebo $\exists$, tak*
$$(T \vdash \varphi \to \psi) \quad \Rightarrow \quad T \vdash (Qx)\varphi \to (Qx)\psi.$$
2) (O ekvivalenci.) *Nechť formule φ' se získá z φ nahrazením některých výskytů podformulí $\psi_1, \dots, \psi_n$ po řadě formulemi $\psi'_1, \dots, \psi'_n$. Pak platí*
$$(T \vdash \psi_1 \leftrightarrow \psi'_1, \cdots, T \vdash \psi_n \leftrightarrow \psi'_n) \quad \Rightarrow \quad T \vdash \varphi \leftrightarrow \varphi'.$$

3) (O variantách.) *Je-li* φ' *varianta* φ, *tak* $\vdash \varphi \leftrightarrow \varphi'$.

4) (Vytýkání kvantifikátorů.)

a) $\vdash (Qx)(\varphi \to \psi) \leftrightarrow (\varphi \to (Qx)\psi)$, *nemá-li* x *volný výskyt ve* φ *a* Q *je kvantifikátor.*

b) $\vdash (Qx)(\varphi \to \psi) \leftrightarrow ((Q'x)\varphi \to \psi)$, *nemá-li* x *volný výskyt ve* ψ, Q *je kvantifikátor a* Q' *je* $\exists$ *resp.* $\forall$, *pokud* Q *je* $\forall$ *resp.* $\exists$.

c) $\vdash (Qx)(\varphi \diamond \psi) \leftrightarrow ((Qx)\varphi \diamond \psi)$, *nemá-li* x *volný výskyt ve* ψ, Q *je kvantifikátor a* $\diamond$ *je* & *nebo* $\vee$.

Důkaz. 1) Z axiomu $(\forall x)\varphi \to \varphi$ a $T \vdash \varphi \to \psi$ plyne $T \vdash (\forall x)\varphi \to \psi$ a užitím pravidla $\forall$-zavedení požadované $T \vdash (\forall x)\varphi \to (\forall x)\psi$. Tvrzení pro Q rovno $\exists$ plyne z dokázaného a z definice $\exists$.

2) Indukcí dle složitosti φ. Je-li φ atomická, φ' je φ nebo některé ψ'_i a φ je ψ_i; tvrzení pak jasně platí. Indukční krok pro negaci a implikaci je snadný a pro obecnou kvantifikaci plyne z pravidla distribuce $\forall$.

3) Díky tvrzení o ekvivalenci a definici varianty stačí zřejmě dokázat, že $\vdash (\forall x)\psi \leftrightarrow (\forall y)\psi(x/y)$, není-li proměnná y volná ve ψ. Označme $\psi(x/y)$ jako ψ'; zřejmě $\psi'(y/x)$ je ψ. Jak $(\forall y)\psi' \to \psi$, tak $(\forall x)\psi \to \psi'$ je axiom substituce; pomocí pravidla $\forall$-zavedení dostaneme snadno dokazovanou ekvivalenci.

4) a) Buď Q rovno $\forall$. Stačí dokázat $\leftarrow$. $((\forall x)\psi \to \psi) \to ((\varphi \to (\forall x)\psi) \to (\varphi \to \psi))$ je tautologie a její předpoklad je axiom substituce; pomocí modus ponens a pravidla $\forall$-zavedení dostaneme žádanou implikaci.

Buď Q rovno $\exists$. Dokážeme $\to$. Jako výše je $(\psi \to (\exists x)\psi) \to ((\varphi \to \psi) \to (\varphi \to (\exists x)\psi))$ tautologie a $\vdash \psi \to (\exists x)\psi$, tedy $\vdash (\varphi \to \psi) \to (\varphi \to (\exists x)\psi)$. Užitím pravidla $\exists$-zavedení získáme dokazovaný vztah.

Dokážeme $\leftarrow$. Platí $\vdash \neg\varphi \to (\exists x)(\varphi \to \psi)$ (neboť $\vdash (\varphi \to \psi) \to (\exists x)(\varphi \to \psi)$ díky 4.1.4, 1) a $\neg\varphi \to (\varphi \to \psi)$ je tautologie) a dále $\vdash (\exists x)\psi \to (\exists x)(\varphi \to \psi)$ (užitím pravidla distribuce na tautologii $\psi \to (\varphi \to \psi)$). Pravidlo rozbor případů, $\vdash (\neg\varphi \vee (\exists x)\psi) \leftrightarrow (\varphi \to (\exists x)\psi)$ a tvrzení o ekvivalenci dají $\vdash (\varphi \to (\exists x)\psi) \to (\exists x)(\varphi \to \psi)$.

b) plyne z a), užijeme-li $\vdash (\neg\psi \to (Qx)\neg\varphi) \leftrightarrow ((Q'x)\varphi \to \psi)$ a $\vdash (\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)$.

c) plyne z a), b) a ekvivalentu $\diamond$ pomocí $\to$. □

Prenexní tvar formulí.

4.1.7. **Prenexní tvar formulí. Prenexní operace.**

1. Formule φ je v *prenexním tvaru*, má-li tvar $(Q_1x_1)\dots(Q_nx_n)\psi$, kde Q_i je $\forall$ nebo $\exists$, $x_1,\dots,x_n$ jsou navzájem různé proměnné a ψ je otevřená formule; $(Q_1x_1)\dots(Q_nx_n)$ se nazývá *prefix* a ψ *otevřené jádro* φ.

2. *Prenexní operace* na formulích jsou dány pravidly pa) – pf), přičemž Q' je $\exists$ resp. $\forall$, když Q je $\forall$ resp. $\exists$ a $\diamond$ je & nebo $\vee$; nahrazená a nahrazující formule jsou za uvedených předpokladů logicky ekvivalentní díky tvrzení o variantách, o vytýkání kvantifikátorů a zavedení $\exists$.

pa) Nahraď podformuli její variantou.
pb) Nahraď podformuli $\neg(Qx)\psi$ za $(Q'x)\neg\psi$.
pc) Nahraď podformuli $(Qx)\psi \diamond \chi$ za $(Qx)(\psi \diamond \chi)$, není-li x volná v χ.
pd) Nahraď podformuli $\psi \diamond (Qx)\chi$ za $(Qx)(\psi \diamond \chi)$, není-li x volná ve ψ.
pe) Nahraď podformuli $(Qx)\psi \to \chi$ za $(Q'x)(\psi \to \chi)$, není-li x volná v χ.
pf) Nahraď podformuli $\psi \to (Qx)\chi$ za $(Qx)(\psi \to \chi)$, není-li x volná ve ψ.

VĚTA 4.1.8. (O prenexním tvaru.) *Ke každé formuli lze nalézt pomocí prenexních operací formuli v prenexním tvaru s ní ekvivalentní.*

Důkaz. Označme φ' formuli v prenexním tvaru ekvivalentní s φ. Dokazujeme tvrzení indukcí dle složitosti φ. Atomická φ je v prenexním tvaru. Je-li φ tvaru $\neg\psi$, získáme φ' z $\neg\psi'$ po postupné aplikaci pb) a užitím tvrzení o ekvivalenci. Podobně, je-li φ tvaru $\psi \to \chi$, pomocí pa) lze docílit, že proměnné v prefixech ψ', χ' jsou různé a navíc jsou různé od proměnných volných v ψ', χ'.

Aplikací pe), pf) získáme φ'. Pro φ tvaru $(\forall x)\psi$ je φ ekvivalentní $(\forall x)\psi'$ a pomocí tvrzení pa) docílíme, aby všechny proměnné v prefixu byly různé. $\square$

Teorémy s kvantifikátory.

TVRZENÍ 4.1.9. (Teorémy s kvantifikátory.) *Následující formule jsou logicky dokazatelné, přičemž Q je kvantifikátor.*

a)	$(\forall x)(\varphi \,\&\, \psi) \leftrightarrow (\forall x)\varphi \,\&\, (\forall x)\psi$	$(\exists x)(\varphi \vee \psi) \leftrightarrow (\exists x)\varphi \vee (\exists x)\psi$
b)	$(\exists x)(\varphi \,\&\, \psi) \to (\exists x)\varphi \,\&\, (\exists x)\psi$	$(\forall x)\varphi \vee (\forall x)\psi \to (\forall x)(\varphi \vee \psi)$
c)	$(\forall x)(\forall y)\varphi \leftrightarrow (\forall y)(\forall x)\varphi$	$(\exists x)(\exists y)\varphi \leftrightarrow (\exists y)(\exists x)\varphi$
d)	$(\exists x)(\forall y)\varphi \to (\forall y)(\exists x)\varphi$	$(Qx)\varphi \leftrightarrow \varphi$, *není-li x volná ve φ*
e)	*Implikace $\to$ v* b) *a* d) *nelze obrátit.*	

Důkaz. Dokážeme nejprve

i) $\vdash (Qx)(\varphi \,\&\, \psi) \to (Qx)\varphi \,\&\, (Qx)\psi$, ii) $\vdash (\forall x)\varphi \,\&\, (\forall x)\psi \to (\forall x)(\varphi \,\&\, \psi)$.

Nechť L-formule φ, ψ mají všechny volné proměnné mezi $x, x_1, \ldots, x_n$. Buďte dále $c_1, \ldots, c_n$ nové konstantní symboly, T prázdná teorie v jazyce $L \cup \{c_1, \ldots, c_n\}$ a φ' resp. ψ' formule

$$\varphi(x, x_1/c_1, \ldots, x_n/c_n) \text{ resp. } \psi(x, x_1/c_1, \ldots, x_n/c_n).$$

i) Máme $\vdash (Qx)(\varphi \,\&\, \psi) \to (Qx)\varphi, (Qx)\psi$ z pravidla distribuce. Odtud plyne

$$T, (Qx)(\varphi' \,\&\, \psi') \vdash (Qx)\varphi', (Qx)\psi'$$

a pomocí vět o dedukci a o konstantách dostáváme i). ii) Užitím axiomu substituce, tvrzení o tautologiích a modus ponens dostaneme $T, (\forall x)\varphi', (\forall x)\psi' \vdash \varphi' \,\&\, \psi'$. Užitím generalizace a vět o dedukci a konstantách dostaneme ii).

Prvá formule z a) plyne snadno z i), ii), druhá snadno z prvé, prvá formule z b) z i), druhá snadno z prvé. c) Prvá formule. Z axiomů substituce: $\vdash (\forall x)(\forall y)\varphi \to (\forall y)\varphi$, $\vdash (\forall y)\varphi \to \varphi$; odtud díky tvrzení o tautologiích $\vdash (\forall x)(\forall y)\varphi \to \varphi$. Užitím axiomu $\forall$-zavedení pak $\vdash (\forall x)(\forall y)\varphi \to (\forall y)(\forall x)\varphi$. Ze symetrie plyne i obrácená implikace a nakonec dokazovaná ekvivalence. Druhá formule z c) plyne snadno z prvé. d) Prvá formule: $\vdash \varphi \to (\exists x)\varphi$, dle pravidla distribuce tedy $\vdash (\forall y)\varphi \to (\forall y)(\exists x)\varphi$, užitím pravidla $\exists$-zavedení pak dokazované. Druhá formule pro Q rovno $\forall$: implikace $\to$ plyne snadno z axiomu substituce, opačná z pravidla $\forall$-zavedení. Pro Q rovno $\exists$ to je důsledek právě dokázaného. e) Pro b) lze užít model $\langle 2, 0, 1\rangle$ a formule $x = 0$, $x = 1$ jazyka $\langle c_0, c_1\rangle$, pro d) pak model $\langle 2\rangle$ a formuli $x \neq y$. $\square$

Kvantifikátorová hierarchie formulí.

Kvantifikátorová hierarchie L-formulí je tvořená množinami $\forall_{n,L}$-formulí a $\exists_{n,L}$-formulí. Ty jsou definovány následovně.

4.1.10. $\forall_{n,L}$- a $\exists_{n,L}$-formule. Univerzální a existenční formule.

Buď L jazyk, $0 \leq n \in \mathbb{N}$ a T buď L-teorie.

1. $\forall_{n,L}$- *formule* a $\exists_{n,L}$-*formule* definujeme induktivně pravidly:

- $\forall_{0,L}$-*formule* a $\exists_{0,L}$-*formule* jsou právě bezkvantifikátorové formule jazyka L.
- $\forall_{n+1,L}$-formule jsou právě tvaru $(\forall \overline{x})\varphi$, kde φ je nějaká $\exists_{n,L}$-formule a $\exists_{n+1,L}$-formule jsou právě tvaru $(\exists \overline{x})\varphi$, kde φ je nějaká $\forall_{n,L}$-formule.

$\forall_{1,L}$- resp. $\exists_{1,L}$-formule se také nazývá *univerzální* resp. *existenční* L-formule; $\forall_{2,L}$-formule pak *univerzálně-existenční* L-formule – též $\forall\exists$ L-formule – atd.

2. Místo $\forall_{n,L}$-formule říkáme také $\forall_n$-*formule jazyka* L a podobně pro $\exists_n$.

3. Buď T nějaká teorie v jazyce rozšiřujícím L. $(\forall_{n,L})^T$ je množina všech $\forall_{n,L}$-*formulí v* T, tj. takových, které jsou ekvivalentní v T nějaké $\forall_{n,L}$-formuli. Podobně pro $\exists_{n,L}$.

Symbolem $(\forall_n)^L$ označíme množinu právě všech L-formulí, logicky ekvivalentních s nějakou $\forall_{n,L}$-formulí. Podobně pro $\exists_n$.

4.1.11. Zřejmě je každá $\forall_{n,L}$-formule resp. $\exists_{n,L}$-formule tvaru

$$(\forall \overline{x}^n)(\exists \overline{x}^{n-1})(\forall \overline{x}^{n-2}) \cdots (Q\overline{x}^1)\varphi \qquad \text{resp.} \qquad (\exists \overline{x}_n)(\forall \overline{x}^{n-1})(\exists \overline{x}^{n-2}) \cdots (Q\overline{x}^1)\varphi, \tag{4.2}$$

kde φ je nějaká bezkvantifikátorová L-formule. Protože každá formule je ekvivalentní formuli v prenexním tvaru, platí:

Každá L-formule je ekvivalentní nějaké $\forall_{n,L}$-formuli nebo $\exists_{n,L}$-formuli.

Navíc můžeme předpokládat, že $\overline{x}^n \smile \cdots \smile \overline{x}^1$ v (4.2) je prostá sekvence a tedy uvedený tvar je prenexní. Jinak totiž lze vzít variantu prvé formule ve tvaru $(\forall \overline{y}^n)(\exists \overline{y}^{n-1})(\forall \overline{y}^{n-2}) \cdots (Q\overline{y}^1)\varphi'$ s jistou φ' otevřenou a prostou sekvencí $\overline{y}^n \smile \cdots \smile \overline{y}^1$ (a podobně pro druhou formuli v (4.2)).

TVRZENÍ 4.1.12. *Nechť T je L-teorie.*

1) a) *Obory $(\forall_{n,L})^T$ a $(\exists_{n,L})^T$ jsou uzavřené na varianty, na tvoření instancí, na konjunkci a disjunkci. Dále $\varphi \in (\forall_{n,L})^T \Leftrightarrow \neg\varphi \in (\exists_{n,L})^T$ pro L-formuli φ.*
   b) *Pro $n > 0$ je obor $(\forall_{n,L})^T$ [$(\exists_{n,L})^T$] uzavřený na univerzální [existenční] kvantifikaci.*
2) $\mathrm{b}((\forall_{n,L})^T) = \mathrm{b}((\exists_{n,L})^T) \subseteq (\forall_{n+1,L})^T \cap (\exists_{n+1,L})^T$.
3) *Buď L s rovností, $n > 0$. Je-li φ z $(\exists_{n,L})^T$ a $T \vdash (\exists! y)\varphi(\overline{x}, y)$, je φ z $(\forall_{n,L})^T \cap (\exists_{n,L})^T$.*

Důkaz. 1) a) Tvrzení o variantách je patrné, tvrzení o instancích pak plyne z toho, že substituce termu za proměnnou formuli co do uvažovaného tvaru nezmění. Zbytek plyne užitím prenexních operací. b) Prvá část plyne přímo z definice.

2) plyne snadno, uvědomíme-li si, že „zbytečná kvantifikace“ (Qx) proměnné x nepatřící φ poskytuje formuli, ekvivalentní s φ.

3) Máme $T \vdash \neg\varphi(\overline{x}, y) \leftrightarrow (\exists y')(y' \neq y \;\&\; \varphi(\overline{x}, y/y'))$ (kde y' je různá od y a nepatřící φ). Na pravé straně $\leftrightarrow$ je formule z $(\exists_{n,L})^T$ a dle 1) a) tedy tvrzení platí. □

Teorémy a pravidla logiky s rovností.

VĚTA 4.1.13. (O rovnosti.)

1) $\vdash x = x, \quad \vdash x = y \leftrightarrow y = x, \quad \vdash x = y \to y = z \to x = z.$
2) *Buďte $t(x_1, \ldots, x_n), t_1, \ldots, t_n, s_1, \ldots, s_n$ termy a $\varphi(x_1, \ldots, x_n)$ formule teorie T.*
   a) *Nechť $T \vdash t_1 = s_1, \ldots, T \vdash t_n = s_n$ a nechť t' resp. φ' se získá z t resp. φ nahrazením některých výskytů $t_1, \ldots, t_n$ odpovídajícími termy $s_1, \ldots, s_n$. Pak platí*
   $$T \vdash t = t' \quad \text{a} \quad T \vdash \varphi \leftrightarrow \varphi'.$$
   b1) $\quad T \vdash t_1 = s_1 \to \ldots \to t_n = s_n \to t(t_1, \ldots, t_n) \;=\; t(s_1, \ldots, s_n).$
   b2) $\quad T \vdash t_1 = s_1 \to \ldots \to t_n = s_n \to \varphi(t_1, \ldots, t_n) \leftrightarrow \varphi(s_1, \ldots, s_n).$

Důkaz. 1) Dokážeme $\vdash x = y \to y = x$. Formule $x = y \to x = x \to x = x \to y = x$ je axiom rovnosti, tedy $\vdash x = y \to (x = x \to y = x)$ užitím $\vdash x = y \to x = x$ (díky $\vdash x = x$). Odtud analogicky $\vdash x = y \to y = x$. Tudíž i $\vdash y = x \to x = y$, tedy nakonec $\vdash x = y \leftrightarrow y = x$. Obdobně plyne $\vdash x = y \to y = z \to x = z$.

2) a) Indukcí dle složitosti t. Je-li t proměnná nebo konstantní symbol, je t' rovno t nebo s_i a t je t_i; $T \vdash t = t'$ tedy platí. Buď t tvaru $F(r_1, \ldots, r_m)$. Pak t' je tvaru $F(r'_1, \ldots, r'_m)$, kde $T \vdash r_i = r'_i$ pro $i = 1, \ldots, m$ dle indukčního předpokladu. Z axiomu rovnosti a substituce dostáváme $\vdash r_1 = r'_1 \to \ldots \to r_m = r'_m \to t = t'$, užitím modus ponens konečně $T \vdash t = t'$.

Indukcí podle složitosti φ. Buď φ atomická tvaru $R(r_1, \ldots, r_m)$; pak φ' je tvaru $R(r'_i, \ldots, r'_m)$, kde $T \vdash r_i = r'_i$ pro $i = 1, \ldots, m$ dle již dokázané části. Z axiomu rovnosti a substituce plyne $\vdash r_1 = r'_1 \to \ldots \to r_m = r'_m \to \varphi \to \varphi'$, užitím modus ponens konečně $T \vdash \varphi \to \varphi'$. Ze symetrie rovnosti plyne podobně i $T \vdash \varphi' \to \varphi$. Indukční krok pro $\neg$ a $\to$ plyne ihned užitím vhodných tautologií (např. $((\varphi_0 \leftrightarrow \varphi'_0) \;\&\; (\varphi_1 \leftrightarrow \varphi'_1) \to (\varphi_0 \to \varphi_1) \leftrightarrow (\varphi'_0 \to \varphi'_1))$ pro případ $\to$) a indukčního předpokladu. Indukční krok pro $\forall$ plyne užitím pravidla distribuce.

b1) Nahraďme každou proměnnou vyskytující se v t_i nebo s_i novým konstantním symbolem, kterým nahradíme tyto proměnné i v termech $t(t_1, \ldots, t_n)$, $t(s_1, \ldots, s_n)$; získáme tak t'_i a s'_i a $t'(t'_1, \ldots, t'_n)$, $t'(s'_1, \ldots, s'_n)$. Díky větě o konstantách stačí dokázat

$$T' \vdash t'_1 = s'_1 \to \ldots \to t'_n = s'_n \to t'(t'_1, \ldots, t'_n) = t'(s'_1, \ldots, s'_n),$$

kde T' je T v jazyce rozšířeném o nové konstanty. To je díky větě o dedukci ekvivalentní s $T', t'_1 = s'_1 \,\&\, \cdots \,\&\, t'_n = s'_n \vdash t'(t'_1, \ldots, t'_n) = t'(s'_1, \ldots, s'_n)$; tento vztah plyne z a). b2) se dokáže stejně. □

TVRZENÍ 4.1.14. *Není-li x proměnná termu t, je dokazatelné:*

$$1)\ \varphi(x/t) \leftrightarrow (\forall x)(x = t \to \varphi), \qquad 2)\ \varphi(x/t) \leftrightarrow (\exists x)(x = t \,\&\, \varphi).$$

Důkaz. 1) Axiom substituce dává $\vdash (\forall x)(x = t \to \varphi) \to (t = t \to \varphi(x/t))$. (Implicite se předpokládá substituovatelnost t za x do φ.) Užitím tautologie odtud plyne $\vdash t = t \to ((\forall x)(x = t \to \varphi) \to \varphi(x/t))$ a dále $\vdash (\forall x)(x = t \to \varphi) \to \varphi(x/t)$ díky $\vdash t = t$. Opačnou implikaci dokážeme pomocí

$$\vdash x = t \to (\varphi \leftrightarrow \varphi(x/t)). \tag{4.3}$$

Užitím tautologie plyne $\vdash \varphi(x/t) \to (x = t \to \varphi)$. Jelikož x není volná v $\varphi(x/t)$, pravidlo $\forall$-zavedení dá $\vdash \varphi(x/t) \to (\forall x)(x = t \to \varphi)$.

2) Z $\psi(x/t) \to (\exists x)\psi$, aplikovaného na ψ tvaru $x = t \,\&\, \varphi$ dostaneme $\vdash (t = t \,\&\, \varphi(x/t)) \to (\exists x)(x = t \,\&\, \varphi)$. Odtud díky $\vdash t = t$ máme $\vdash \varphi(x/t) \to (\exists x)(x = t \,\&\, \varphi)$. Opačná implikace. Z (4.3) plyne užitím tautologie: $\vdash (x = t \,\&\, \varphi) \to \varphi(x/t)$. Protože x není volná v $\varphi(x/t)$, pravidlem $\exists$-zavedení získáme $\vdash (\exists x)(x = t \,\&\, \varphi) \to \varphi(x/t)$. □

Protipříklady.

PŘÍKLADY 4.1.15.

a) Formule $\varphi \to (\forall x)\varphi$ není obecně pravdivá (a nelze ji tedy vzít jako axiom).
Svědčí o tom $\langle 2, \{0\}\rangle \not\models U(x) \to (\forall x)U(x)$, kde U je unární relační symbol.

b) Formule $(\forall x)\varphi \to \varphi'$, kde φ' se získá „nekorektní substitucí“ za x do φ, není obecně pravdivá.
Svědčí o tom φ tvaru $(\exists y)(x \neq y)$ a φ' tvaru $(\exists y)(y \neq y)$. Je-li $\mathcal{A}$ alespoň dvouprvková struktura, není $\mathcal{A} \models (\forall x)\varphi \to \varphi'$.

c) Formule $(\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$ není obecně pravdivá, je-li x volná ve φ.
Svědčí o tom $\langle 2, \{0\}\rangle \not\models (\forall x)(U(x) \to U(x)) \to (U(x) \to (\forall x)U(x))$, kde U je unární relační symbol.

d) V pravidlu $\forall$-zavedení „$T \vdash \varphi \to \psi \Rightarrow T \vdash \varphi \to (\forall x)\psi$, pokud x není volná proměnná φ“ nelze vynechat, že x není volná proměnná φ.
Svědčí o tom T prázdná a φ, ψ obě $U(x)$, kde U je unární relační symbol.

e) Ve větě o dedukci „$T, \psi \vdash \varphi \Rightarrow T \vdash \psi \to \varphi$, jakmile ψ je sentence“ nelze vynechat předpoklad, že ψ je sentence.
Je totiž $U(x) \vdash (\forall x)U(x)$, není však $\vdash U(x) \to (\forall x)U(x)$.

f) V tvrzení o důkazu sporem „$(T, \neg\varphi$ sporná $) \Rightarrow T \vdash \varphi$, jakmile je φ sentence“ nelze vynechat předpoklad, že φ je sentence.
Svědčí o tom T prázdná a φ tvaru $U(x) \to (\forall x)U(x)$, kde U je unární relační symbol.

g) Pokud „variujeme“ chybně x na y ve formuli φ tvaru $(\exists x)(x \neq y)$ a získáme tak φ' tvaru $(\exists y)(y \neq y)$, zřejmě není $\vdash \varphi \leftrightarrow \varphi'$.

4.2 Existence modelu, kompletnost, kompaktnost.

Budeme definovat kanonickou strukturu $\mathcal{A}$ pro teorii T a ukážeme, že je modelem T, pokud je T henkinovská a kompletní. Ukážeme dále, že každá bezesporná teorie T má kompletní henkinovskou extenzi a tedy i model, dokonce kardinality nejvýše rovné kardinalitě jazyka teorie T. Důsledkem je pak věta o kompletnosti a kompaktnosti – to je formulováno v 4.2.10. Dále uvedeme některé důsledky (viz 4.2.12 – 4.2.18).

O kompletních teoriích.

ZNAČENÍ 4.2.1. JKE je zkratka za frázi „jednoduchá/é kompletní extenze“.

TVRZENÍ 4.2.2.

1) *Teorie T je kompletní* $\Leftrightarrow$ Thm(T) *je maximální bezesporná.*
2) *Bezesporná teorie T má maximální bezespornou jednoduchou extenzi; ta je kompletní.*

Důkaz. 1) Je T ekvivalentní s Thm(T), tedy $\Rightarrow$ platí. Buď naopak Thm(T) maximální bezesporná; stačí dokázat, že Thm(T) je kompletní. Pro sentenci φ je $\mathrm{Thm}(T) \vdash \varphi$ nebo $\mathrm{Thm}(T) \vdash \neg\varphi$, neboť $\mathrm{Thm}(T) \nvdash \neg\varphi$ implikuje, že $\mathrm{Thm}(T) \cup \{\varphi\}$ je bezesporná podle tvrzení o důkazu sporem; díky maximalitě pak $\mathrm{Thm}(T) \vdash \varphi$.

2) Hledaná maximální bezesporná extenze je maximální prvek množiny $\mathcal{T}$ všech bezesporných množin $L(T)$-formulí, které rozšiřují T. Jeho existence plyne z principu maximality (ekvivalentního s axiomem výběru) aplikovaného na $\mathcal{T}$ uspořádané inkluzí; v tomto uspořádání má totiž každý řetěz majorantu, rovnu jeho sjednocení. $\square$

TVRZENÍ 4.2.3. *Buď $\mathcal{A} \models T$. Pak platí:*

1) Th$(\mathcal{A})$ *je* JKE *teorie T.*
2) Th$(\mathcal{A})$ *je maximální bezesporná množina sentencí (tj. přidáním nové $L(T)$-sentence se stane spornou).*
3) *Je-li navíc T kompletní, je* Th$(\mathcal{A})$ *ekvivalentní s T.*

Důkaz. 1) Teorie Th$(\mathcal{A})$ má model $\mathcal{A}$ a je proto bezesporná, a dále dokazuje sentenci φ, když $\mathcal{A} \models \varphi$, a dokazuje $\neg\varphi$, když $\mathcal{A} \models \neg\varphi$; tudíž to je kompletní teorie. Je to extenze T, tj. $\mathrm{Thm}(\mathrm{Th}(\mathcal{A})) \supseteq \mathrm{Thm}(T)$, neboť když $T \vdash \varphi$, tak $\mathcal{A} \models \text{g.c.}(\varphi)$, tedy $\text{g.c.}(\varphi) \in \mathrm{Th}(\mathcal{A})$ a tudíž a $\varphi \in \mathrm{Thm}(\mathrm{Th}(\mathcal{A}))$.

2) Je-li φ sentence nepatřící Th$(\mathcal{A})$, obsahuje teorie $S = \mathrm{Th}(\mathcal{A}) \cup \{\varphi\}$ i $\neg\varphi$ a díky tautologii $\varphi \to (\neg\varphi \to \psi)$ plyne z 4.1.1, že S je sporná.

3) Díky 1) zbývá dokázat, že T je extenze Th$(\mathcal{A})$. Když $\mathrm{Th}(\mathcal{A}) \vdash \varphi$, tak $\mathcal{A} \models \varphi$, tedy $\mathcal{A} \models \varphi'$, kde φ' je uzávěr φ. Díky kompletnosti T je $T \vdash \varphi'$ a tedy i $T \vdash \varphi$. $\square$

Kanonická struktura pro teorii. Henkinovské teorie.

4.2.4. **Kanonická struktura pro teorii.**

Nechť $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ je jazyk s konstantním symbolem a T je L-teorie.

1. *Konstantní struktura pro T* je $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$-struktura $\mathcal{A}$, jež je expanzí struktury $\underline{\mathrm{D}}(\mathcal{F})$ designátorů (čili konstantních L-termů), přičemž pro n-ární $R \in \mathcal{R}$ a konstantní L-termy $t_1, \ldots, t_n$ je

$$R^A(t_1, \ldots, t_n) \quad \Leftrightarrow \quad T \vdash R(t_1, \ldots, t_n).$$

Poznamenejme, že pro konstantní term t platí $t^A = t$. Je-li L bez rovnosti, říkáme, že $\mathcal{A}$ je *kanonická struktura pro T.*

2. Buď L navíc s rovností. Definujeme ekvivalenci $\sim$ na univerzu A:

$$t \sim s \quad \Leftrightarrow \quad T \vdash t = s.$$

Pak pro $t_1 \sim t'_1, \ldots, t_n \sim t'_n$ a n-ární relační symbol R resp. funkční symbol F je

$$R^A(t_1, \dots, t_n) \Leftrightarrow R^A(t'_1, \dots, t'_n) \quad \text{resp.} \quad F^A(t_1, \dots, t_n) \sim F^A(t'_1, \dots, t'_n).$$

Můžeme tedy definovat L-strukturu $\mathcal{B}$ s univerzem $B = \{t/{\sim};\ t \in A\}$ korektně pomocí reprezentantů faktorů takto: pro $R, F, t_1, \dots, t_n$ jako výše je

$$\begin{array}{rcl} R^B(t_1/{\sim}, \dots, t_n/{\sim}) & \Leftrightarrow & R^A(t_1, \dots, t_n), \\ F^B(t_1/{\sim}, \dots, t_n/{\sim}) & = & F^A(t_1, \dots, t_n)/{\sim}. \end{array}$$

Říkáme, že $\mathcal{B}$ je *kanonická struktura pro T*.

Protože pro konstantní term t je $t^A = t$, indukcí podle složitosti termu t snadno plyne:

$$t^B = t/{\sim}. \tag{4.4}$$

TVRZENÍ 4.2.5. *Nechť $\mathcal{B}$ je kanonická struktura pro teorii T. Pak $\|\mathcal{B}\| \le \|L(T)\|$ a pro každou atomickou $L(T)$-sentenci φ platí:*

$$\mathcal{B} \models \varphi \quad \Leftrightarrow \quad T \vdash \varphi. \tag{4.5}$$

Důkaz. Je $B = \{t/{\sim};\ t$ je konstantní $L(T)$-term$\}$ pro jistou ekvivalenci $\sim$, tudíž $|B| \le \|L(T)\|$. Zbytek tvrzení plyne ihned z konstrukce $\mathcal{B}$. □

Chceme najít podmínku na teorii T tak, aby kanonická struktura $\mathcal{B}$ pro T pak splňovala (4.5) pro každou $L(T)$-sentenci φ; potom by platilo $\mathcal{B} \models T$ a také, že je T kompletní. Hledanou podmínkou je, že teorie T je kompletní a tzv. henkinovská; to říká 4.2.7. Podle 4.2.8 má každá bezesporná teorie T_0 kompletní henkinovskou extenzi T; kanonická struktura pro T, zredukovaná na $L(T_0)$, je pak modelem T_0.

4.2.6. **Henkinovské konstanty, henkinovská teorie.**
Nechť T je L-teorie. Množina D (ne nutně všech) konstantních symbolů jazyka L je množina *henkinovských konstant* teorie T, když pro každou L-formuli $\varphi(x)$ s nejvýše jednou volnou proměnnou existuje konstantní symbol d z D tak, že $T \vdash (\exists x)\varphi \to \varphi(x/d)$. *Henkinovská teorie* je taková teorie, jejíž konstantní symboly tvoří množinu henkinovských konstant této teorie.

TVRZENÍ 4.2.7. (O kanonické struktuře pro kompletní henkinovskou teorii.) *Buď T kompletní henkinovská teorie, $\mathcal{A}$ kanonická struktura pro T. Pak platí:*

pro každou $L(T)$-sentenci φ je $\mathcal{A} \models \varphi \Leftrightarrow T \vdash \varphi$.

Důkaz. Říkejme, že výška φ je počet výskytů $\neg, \to$ a kvantifikací ve φ. Dokážeme indukcí, že pro každé $n \in \mathbb{N}$ platí:

$(*)_n$ Každá sentence φ výšky nejvýše n splňuje $\mathcal{A} \models \varphi \Leftrightarrow T \vdash \varphi$.

Pro $n = 0$ to platí díky (4.2.5), neboť φ je atomická sentence. Nechť platí $(*)_n$ a φ je výšky $n + 1$. Je-li φ tvaru $\neg\psi$, plyne dokazované ihned z kompletnosti T. Buď φ tvaru $\psi \to \psi'$. Nechť $\mathcal{A} \models \varphi$. Pokud $\mathcal{A} \not\models \psi$, z indukčního předpokladu a kompletnosti T plyne $T \vdash \neg\psi$ a díky tautologii $\neg\psi \to (\psi \to \psi')$ i $T \vdash \psi \to \psi'$. Pokud $\mathcal{A} \models \psi$, tak z indukčního předpokladu plyne $T \vdash \psi'$ a tedy i $T \vdash \psi \to \psi'$. Nechť $\mathcal{A} \not\models \varphi$; pak $\mathcal{A} \models \psi$ a $\mathcal{A} \not\models \psi'$, tedy $T \vdash \psi$, $T \vdash \neg\psi'$ a díky bezespornosti T i $T \nvdash \psi \to \psi'$.

Buď konečně φ tvaru $(\forall x)\psi$. Nechť D je množina henkinovských konstant teorie T. Buď $\mathcal{A} \models \varphi$. Kdyby $T \nvdash \varphi$, tj. $T \vdash \neg\varphi$, tak $T \vdash (\exists x)\neg\psi$, tudíž $T \vdash \neg\psi(d)$ pro nějaké $d \in D$. Výška $\psi(d)$ je nejvýše n, tudíž díky indukčnímu předpokladu a kompletnosti T je $\mathcal{A} \models \neg\psi(d)$, což díky $\mathcal{A} \models (\forall x)\psi$ není možné.

Buď naopak $\mathcal{A} \models \neg\varphi$, tj. $\mathcal{A} \models \neg(\forall x)\psi$. Tudíž $\mathcal{A} \models \neg\psi[a]$ pro jisté $a \in A$. Přitom a je t resp. $t/{\sim}$ s nějakým konstantním L-termem t, je-li L bez rovnosti resp. s rovností; $\sim$ je z 2. v 4.2.4.

Buď L bez rovnosti. Díky $t^A = t$ máme tedy (dle tvrzení o korektnosti substituce) $\mathcal{A} \models \neg\psi(x/t)$. Buď L s rovností. Dle (4.4) je $t^A = t/{\sim}$, máme tedy (dle tvrzení o korektnosti substituce) opět $\mathcal{A} \models \neg\psi(x/t)$. Je výška $\psi(x/t) \le n$, tedy dle indukčního předpokladu a kompletnosti T je $T \vdash \neg\psi(x/t)$, tedy $T \vdash (\exists x)\neg\psi$ a tedy $T \vdash \neg\varphi$. □

VĚTA 4.2.8. (O maximální a henkinovské extenzi.) *Každá teorie T má konzervativní henkinovskou extenzi v jazyce kardinality $\|L(T)\|$. Speciálně má každá bezesporná teorie T kompletní henkinovskou extenzi v jazyce kardinality $\|L(T)\|$.*

Důkaz. Buď L jazyk teorie T. Nechť D_n, $n \in \omega$, jsou prosté a disjunktní soubory konstantních symbolů nepatřících do L, definované indukcí takto:

$$D_0 = \langle d_{\varphi(x)};\ \varphi(x) \text{ je } L\text{-formule}\rangle,$$
$$D_n = \langle d_{\varphi(x)};\ \varphi(x) \text{ je } (L \cup \textstyle\bigcup_{i<n} D_i)\text{-formule, v níž je symbol z } D_{n-1}\rangle;$$

$d_{\varphi(x)}$ je *speciální konstanta pro* $\varphi(x)$ a $(\exists x)\varphi \to \varphi(x/d_{\varphi(x)})$ je *speciální axiom pro* $d_{\varphi(x)}$. Buď $D = \bigcup_{i\in\omega} D_i$, L' extenze L o konstantní symboly z D a T' rozšíření T o speciální axiomy pro speciální konstanty. Zřejmě $\|L'\| = \|L\|$ a D je množina henkinovských konstant teorie T' v L'.

Dokážeme, že T' je konzervativní extenze T. Extenze T_0 teorie T o nové konstantní symboly z D (bez přidání axiomů) je podle tvrzení o konstantách konzervativní extenze T; stačí tedy dokázat, že T' je konzervativní extenze T_0. Nechť χ je $L(T_0)$-formule, $T' \vdash \chi$ a $\psi_1, \ldots, \psi_m$ všechny navzájem různé speciální axiomy, vyskytující se v důkazu χ v T'; tedy

$$T_0 \vdash \psi_1 \to \psi_2 \to \cdots \to \psi_m \to \chi.$$

Indukcí podle m dokážeme, že $T_0 \vdash \chi$. Pro $m = 0$ to triviálně platí. Buď $m > 0$. Buď n největší takové, že nějaký konstantní symbol z D_n je v některé formuli ψ_i, $i = 1, \ldots, m$; můžeme předpokládat, že je v ψ_1. Nechť ψ_1 je tvaru

$$(\exists x)\varphi \to \varphi(x/d_{\varphi(x)}).$$

Pak $d_{\varphi(x)}$ není v žádné formuli $\psi_2, \ldots, \psi_m$, neboť jinak takové ψ_i je speciální axiom pro d z $D_{n'}$ s $n' > n$. Nechť proměnná y se nevyskytuje a není kvantifikovaná v žádné z formulí $\psi_1, \ldots, \psi_m, \chi$. Z tvrzení o konstantách plyne

$$T_0 \vdash ((\exists x)\varphi \to \varphi(x/y)) \to (\psi_2 \to \cdots \to \psi_m \to \chi),$$

neboť $((\exists x)\varphi \to \varphi(x/y))(y/d_{\varphi(x)})$ je ψ_1. Užitím pravidla $\exists$-zavedení pak získáme

$$T_0 \vdash (\exists y)((\exists x)\varphi \to \varphi(x/y)) \to (\psi_2 \to \cdots \to \psi_m \to \chi).$$

Tvrzení o variantách dá $T_0 \vdash (\exists x)\varphi \to (\exists y)\varphi(x/y)$, vytýkání kvantifikátorů pak $T_0 \vdash (\exists y)((\exists x)\varphi \to \varphi(x/y))$. Konečně pravidlo modus ponens dá $T_0 \vdash \psi_2 \to \cdots \to \psi_m \to \chi$ a dle indukčního předpokladu $T_0 \vdash \chi$. Speciální tvrzení plyne ještě z toho, že bezesporná teorie má dle 4.2.2 jednoduchou kompletní extenzi. □

Uveďme ještě jedno tvrzení o henkinovských teoriích.

TVRZENÍ 4.2.9. *Buď T kompletní henkinovská teorie. Pak každá $L(T)$-sentence je v T ekvivalentní bezkvantifikátorové sentenci.*

Důkaz. Buď φ nějaká $L(T)$-sentence. Dokazujeme tvrzení indukcí podle výšky φ, tj. podle počtu výskytů $\neg, \to$ a kvantifikací v φ. Pro výšku 0 není co dokazovat. Nechť to platí pro formule výšky nejvýše n. Buď φ výšky $n + 1$. Je-li φ tvaru $\neg\psi$ nebo $\psi \to \chi$, získáme dokazované tvrzení pro φ snadno užitím indukčního předpokladu a tvrzení o ekvivalenci.

Buď konečně φ tvaru $(\forall x)\psi(x)$ a D množina henkinovských konstant teorie T.

Nechť $T \vdash \neg\varphi$. Pak $T \vdash (\exists x)\neg\psi$ a tedy $T \vdash \neg\psi(d)$ pro jisté $d \in D$. Dokážeme $T \vdash \varphi \leftrightarrow \psi(d)$. Implikace $\to$ platí díky $\vdash \neg\psi(d) \to (\exists x)\neg\psi$. Dokažme $\leftarrow$. Neplatí-li to, díky kompletnosti T je $T \vdash \psi(d)\ \&\ \neg\varphi$ a T je sporná, což není možné.

Nechť $T \vdash \varphi$. Pak $T \vdash \varphi \to \psi(d)$ pro jakékoli $d \in D$. Když $T \nvdash \psi(d) \to \varphi$, tak díky kompletnosti T je $T \vdash \psi(d)\ \&\ \neg\varphi$ a T je sporná, což není možné.

Celkem tedy máme $T \vdash \varphi \leftrightarrow \psi(d)$ pro jistý konstantní symbol d a dle indukčního předpokladu je $\psi(d)$ v T ekvivalentní nějaké bezkvantifikátorové sentenci. □

Existence modelu a základní důsledky.

VĚTA 4.2.10. (O existenci modelu, kompletnosti a kompaktnosti.)

1) (O existenci modelu.) *Každá bezesporná teorie T má model kardinality nejvýše $\|L(T)\|$.*
2) (O kompletnosti.) *Formule teorie T je v T dokazatelná, právě když je v T pravdivá.*
3) (O kompaktnosti.) *Teorie má model, právě když každá její konečná část má model.*

Důkaz. 1) Hledaným modelem je redukt na $L(T)$ kanonické struktury pro nějakou maximální bezespornou henkinovskou extenzi T' teorie T v jazyce $L(T')$ kardinality $\|L(T)\|$ – viz 4.2.7, 4.2.8.

2) Pro formuli $\varphi(\overline{x})$ užitím pravidla generalizace, důkazu sporem a věty o existenci modelu máme: $T \nvdash \varphi \Leftrightarrow T \nvdash (\forall \overline{x})\varphi \Leftrightarrow T, (\exists \overline{x})\neg\varphi$ je bezesporná $\Leftrightarrow T, (\exists \overline{x})\neg\varphi$ má model $\Leftrightarrow T \not\models \varphi$.

3) plyne z toho, že teorie je sporná, právě když je nějaká její konečná část sporná. $\square$

4.2.11. Pojmy spornost, kompletnost, extenze a ekvivalence, konečná či otevřená axiomatizovatelnost teorií ev. další jsme definovali nejprve syntakticky, užitím $\vdash$, a pak jsme také uvedli i jejich sémantické varianty, získané nahrazením vztahu $\vdash$ v „syntaktické" definici vztahem $\models$. Nyní vidíme, že tyto verze jsou díky kompletnosti predikátové logiky ekvivalentní.

VĚTA 4.2.12. *Buď L jazyk s rovností.*

1) *Je-li $\kappa \geq \|L\|$, je každá nekonečná L-struktura elementárně ekvivalentní s nějakou L-strukturou kardinality κ.*
2) *Nechť T je L-teorie.*
   a) *Má-li T nekonečný model, má model každé kardinality $\geq \|L\|$.*
   b) *Má-li T pro každé $n < \omega$ alespoň n-prvkový model, má nekonečný model.*

   Důsledek: Má-li teorie T pro každé $n < \omega$ konečný model kardinality alespoň n, není třída všech konečných modelů teorie T axiomatizovatelná. Speciálně třída všech konečných L-struktur není axiomatizovatelná.
3) (Kategorické kriterium kompletnosti.) *Má-li L-teorie T jen nekonečné modely a v nějaké kardinalitě $\kappa \geq \|L\|$ až na izomorfizmus jediný model, je T kompletní.*

Důkaz. 1) Buď $\mathcal{A}$ nekonečná L-struktura, $T' = \mathrm{Th}(\mathcal{A}) \cup \{c \neq d;\ \ c, d$ jsou různé z $C\}$ teorie v jazyce L', jenž je extenzí L o κ nových konstantních symbolů tvořících C. Teorie T' je díky větě o kompaktnosti bezesporná a má tedy model $\mathcal{B}$ kardinality $\leq \|L'\| = \kappa$; je ovšem $|B| = \kappa$. Redukt $\mathcal{B}$ na L je model $\mathrm{Th}(\mathcal{A})$ kardinality κ, tedy to je hledaný model.

2) a) plyne z 1): pro nekonečný model $\mathcal{A}$ teorie T existuje s ním elementárně ekvivalentní model kardinality κ a ten je ovšem modelem T.

b) Buď T' teorie $T \cup \{c \neq d;\ \ c, d$ jsou různé z $C\}$ v jazyce L', jenž je extenzí L o spočetně nových konstantních symbolů tvořících C. Každá konečná část $S \subseteq T'$ má dle učiněných předpokladů model, dle věty o kompaktnosti má T' model; ten je ovšem nekonečný a jeho redukt na L je nekonečný model T. Důsledek plyne bezprostředně.

3) Buď $\mathcal{A} \models T$, $|A| = \kappa$. Nechť φ je L-sentence. Dokážeme, že $T \models \varphi \Leftrightarrow \mathcal{A} \models \varphi$; díky větě o kompletnosti pak $T \vdash \varphi \Leftrightarrow \mathcal{A} \models \varphi$ a T je tedy kompletní. Pro $\mathcal{B} \models T$ existuje dle 1) $\mathcal{B}' \equiv \mathcal{B}$ s $|B'| = \kappa$. Jelikož $\mathcal{B}' \cong \mathcal{A}$, máme $\mathcal{B} \models \varphi \Leftrightarrow \mathcal{B}' \models \varphi \Leftrightarrow \mathcal{A} \models \varphi$. $\square$

4.2.13. **Elementární diagram.**
Elementární diagram struktury $\mathcal{A}$ je množina všech $L(\mathcal{A}_A)$-sentencí platných v $\mathcal{A}_A$, tj. je to $\mathrm{Th}(\mathcal{A}_A)$; značí se též

$$\Delta^e(\mathcal{A}).$$

TVRZENÍ 4.2.14. *Nechť $\mathcal{A}$, $\mathcal{B}$ jsou L-struktury.*

1) *Zobrazení $h : A \to B$ je elementární vnoření $\mathcal{A}$ do $\mathcal{B} \Leftrightarrow \langle \mathcal{B}, ha \rangle_{a \in A} \models \Delta^e(\mathcal{A})$.*
2) *Je-li $\mathcal{C} \models \Delta^e(\mathcal{A})$, je redukt struktury $\mathcal{C}$ na L až na izomorfizmus elementární extenze $\mathcal{A}$.*

Důkaz plyne snadno z definic. □

VĚTA 4.2.15. (Löwenheim-Skolemova nahoru.) *Buď L jazyk s rovností, $\mathcal{A}$ nekonečná L-struktura. Struktura $\mathcal{A}$ má elementární extenzi libovolné kardinality alespoň rovné $\|L\| + \|\mathcal{A}\|$.*

Důkaz. Buď $\kappa \geq \|L\| + \|\mathcal{A}\| = \|L_A\|$ kardinál a C buď κ-prvková množina nových konstantních symbolů. Teorie $\mathrm{Th}(\mathcal{A}_A) \cup \{c \neq d;\ c, d$ jsou různé z $C\}$ je bezesporná, má tedy model kardinality nejvýše κ. Je to však zřejmě model mohutnosti právě κ; jeho L-redukt je, až na izomorfizmus, hledaným elementárním rozšířením. □

TVRZENÍ 4.2.16. (O kompletních teoriích.)

1) a) *Bezesporná teorie je kompletní, právě když jsou její každé dva modely elementárně ekvivalentní.*

   b) *Bezesporná teorie v jazyce s rovností je kompletní a má konečný model, právě když jsou její každé dva modely izomorfní.*

2) (O JKE.) *Buď $\mathcal{T}$ neprázdná množina* JKE *teorie T a taková, že $\mathcal{A} \models T \Rightarrow$ existuje $T' \in \mathcal{T}$ tak, že $\mathcal{A} \models T'$. Pak je v $\mathcal{T}$, až na ekvivalenci teorií, každá* JKE *teorie T.*

Důkaz. Buď T uvažovaná teorie. 1) a) Implikace $\Rightarrow$ je jasná; dokážeme opačnou. Existuje $\mathcal{A} \models T$. Buď φ sentence teorie T a $T \not\vdash \varphi$. Pak $\mathcal{A} \models \neg\varphi$, tudíž $T \models \neg\varphi$ díky tomu, že každé dva modely teorie T jsou elementárně ekvivalentní. Nakonec $T \vdash \neg\varphi$ plyne z věty o kompletnosti.

b) Díky 2.3.3 stačí dokázat implikaci $\Leftarrow$. Jelikož dva izomorfní modely jsou elementárně ekvivalentní, plyne to z a) a z 4.2.12, 2) a).

2) Buď S nějaká JKE teorie T, $\mathcal{A} \models S$. Pak existuje $T' \in \mathcal{T}$ s T' ekvivalentní $\mathrm{Th}(\mathcal{A})$; tudíž je i S ekvivalentní T'. □

PŘÍKLADY 4.2.17.

1. Nearchimedovské těleso.

Pro každou nekonečnou kardinalitu κ existuje uspořádané nearchimedovské těleso velikosti κ elementárně ekvivalentní s uspořádaným tělesem $\underline{\mathbb{R}}' = \langle \mathbb{R}, \leq \rangle$ reálných čísel. Přitom uspořádané těleso je *archimedovské*, když v něm pro každé jeho dva prvky $a, b > 0$ existuje n s $b < na$; těleso $\underline{\mathbb{R}}'$ je archimedovské.
Důkaz. Buď $S = \mathrm{Th}(\underline{\mathbb{R}}') \cup \{n1 \leq c;\ n < \omega\}$, kde c je konstantní symbol nepatřící do jazyka uspořádaných těles. Pak je S bezesporná, neboť každý její konečný fragment má model, snadno sestrojitelný pomocí $\underline{\mathbb{R}}'$. Protože jazyk teorie S je spočetný, existuje pro každé $\kappa \geq \omega$ model $\mathcal{A} \models S$ kardinality κ; jeho redukt má požadované vlastnosti. □

2. Nestandardní model přirozených čísel.

Existuje spočetný model elementárně ekvivalentní se standardním modelem $\underline{\mathbb{N}}$ přirozených čísel, který není izomorfní s $\underline{\mathbb{N}}$.
Důkaz. Buď $S = \mathrm{Th}(\underline{\mathbb{N}}) \cup \{\underline{n} \leq c;\ n < \omega\}$, kde c je nový konstantní symbol, nepatřící do jazyka aritmetiky. Pak je S bezesporná, neboť každý její konečný fragment má model sestrojitelný snadno pomocí $\underline{\mathbb{N}}$. Jelikož jazyk S je spočetný, má S spočetný model; jeho redukt na jazyk aritmetiky je hledaný – je to tzv. nestandardní model přirozených čísel. □

O axiomatizovatelnosti.

VĚTA 4.2.18. (O konečné a otevřené axiomatizovatelnosti.)

1) *Třída K nějakých L-struktur je konečně axiomatizovatelná, právě když K i $-\mathsf{K}$ je axiomatizovatelná.*

2) *Teorie v jazyce s rovností je axiomatizovatelná otevřenými formulemi, právě když každá podstruktura jejího modelu je jejím modelem.*

Důkaz. 1) Implikace $\Rightarrow$ je jasná. Dokážeme opačnou. Nechť T, S jsou takové L-teorie, že $\mathsf{K} = \mathsf{M}(T) = -\mathsf{M}(S)$. Pak $\mathsf{M}(T \cup S) = \mathsf{M}(T) \cap \mathsf{M}(S) = \emptyset$, tedy díky kompaktnosti existují $T' \subseteq T$, $S' \subseteq S$ konečné tak, že $T' \cup S'$ nemá model; pak $\emptyset = \mathsf{M}(T' \cup S') = \mathsf{M}(T') \cap \mathsf{M}(S')$. Konečně $\mathsf{M}(T) \subseteq \mathsf{M}(T') \subseteq -\mathsf{M}(S') \subseteq -\mathsf{M}(S) \subseteq \mathsf{M}(T)$, tedy $\mathsf{M}(T) = \mathsf{M}(T')$.

2) Označme T uvažovanou teorii a L její jazyk.

a) Implikace $\Rightarrow$. Když $\mathcal{B} \subseteq \mathcal{A} \models \varphi$ a φ je otevřená L-formule, tak $\mathcal{B} \models \varphi$.

b) Implikace $\Leftarrow$. Buď T' množina všech otevřených L-formulí dokazatelných v T; dokážeme, že L-teorie T' je ekvivalentní T, což díky kompletnosti právě znamená $\mathsf{M}(T') = \mathsf{M}(T)$. Stačí dokázat, že $\mathsf{M}(T') \subseteq \mathsf{M}(T)$ (neboť inkluze $\supseteq$ je triviální). Buď $\mathcal{B} \models T'$; dokazujeme $\mathcal{B} \models T$. Stačí najít $\mathcal{A} \models T$ s $\mathcal{B} \subseteq \mathcal{A}$. Nechť T_0 je L_B-teorie s axiomatikou T a T_1 je extenze T_0 o všechny bezkvantifikátorové L_B-sentence platné v $\mathcal{B}_B$. T_1 má model, jak dokážeme níže. Takový model je tvaru $\langle \mathcal{A}, c_b^* \rangle_{b \in B}$, přičemž $\mathcal{A} \models T$ a c_b^* je interpretace jména c_b prvku b z B. Pak je $\mathcal{B}$ vnořeno do $\mathcal{A}$ zobrazením $h(b) = c_b^*$ (pro $b \in B$), neboť pro atomickou $\varphi(\overline{x})$ a $\overline{b} \in B^{\mathrm{l}(\overline{x})}$ je $\mathcal{B} \models \varphi[\overline{b}] \Leftrightarrow \mathcal{B}_B \models \varphi(\overline{b}) \Leftrightarrow \mathcal{A}_{h[B]} \models \varphi(c_{b_0}^*, \dots) \Leftrightarrow \mathcal{A} \models \varphi[h\overline{b}]$. Tedy $\mathcal{B}$ je (až na izomorfizmus) podstruktura $\mathcal{A}$. Zbývá dokázat bezespornost T_1. Je-li T_1 sporná, existuje bezkvantifikátorová L_B-sentence ψ platná v $\mathcal{B}_B$ tak, že T, ψ je sporná teorie, tedy $T \vdash \neg\psi$. Podle věty o konstantách i $T \vdash \neg\psi'$, kde ψ' se získá z ψ nahrazením každého výskytu jména v ní novou proměnnou. Pak $\neg\psi'$ je v T', tedy $\mathcal{B} \models \neg\psi'$ a speciálně $\mathcal{B}_B \models \neg\psi$ – spor. □

PŘÍKLADY 4.2.19. Neaxiomatizovatelné třídy.

1. Teorie FL_0 těles charakteristiky 0 není konečně axiomatizovatelná.

Důkaz. Buď L jazyk teorie těles. Třída $\mathsf{K} = \{\mathcal{A} \models L;\ \mathcal{A} \models \mathrm{FL}_0\}$ všech těles charakteristiky 0 totiž není konečně axiomatizovatelná, neboť $-\mathsf{K}$ není axiomatizovatelná. Kdyby totiž S axiomatizovala $-\mathsf{K}$, tak, značí-li FL teorii těles, $S' = S \cup \mathrm{FL} \cup \{p1 \neq 0;\ p \text{ je prvočíslo}\}$ by byla bezesporná, neboť těleso $\mathbb{Z}_p \in -\mathsf{K}$ a je to model fragmentu $S \cup \mathrm{FL} \cup \{q1 \neq 0;\ q < p,\ q \text{ je prvočíslo}\}$. Její model patří do $-\mathsf{K}$ i K – spor. □

2. Třída $\mathsf{K} = \{\mathcal{A};\ \mathcal{A} = \langle A, \leq \rangle \models \text{ je dobré uspořádání}\}$ všech dobrých uspořádání není axiomatizovatelná. Přitom dobré uspořádání je takové lineární uspořádání, jehož každá neprázdná podmnožina má nejmenší prvek.

Důkaz. Sporem. Nechť S axiomatizuje K, $S' = S \cup \{c_{i+1} \leq c_i \ \&\ c_{i+1} \neq c_i;\ i \in \mathbb{N}\}$, kde c_i jsou nové konstantní symboly. Pak S' je bezesporná, neboť existuje nekonečné dobré uspořádání; to dovoluje sestrojit model každého konečného fragmentu teorie S'. Tudíž S' má model $\mathcal{A}$. Jeho redukt $\langle A, \leq^A \rangle$ na jazyk $\langle \leq \rangle$ uspořádání je dobré uspořádání. Avšak množina $\{c_i^A;\ i \in \mathbb{N}\}$ nemá v $\langle A, \leq^A \rangle$ nejmenší prvek. □

3. Třída K všech Booleových algeber izomorfních nějaké potenční Booleově algebře není axiomatizovatelná, neboť v K není spočetná Booleova algebra.

4.3 Extenze teorie o funkční symbol a definicemi.

Nadále, není-li řečeno jinak, pracujeme v logice s rovností.

Extenze teorie o funkční symbol. Skolemova varianta.

VĚTA 4.3.1. (Extenze o funkční symbol.) *Buď* $T \vdash (\exists y)\psi(x_1,\dots,x_n,y)$ *a nechť* T' *je extenze* T *o axiom* $\psi(y/F(x_1,\dots,x_n))$, *kde* F *je* n*-ární funkční symbol (eventuálně nulární), nevyskytující se v* $L(T)$ *(a* $F(x_1,\dots,x_n)$ *je substituovatelné za* y *do* ψ*). Pak je* T' *konzervativní extenze* T*.*

Důkaz. Nechť $T' \vdash \varphi$ a φ je $L(T)$-formule. Buď $\mathcal{A} \models T$ a $f : A^n \to A$ taková funkce, že pro každé $\langle a_1,\dots,a_n\rangle \in A^n$ platí $\mathcal{A} \models \psi[a_1,\dots,a_n,f(a_1,\dots,a_n)]$; tu sestrojíme užitím axiomu výběru. Pak expanze $\mathcal{A}'$ struktury $\mathcal{A}$ o funkci f je model T', tedy $\mathcal{A}' \models \varphi$, tedy i $\mathcal{A} \models \varphi$. Z věty o kompletnosti plyne $T \vdash \varphi$. □

Věta 4.3.1 umožní dokázat větu 4.3.3, a to pomocí Skolemovy varianty formule.

4.3.2. **Skolemova varianta.**

Připomeňme, že univerzální formule v prenexním tvaru je formule v prenexním tvaru taková, že všechny kvantifikce v ní jsou univerzální.

Buď φ sentence v prenexním tvaru. Uzavřená univerzální formule v prenexním tvaru φ_S s vlastností $\vdash \varphi_S \to \varphi$ a zvaná *Skolemova varianta* formule φ se sestrojí následovně.

Nechť φ' je φ pro φ univerzální v prenexním tvaru a φ' je $(\forall x_1,\dots,x_n)\psi(y/F(x_1,\dots,x_n))$, pokud φ má tvar $(\forall x_1,\dots,x_n)(\exists y)\psi$ (s $n \geq 0$), přičemž F je nový n-ární funkční symbol; substituce je korektní díky prostotě sekvence proměnných v prefixu. Formule φ' má o jeden existenční kvantifikátor méně než φ, některá formule $\varphi''^{\cdots\prime}$ je tedy univerzální v prenexním tvaru a prvou takovou označme φ_S. Platí

$$\vdash \psi(y/F(x_1,\dots,x_n)) \to (\exists y)\psi,$$

tedy i $\vdash \varphi' \to \varphi$. Odtud plyne $\vdash \varphi_S \to \varphi$. Dále opakovanou aplikací 4.3.1 dostaneme, že

$$T \vdash \varphi \quad \Rightarrow \quad T, \varphi_S \text{ je konzervativní extenze } T. \tag{$*$}$$

VĚTA 4.3.3. *Každá teorie má otevřenou konzervativní extenzi.*

Důkaz. Buď T uvažovaná teorie. $L(T)$-teorie T_1 tvořená prenexními tvary uzávěrů axiomů T je ekvivalentní s T; to plyne z věty o prenexních tvarech a uzávěru. Buď $T_2 = T_1 \cup S$, kde $S = \{\varphi_S;\ \varphi \in T_1\}$. Přitom pro různá φ jsou do φ_S přidány různé nové funkční symboly. Pro $S_0 \subseteq S$ konečné dle $(*)$ je $T_1 \cup S_0$ konzervativní extenze T_1, tedy i T_2 je konzervativní extenze T_1. Každý axiom z T_1 je dokazatelný v S, tedy je S ekvivalentní s T_2 a speciálně konzervativní extenze T. Nahraďme každý axiom z S otevřenou formulí, jíž je generálním uzávěrem; získaná teorie je otevřená a ekvivalentní s S, tedy to je hledaná konzervativní extenze teorie T. □

PŘÍKLADY. 1. Teorie Booleových algeber je otevřená teorie. Tedy podstruktura Booleovy algebry je Booleova algebra.

2. Teorie grup v jazyce $\langle +, -, 0\rangle$ je otevřená; pak je podstruktura grupy grupa.

V jazyce $\langle +, 0\rangle$ je třeba axiom $x + (-x) = 0 \;\&\; 0 = (-x) + x$ zapsat jako $(\exists y)(x + y = 0 \;\&\; 0 = y + x)$. Axiomatika pak již není otevřená. Je $\langle \mathbb{Z}, +, 0\rangle$ grupa, $\langle \mathbb{N}, +, 0\rangle$ její podstruktura, která není grupou.

Extenze teorie o definovaný symbol.

4.3.4. **Extenze teorie o definovaný symbol.**

1. Nechť R je n-ární predikátový symbol nepatřící do jazyka $L(T)$ a $\chi(x_1,\dots,x_n)$ formule jazyka $L(T)$. Generální uzávěr formule

$$R(x_1,\dots,x_n) \leftrightarrow \chi(x_1,\dots,x_n)$$

je tzv. *definující axiom* R. Teorie v jazyce $L(T)$ rozšířeném o $\{R\}$ s axiomy T a uvedeným axiomem je *extenze teorie* T *o* formulí χ *definovaný relační symbol* R.

2. Buď F nějaký n-ární funkční symbol nepatřící do $L(T)$ a $\varphi(x_1,\dots,x_n,y)$ formule jazyka L. Nechť v T je dokazatelné

$$(\forall x_1,\dots,x_n)(\exists y)\chi(x_1,\dots,x_n,y),$$
$$(\forall x_1,\dots,x_n)(\forall y,y')((\chi(x_1,\dots,x_n,y)\ \&\ \chi(x_1,\dots,x_n,y'))\to y=y');$$

tyto dva vztahy nazýváme po řadě *podmínka existence* a *jednoznačnosti definice n-árního funkčního symbolu* formulí $\chi(x_1,\dots,x_n,y)$ v T. Generální uzávěr formule

$$F(x_1,\dots,x_n)=y\leftrightarrow\chi(x_1,\dots,x_n,y)$$

je tzv. *definující axiom F*. Teorie v jazyce $L(T)$ rozšířeném o $\{F\}$ s axiomy T a uvedeným axiomem je *extenze teorie T o* formulí χ *definovaný funkční symbol F.*

Pokud speciálně se v χ proměnné $x_1,\dots,x_n$ nevyskytují, získáváme tak definovaný nulární funkční symbol, čili *definovaný konstantní symbol.*

Upozorněme na speciální případ, kdy definující axiom je

$$F(x_1,\dots,x_n)=y\leftrightarrow t(x_1,\dots,x_n)=y$$

a t je term; zde je ovšem splněná podmínka existence a jednoznačnosti.

LEMMA 4.3.5. *Extenze teorie T o definovaný symbol je konzervativní extenze T.*

Důkaz. V případě funkčního symbolu to plyne z 4.3.1. Uvažovaná extenze T' je totiž ekvivalentní s extenzí T o axiom $\chi'(y/F(x_1,\dots,x_n))$, kde χ' je jistá varianta χ. V případě relačního symbolu plyne tvrzení užitím zřejmé modifikace důkazu 4.3.1. □

4.3.6. **Překlad definovaného symbolu.**

Buď T' extenze teorie T o nějaký formulí χ definovaný n-ární relační resp. funkční symbol R resp. F, přičemž všechny volné proměnné χ jsou mezi navzájem různými proměnnými $x_1,\dots,x_n$ resp. $x_1,\dots,x_n,y$.

Buď φ formule jazyka $L(T')$. Nechť χ' je varianta χ, ve které není žádná proměnná formule φ ani vázaná ani kvantifikovaná; pak každý term vyskytující se ve φ je substituovatelný do χ' za x_i, $i=1,\dots,n$. dR- resp. dF-*překlad φ do T* (závislý na χ') je formule φ^* jazyka $L(T)$, kterou získáme podle (dR) resp. (dF) uvedených níže, jde-li o relační resp. funkční symbol R resp. F.

(dR) φ^* se získá z φ nahrazením každé podformule $R(t_1,\dots,t_n)$ formulí $\chi'(t_1,\dots,t_n)$.

(dF) φ^* se získá z φ nahrazením každé atomické podformule ψ formulí ψ^*, přičemž pro ψ atomickou je ψ^* definováno indukcí podle počtu výskytů F ve ψ: Je-li tento počet 0, buď ψ^* rovno ψ. Jinak je ψ tvaru $\psi_0(z/F(t_1,\dots,t_n))$, kde ψ_0 je atomická formule obsahující o jeden výskyt F méně než ψ, $t_1,\dots,t_n$ neobsahují F a dále z nepatří formulím χ', ψ; buď pak ψ^* následující formule (substituce jsou korektní):

$$(\exists z)(\chi'(x_1/t_1,\dots,x_n/t_n,y/z)\ \&\ \psi_0^*).\tag{4.6}$$

Vezmeme-li místo χ' jinou variantu s vlastnostmi uvedenými pro χ', bude zřejmě překlad sestrojený pomocí ní variantou φ^* a tedy ekvivalentní s φ^*. Dále $(\neg\varphi)^*$ je $\neg\varphi^*$, $(\varphi\to\psi)^*$ je $\varphi^*\to\psi^*$, volné proměnné φ jsou právě volné proměnné φ^*.

VĚTA 4.3.7. (O překladu definovaného symbolu.) *Když T' je extenze T o definovaný symbol S, tak pro $L(T')$-formuli φ a její dS-překlad φ^* platí*

$$\text{a)}\ \ T'\vdash\varphi\leftrightarrow\varphi^*,\qquad \text{b)}\ \ T'\vdash\varphi\ \Leftrightarrow\ T\vdash\varphi^*.$$

Důkaz. Dokážeme $T'\vdash\varphi\leftrightarrow\varphi^*$; protože T' je dle 4.3.5 konzervativní extenze T, plyne odtud b). Nechť S je n-ární symbol definovaný formulí χ a χ' buď varianta χ, v níž není žádná proměnná formule φ vázaná ani kvantifikovaná, přičemž překlad φ^* je sestrojený pomocí χ'.

Nechť S je relační symbol R a χ je $\chi(x_1,\dots,x_n)$. Pak $T'\vdash R(t_1,\dots,t_n)\leftrightarrow\chi'(x_1/t_1,\dots,x_n/t_n)$ platí pro termy $t_1,\dots,t_n$ vyskytující se ve φ; to plyne z tvrzení o variantách, z axiomu substituce a pravidla modus ponens. Z věty o ekvivalenci plyne pak ihned $T'\vdash\varphi\leftrightarrow\varphi^*$.

Nechť S je funkční symbol F a χ je $\chi(x_1, \dots, x_n, y)$. Stačí dokázat $T' \vdash \varphi \leftrightarrow \varphi^*$ pro φ atomickou; označme ji ψ. Provedeme to indukcí podle počtu výskytů F v ψ. Je-li tento počet 0, platí to. Jinak, jako v (dF), je ψ tvaru $\psi_0(z/F(t_1, \dots, t_n))$, kde ψ_0 je atomická formule obsahující o jeden výskyt F méně než ψ, $t_1, \dots, t_n$ neobsahují F, z není kvantifikovaná v χ' a ψ^* je (4.6). Tvrzení o variantách, axiom substituce a pravidlo modus ponens dají $T' \vdash F(t_1, \dots, t_n) = z \leftrightarrow \chi'(x_1/t_1, \dots, x_n/t_n, y/z)$, tvrzení o ekvivalenci pak $T' \vdash (\exists z)(F(t_1, \dots, t_n) = z \;\&\; \psi_0^*) \leftrightarrow \psi^*$; máme tedy $T' \vdash \psi_0^*(z/F(t_1, \dots, t_n)) \leftrightarrow \psi^*$. Dle indukčního předpokladu je $T' \vdash \psi_0 \leftrightarrow \psi_0^*$, tedy i $T' \vdash \psi_0(z/F(t_1, \dots, t_n)) \leftrightarrow \psi^*$. □

4.3.8. **Extenze teorie o definice.**

Extenze (rozšíření) teorie o definice, též *definicemi* je taková její extenze, která se získá postupným rozšiřováním o definovaný relační či funkční symbol.

Postupné rozšiřování zde znamená konstrukci rekurzí, a to eventuálně transfinitní, kdy v limitních krocích se sjednotí všechny již získané teorie.

VĚTA 4.3.9. (O extenzi teorie o definice.) *Extenze T' teorie T o definice je konzervativní. Model teorie T lze jednoznačně expandovat do modelu T'.*

Důkaz. V každém kroku při sestrojování T' máme dle 4.3.5 konzervativní extenzi T, speciálně je T' konzervativní extenze T.

Je-li $\mathcal{A} \models T$, v každém kroku při sestrojování T' máme také jednoznačnou expanzi do modelu právě získané teorie, neboť model $\mathcal{A}_0$ jakékoli teorie T_0 lze jednoznačně expandovat do modelu extenze T_0' teorie T_0 o definovaný symbol. Jde-li totiž o formulí χ definovaný n-ární funkční symbol F, je expanze $\mathcal{A}_0'$ struktury $\mathcal{A}_0$ o funkci

$$f = \{\langle a_1, \dots, a_n, b\rangle \in A_0^{n+1};\ \mathcal{A}_0 \models \chi[a_1, \dots, a_n, b]\}$$

model T_0' a zřejmě je $\mathcal{A}_0'$ jediná expanze $\mathcal{A}_0$, která je modelem T_0'. Obdobně je tomu s extenzí o definovaný relační symbol. □

Užitečné je následující tvrzení o vztahu teorie T a její extenze T' o definice:

TVRZENÍ 4.3.10. *Buď T' a extenze teorie T o definice. Pak platí:*

1) *T je kompletní $\Leftrightarrow$ T' je kompletní.*
2) *T má prvomodel $\Leftrightarrow$ T' má prvomodel.*
3) $\mathrm{I}(\kappa, T) = \mathrm{I}(\kappa, T')$ *pro každou nenulovou velikost κ.*
4) a) *T má eliminaci kvantifikátorů $\Rightarrow$ T' má eliminaci kvantifikátorů.*
   b) *T je modelově kompletní $\Rightarrow$ T' je modelově kompletní.*
   c) *Implikace v* a), b) *nelze obrátit.*

Důkaz. Buď L resp. L' jazyk T resp. T'. Pro L'-formuli $\varphi'(\overline{x})$ buď $\varphi(\overline{x})$ „překlad φ' do T“, tj. φ je L-formule s $T' \vdash \varphi' \leftrightarrow \varphi$. Dále pro $\mathcal{A} \models T$ resp. $\mathcal{A}' \models T'$ buď $\mathcal{A}'$ resp. $\mathcal{A}$ jednoznačná expanze $\mathcal{A}$ do modelu T' resp. redukt $\mathcal{A}'$ na jazyk L.

1) plyne bezprostředně z definic.

2) Buď $\mathcal{A}'$ prvomodel teorie T'. Pak redukt $\mathcal{A}$ je prvomodel T, neboť pro $\mathcal{B} \models T$ existuje elementární vnoření $\mathcal{A}'$ do $\mathcal{B}'$ a to je ovšem také elementární vnoření $\mathcal{A}$ do $\mathcal{B}$. Buď $\mathcal{A}$ prvomodel T. Pak expanze $\mathcal{A}'$ je prvomodel T'. Pro $\mathcal{B}' \models T'$ totiž existuje elementární vnoření h modelu $\mathcal{A}$ do $\mathcal{B}$. To je také elementární vnoření $\mathcal{A}'$ do $\mathcal{B}'$. Je-li totiž $\varphi'(\overline{x})$ nějaká L'-formule a $\overline{a} \in A^{\mathrm{l}(\overline{a})}$, máme

$$\mathcal{A}' \models \varphi'[\overline{a}] \quad\Leftrightarrow\quad \mathcal{A} \models \varphi[\overline{a}] \quad\Leftrightarrow\quad \mathcal{B} \models \varphi[h\overline{a}] \quad\Leftrightarrow\quad \mathcal{B}' \models \varphi'[h\overline{a}].$$

3) Zřejmě platí pro $\mathcal{A} \models T$, $\mathcal{B} \models T$, $\mathcal{A}' \models T'$, $\mathcal{B}' \models T'$:

$$\mathcal{A} \cong \mathcal{B} \quad\Leftrightarrow\quad \mathcal{A}' \cong \mathcal{B}'.$$

Je-li K resp. K' množina obsahující pro každou třídu ekvivalence $\cong$ na $\mathsf{M}(\kappa, T)$ resp. $\mathsf{M}(\kappa, T')$ právě jednu strukturu z ní (výběr z $\cong$-faktorů), je zobrazení $\mathsf{K} \ni \mathcal{A} \mapsto \mathcal{A}' \in \mathsf{K}'$ prosté zobrazení K na K'; tedy $|\mathsf{K}| = |\mathsf{K}'|$. Máme konečně $\mathrm{I}(\kappa, T) = |\mathsf{K}| = |\mathsf{K}'| = \mathrm{I}(\kappa, T')$.

4) a) Pro L'-formuli $\varphi'(\overline{x})$ s $\mathrm{l}(\overline{x}) > 0$ a její „překlad φ do T“ existuje $\varphi_0(\overline{x})$ otevřená tak, že $T \vdash \varphi \leftrightarrow \varphi_0$; pak $T' \vdash \varphi' \leftrightarrow \varphi_0$.

b) Buďte $\mathcal{A}' \subseteq \mathcal{B}'$ modely T', $\varphi'(\overline{x})$ nějaká L'-formule, $\overline{a} \in A^{\mathrm{l}(\overline{x})}$. Máme jasně: $\mathcal{A}' \models \varphi'[\overline{a}] \Leftrightarrow \mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B}' \models \varphi'[\overline{a}]$.

c) Svědčí o tom teorie T rovna SC a její extenze T' o axiom $0 = y \leftrightarrow (\forall x)(\mathrm{S}x \neq y)$. SC není modelově kompletní, neboť např. $\langle \mathbb{N} - \{0\}, \mathrm{S}\rangle \subseteq \langle \mathbb{N}, \mathrm{S}\rangle \models \mathrm{SC}$, $\langle \mathbb{N} - \{0\}, \mathrm{S}\rangle \not\prec \langle \mathbb{N}, \mathrm{S}\rangle$. T' je ekvivalentní s teorií SC_0, a ta má eliminaci kvantifikátorů. $\square$

PŘÍKLAD 4.3.11.

Teorie SC_0 je kompletní, má prvomodel $\langle \mathbb{N}, \mathrm{S}, 0\rangle$, má eliminaci kvantifikátorů a je tedy i modelově kompletní.

1) Buď SC_0' extenze teorie SC_0 o definici konstantního symbolů 1: $1 = y \leftrightarrow y = \mathrm{S}0$.
Dle 4.3.10 tedy platí:

SC_0' je kompletní, má prvomodel (zřejmě $\langle \mathbb{N}, \mathrm{S}, 0, 1\rangle$) a stejné izomorfní spektrum jako SC_0. $(*)$

2) Buď SC' rozšíření teorie SC o definice konstantních symbolů $0, 1$:

$$0 = y \leftrightarrow (\forall z)(\mathrm{S}z \neq y) \ \&\ (\forall y' \neq y)(\exists z)(\mathrm{S}z = y'), \qquad 1 = y \leftrightarrow y = \mathrm{S}0.$$

Teorie SC' je jednoduchá bezesporná extenze teorie SC_0', neboť dokazuje každý axiom teorie SC_0'. Protože je SC_0' kompletní, je SC' ekvivalentní s SC_0'. Tedy:

a) Díky 4.3.10 a $(*)$ platí
SC je kompletní, má prvomodel (zřejmě $\langle \mathbb{N}, \mathrm{S}\rangle$) a stejné izomorfní spektrum jako SC_0.

b) SC' je modelově kompletní (dle 4.3.10 5), neboť SC_0 je modelově kompletní).
SC není modelově kompletní (neboť $\langle \mathbb{N} - \{0\}, \mathrm{S}\rangle \subseteq \langle \mathbb{N}, \mathrm{S}\rangle \models \mathrm{SC}$, $\langle \mathbb{N} - \{0\}, \mathrm{S}\rangle \not\prec \langle \mathbb{N}, \mathrm{S}\rangle$).

4.4 Poznámky.

Příloha A

Vlastnosti konkrétních teorií

A.1 Teorie SC_0, SC.

Buď $\mathcal{A} = \langle A, \mathrm{S}^A, 0^A \rangle \models \mathrm{SC}_0$. SC_0-ekvivalenci $\sim_A^{\mathrm{SC}_0}$, stručněji $\sim_A$, na A definujeme takto:

$$a \sim_A b \;\Leftrightarrow\; S^n a = b \text{ nebo } S^n b = a \text{ pro nějaké } n \text{ přirozené}. \tag{A.1}$$

Pro $q \in A/{\sim_A}$ definujme:

$$\mathcal{A}_{(q)} \text{ je } \langle q, \mathrm{S}^A \restriction q, 0^A \rangle \text{ resp. } \langle q, \mathrm{S}^A \restriction q \rangle, \text{ je-li } q = [0^A]_{\sim_A} \text{ resp. jinak.}$$

TVRZENÍ A.1.1. (Izomorfizmy modelů teorie SC_0.) *Buďte* $\mathcal{A} = \langle A, \mathrm{S}^A, 0^A \rangle$, $\mathcal{B} = \langle A, \mathrm{S}^B, 0^B \rangle$ *modely teorie* SC_0.

1) *Pro* $q \in A/{\sim_A}$ *je* $\mathcal{A}_{(q)} \cong \langle \mathbb{N}, \mathrm{S}, 0 \rangle$ *resp.* $\mathcal{A}_{(q)} \cong \langle \mathbb{Z}, \mathrm{S} \rangle$, *je-li* $q = [0^A]_{\sim_A}$ *resp. jinak.*

2) a) *Nechť* H *je bijekce* $A/{\sim_A}$ *na* $B/{\sim_B}$ *taková, že* $H([0^A]_{\sim_A}) = [0^B]_{\sim_B}$ *a zobrazení* $h : A \to B$ *buď takové, že pro každé* $q \in A/{\sim_A}$ *je jeho restrikce na* q *izomorfizmus* $\mathcal{A}_{(q)}$ *a* $\mathcal{B}_{(H(q))}$. *Pak je* h *izomorfizmus* $\mathcal{A}$ *a* $\mathcal{B}$.

   b) $\mathcal{A} \cong \mathcal{B} \Leftrightarrow |A/{\sim_A}| = |B/{\sim_B}|$.

3) (Izomorfní spektrum teorie SC_0.)

   a) $\mathrm{I}(\kappa, \mathrm{SC}_0) = 1$ *pro* $\kappa > \omega$.

   b) $\mathrm{I}(\omega, \mathrm{SC}_0) = \omega$. *Podrobněji: třída modelů izomorfních se spočetným modelem* $\mathcal{A}$ *teorie* SC_0 *je jednoznačně určená číslem* $|A/{\sim_A}|$, *kterým může být libovolné* $1, 2, \ldots, \omega$, *neboť zřejmě*

$$\text{spočetnými modely } \mathrm{SC}_0 \text{ jsou až na izomorfizmus právě } \underline{\mathbb{J}}_n(0) \text{ s } n \in \mathbb{N} \text{ či } n = \omega. \tag{A.2}$$

Důkaz. 1) Příslušný izomorfizmus najdeme takto. Označme A' výběr z faktorů ekvivalence $\sim_A$ a buď $0^A \in A'$. Pro $b \in A$ buď $b' \in A'$ s $b \sim_A b'$. Pak existuje jediné n tak, že: buď $S^n b' = b$ a pak položme $e(b) = n$, nebo $S^n b = b'$ a pak položme $e(b) = -n$. Zobrazení $b \mapsto e(b)$ je izomorfizmus $\mathcal{A}_{([0^A]_{\sim_A})}$ a $\langle \mathbb{N}, \mathrm{S}, 0 \rangle$ a $\mathcal{A}_{([a]_{\sim_A})}$ a $\langle \mathbb{Z}, \mathrm{S} \rangle$, když $a \not\sim_A 0^A$.

2) a) je zřejmé z 1). b) je bezprostřední důsledek a) a 1). 3) a) je důsledkem 2) a podobně i b).

TVRZENÍ A.1.2.

1) a) *Teorie* SC_0 *je modelově kompletní.*

   b) $\langle \mathbb{N}, \mathrm{S}, 0 \rangle$ *je algebraický prvomodel* SC_0.

   Důsledek: $\langle \mathbb{N}, \mathrm{S}, 0 \rangle$ *je prvomodel* SC_0 *a* SC_0 *je kompletní.* SC_0 *je ekvivalentní* $\mathrm{Th}(\langle \mathbb{N}, \mathrm{S}, 0 \rangle)$.

2) *Teorie* SC_0 *má eliminaci kvantifikátorů.*

3) *Teorie* SC_0 *není* f-*homogenní.*

4) *Teorie* SC_0 *není ani konečně axiomatizovatelná ani otevřeně axiomatizovatelná.*

Důkaz. 1) a) (Pomocí Löwenheim-Skolemovy věty.) Buďte $\mathcal{A} \subseteq \mathcal{B}$ modely teorie SC_0; máme dokázat, že $\mathcal{A} \prec \mathcal{B}$.

Případ $|A| < |B|$. Podle Löwenheim-Skolemovy věty nahoru existuje $\mathcal{C}$ tak, že $\mathcal{A} \prec \mathcal{C}$ a $|C| = |B|$. Nechť $\sim_A$ značí SC_0-ekvivalenci na A a podobně pro B, C. Platí zřejmě následující rovnosti: $\sim_A = \sim_B \cap A^2 = \sim_C \cap A^2$. Existuje tedy bijekce H množiny $B/{\sim_B}$ na $C/{\sim_C}$ identická na $A/{\sim_A}$ (speciálně s $H([0^B]_{\sim_B}) = [0^C]_{\sim_C}$). Ta určuje izomorfizmus h struktury $\mathcal{B}$ a $\mathcal{C}$ identický na A, totiž tak, že restrikce h na $q \in B/{\sim_B}$ je izomorfizmus $\mathcal{B}_{(q)}$ a $\mathcal{C}_{(H(q))}$. Pro formuli $\varphi(\overline{x})$ a $\overline{a} \in A^{l(\overline{x})}$ máme: $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{C} \models \varphi[h\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}]$. Tudíž $\mathcal{A} \prec \mathcal{B}$.

Případ $|A| = |B|$. Podle Löwenheim-Skolemovy věty nahoru existuje $\mathcal{C}$ tak, že $\mathcal{B} \prec \mathcal{C}$ a $|C| > |B|$. Podle dokázaného máme $\mathcal{A} \prec \mathcal{C}$, $\mathcal{B} \prec \mathcal{C}$, tedy i $\mathcal{A} \prec \mathcal{B}$.

b) Pro $\mathcal{A} \models \mathrm{SC}_0$ je $\langle \mathbb{N}, \mathrm{S}, 0\rangle$ izomorfní s $\mathcal{A}_{([0^A]_{\sim_A})}$; tedy $\langle \mathbb{N}, \mathrm{S}, 0\rangle$ je algebraický prvomodel SC_0 a zbytek je důsledkem.

2) Dokážeme, že SC_0 je 1-koexistenční. Buď f neprázdné konečné parciální vnoření modelu $\mathcal{A} \models \mathrm{SC}_0$ do $\mathcal{B} \models \mathrm{SC}_0$; můžeme předpokládat, že $0^A \in \mathrm{dom}(f)$. Nechť $a_0, \ldots, a_{n-1}$ je prosté očíslování $\mathrm{dom}(f)$, $\chi(x_0, \ldots, x_{n-1}, y)$ je elementární konjunkce a $\mathcal{A} \models \chi[a_0, \ldots, a_{n-1}, a]$ s jistým $a \in A$; hledáme b tak, aby platilo $\mathcal{B} \models \chi[f(a_0), \ldots, f(a_{n-1}), b]$. Konjunkty konjunkce χ jsou bez újmy na obecnosti tvaru $\mathrm{S}^n x_i = y$ či $\mathrm{S}^n y = x_i$ a jejich negace. Uvedené rovnosti pišme zkráceně jednotně jako $\mathrm{S}^n x_i = y$ s n celým. Když $a = (S^A)^n a_i$ pro nějaké n celé, buď $b = (S^B)^n f(a_i)$; pak má jasně b požadovanou vlastnost. Jinak má b být různé od konečně prvků tvaru $(S^B)^n f(a_i)$; protože je B nekonečné, takové b existuje.

3) Zobrazení $f : \mathbb{J}_1 \to \mathbb{J}_0$ takové, že $f(\langle 0, 0\rangle) = \langle 0, 0\rangle$, je parciální vnoření $\underline{\mathbb{J}}_1(0)$ do $\underline{\mathbb{J}}_0(0)$. Nelze je bezprostředně rozšířit do $\langle 1, 0\rangle$ $(\in \mathbb{J}_1)$.

4) a) Konečná axiomatizovatelnost. Je-li SC_0 konečně axiomatizovatelná, má axiomatiku T: (Q1), (Q2), (Q7), $\{\mathrm{S}^n x \neq x;\ 0 < n < k\}$ pro jisté $k > 1$. Existuje model T, obsahující $\langle \mathbb{N}, \mathrm{S}, 0\rangle$ a část izomorfní s $\langle k, S\rangle$, kde $Sn = n + 1$ pro $n < k - 1$, $S(k-1) = 0$; to není model SC_0, neboť v něm platí $(\exists x)(\mathrm{S}^k x = x)$ – spor.

b) Otevřená axiomatizovatelnost. Pro $\mathcal{A} \models \mathrm{SC}_0$ s $|A/{\sim_A}| > 1$ buď $a \in A$ takový, že $a \not\sim_A 0^A$. Pak podstruktura $\mathcal{B} \subseteq \mathcal{A}$ s univerzem $B = 0^A/{\sim_A} \cup \{S^n a;\ n \in \mathbb{N}\}$ není model SC_0. □

Teorie SC.

Buď SC° rozšíření teorie SC o definici konstantního symbolu 0:

$$0 = y \leftrightarrow (\forall z)(\mathrm{S}z \neq y)\ \&\ (\forall y' \neq y)(\exists z)(\mathrm{S}z = y').$$

Teorie SC° je jednoduchá bezesporná extenze teorie SC_0; protože je SC_0 kompletní, je SC° s ní ekvivalentní.

TVRZENÍ A.1.3.

1) *Teorie* SC° *je ekvivalentní s* SC_0 *(a konzervativní extenze* SC *o jednu definici).*
   Důsledky:
   a) *Teorie* SC *je kompletní (protože je* SC_0 *kompletní).*
   b) *Teorie* SC *má stejné izomorfní spektrum jako* SC_0 *a* $\langle \mathbb{N}, \mathrm{S}\rangle$ *je prvomodel* SC.
   c) *Teorie* SC *není konečně axiomatizovatelná.*
2) *Teorie* SC *není modelově kompletní a tedy nemá eliminaci kvantifikátorů.*
3) *Teorie* SC *není otevřeně axiomatizovatelná.*

Důkaz. 1) je jasné.

2) Je $\mathcal{A} = \langle \mathbb{N}, \mathrm{S}\rangle \models \mathrm{SC}$ a podstruktura $\mathcal{A}\restriction(\mathbb{N} - \{0\})$ je model SC, není to však elementární podstruktura $\mathcal{A}$.

3) Je $\langle \mathbb{N}, \mathrm{S}\rangle + \langle \mathbb{Z}^+, \mathrm{S}\rangle \subseteq \langle \mathbb{N}, \mathrm{S}\rangle + \langle \mathbb{Z}, \mathrm{S}\rangle \models \mathrm{SC}$, kde $\mathbb{Z}^+ = \{a \in \mathbb{Z} :\ 0 \leq a\}$, avšak $\langle \mathbb{N}, \mathrm{S}\rangle + \langle \mathbb{Z}^+, \mathrm{S}\rangle \not\models$ SC. □

A.2 Teorie DiLO, DiLO°.

Teorie DiLO° je rozšíření DiLO o binární predikátové symboly $<_n$ s $n \in \mathbb{N}$, definované takto:

$$x <_n y \ \leftrightarrow\ x \leq y \ \&\ \text{"mezi } x \text{ a } y \text{ existuje právě } n \text{ prvků".}$$

Tedy $x <_0 y$ znamená, že „x je bezprostřední předchůdce y“. Dále značíme $\langle \mathbb{Z}, \leq \rangle^\circ$ jednoznačnou expanzi $\langle \mathbb{Z}, \leq \rangle$ do modelu DiLO°.

TVRZENÍ A.2.1. (Vlastnosti teorie DiLO a DiLO°.)

1) $\mathrm{I}(\kappa, \mathrm{DiLO}) = 2^\kappa$ *pro* κ *nekonečné.*
2) a) *Teorie* DiLO *není modelově kompletní a tedy nemá eliminaci kvantifikátorů.*

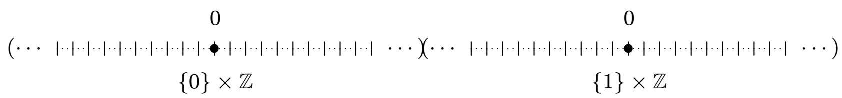
   b) DiLO *není otevřeně axiomatizovatelná.*
3) DiLO° *má eliminaci kvantifikátorů. Tedy pro* DiLO *je eliminační množina formulí*
   $$x = y, \quad x \leq y, \quad x \leq y \ \&\ x \neq y \ \&\ \text{„mezi } x \text{ a } y \text{ existuje právě } n \text{ prvků“}, n \in \mathbb{N}.$$
4) $\langle \mathbb{Z}, \leq \rangle^\circ$ *je algebraický prvomodel* DiLO°. *Tedy:*

   a) DiLO° *je kompletní a tudíž i* DiLO *je kompletní.*

   b) $\langle \mathbb{Z}, \leq \rangle^\circ$ *je prvomodel* DiLO° *a tedy* $\langle \mathbb{Z}, \leq \rangle$ *je prvomodel* DiLO.
5) DiLO° *není* f-*homogenní, neboť* $f = \{\langle \langle 0, 0 \rangle, 0 \rangle\}$ *je parciální vnoření* $\langle \mathbb{Z}, \leq \rangle^\circ + \langle \mathbb{Z}, \leq \rangle^\circ$ *do* $\langle \mathbb{Z}, < \rangle^\circ$, *které nelze bezprostředně rozšířit do* $\langle 1, 0 \rangle$.

Důkaz. 1) Pro ostré lineární uspořádání $\mathcal{A} = \langle A, <^A \rangle$ buď $\mathcal{A}(\mathbb{Z}) = \langle A \times \mathbb{Z}, <_{Le} \rangle$ lexikografické uspořádání. Je diskrétní a kardinality $\max(|A|, \omega)$. Nechť $\mathcal{B} = \langle B, <^B \rangle$ je lineární uspořádání. Pak platí $\mathcal{A}(\mathbb{Z}) \cong \mathcal{B}(\mathbb{Z}) \Rightarrow \mathcal{A} \cong \mathcal{B}$. Buď totiž h isomorfizmus $\mathcal{A}(\mathbb{Z})$ a $\mathcal{B}(\mathbb{Z})$. Definujeme-li $H : A \to B$ vztahem $H(a) = b \Leftrightarrow$ existuje $j \in \mathbb{Z}$ s $h(\langle a, 0 \rangle) = \langle b, j \rangle$, je H izomorfizmus $\mathcal{A}$ a $\mathcal{B}$. Protože na $\kappa \geq \omega$ je 2^κ neizomorfních lineárních uspořádání $\mathcal{A}$, máme 2^κ neizomorfních lineárních uspořádání $\mathcal{A}(\mathbb{Z})$ na $\kappa \times \mathbb{Z}$, tedy 2^κ neizomorfních diskrétních lineárních uspořádání, majících každé velikost univerza κ.

2) a) Buď $\underline{\mathbb{Z}}$ kanonické uspořádání celých čísel. Pak $\mathcal{A} = \underline{\mathbb{Z}} + \underline{\mathbb{Z}} \models \mathrm{DiLO}$. Buď $\mathcal{B}$ podstruktura $\mathcal{A}$ s univerzem $B = \{\langle 0, c \rangle;\, c \leq 0\} \cup \{\langle 1, c \rangle;\, c \geq 0\}$. $\mathcal{A}$, $\mathcal{B}$ jsou modely DiLO, $\mathcal{B} \subseteq \mathcal{A}$, avšak není $\mathcal{B} \prec \mathcal{A}$.



b) Podstruktura modelu otevřené teorie T je model T. Protože

$$\langle \mathbb{N}, \leq \rangle \subseteq \langle \mathbb{Z}, \leq \rangle \models \mathrm{DiLO} \text{ a } \langle \mathbb{N}, \leq \rangle \not\models \mathrm{DiLO},$$

není DiLO ekvivalentní otevřené teorii.

3) Dokážeme, že DiLO° je 1-koexistenční a tedy má eliminaci kvantifikátorů. Buďte $\mathcal{A}, \mathcal{B}$ modely DiLO° a f neprázdné konečné parciální vnoření $\mathcal{A}$ do $\mathcal{B}$. Nechť $(\exists y)\chi(x_0, \ldots, x_{n-1}, y)$ je 1-primitivní formule, kde χ je elementární konjunkce; pro $a_0, \ldots, a_{n-1}$ z $\mathrm{dom}(f)^n$ a d z A hledáme d' z B tak, aby $\mathcal{A} \models \chi[a_0, \ldots, a_{n-1}, d] \Rightarrow \mathcal{B} \models \chi[f(a_0), \ldots, f(a_{n-1}), d']$. Konjunkty formule χ jsou bez újmy na obecnosti tvaru

$$\text{i) } x_i <_k y,\ y <_k x_i,\ x_i = y, \quad \text{ii) negace formulí z i)}, \quad \text{iii) } x_i \leq y,\ y \leq x_i. \qquad (*)$$

Buďte $i_0, i_1 < n$ takové, že $a_{i_0} \leq^A d \leq^A a_{i_1}$, pokud existují, a navíc jsou nejbližší. Pak buď d' z B mezi $f(a_{i_0})$ a $f(a_{i_1})$ takové, aby platilo $\mathcal{A}^\circ \models \psi[a_{i_m}, d] \Leftrightarrow \mathcal{B}^\circ \models \psi[f(a_{i_m}), d']$ pro uvažované konjunkty ψ tvaru i), ii) z $(*)$ a $m < 2$. Platí-li $a_{i_0} <_k d$ či $d <_k a_{i_1}$ pro nějaké k či $a_{i_0} = d$ či $d = a_{i_1}$, je d' jednoznačně určeno. V opačném případě je mezi a_{i_0} a a_{i_1} nekonečně prvků a tudíž i mezi $f(a_{i_0})$ a $f(a_{i_1})$. Dále o a_{i_0}, a_{i_1}, d platí konečně konjunktů tvaru ii), které mají platit o $f(a_{i_0})$, $f(a_{i_1})$, d'. Tyto konjunkty říkají, že d' může být jakýkoli prvek mezi $f(a_{i_0})$, $f(a_{i_1})$ kromě jistých konečně mnoha prvků; takové d' ovšem existuje. Stejně postupujeme i v případě, že a_{i_0} či a_{i_1} neexistuje.

4) Jasně lze $\langle \mathbb{Z}, \leq \rangle^\circ$ vnořit do každého modelu teorie DiLO$^\circ$.

a) DiLO$^\circ$ je kompletní, neboť má eliminaci kvantifikátorů a algebraický prvomodel. Protože DiLO$^\circ$ je konzervativní extenze DiLO, je i DiLO kompletní.

b) Jasně je $\langle \mathbb{Z}, \leq \rangle$ algebraický prvomodel DiLO. Je-li teorie modelově kompletní, je její algebraický prvomodel jejím prvomodelem; odtud plyne zbytek tvrzení.

5) je jasné. □

A.3 Teorie DeLO.

TVRZENÍ A.3.1. (Vlastnosti teorie DeLO.)

1) $\mathrm{I}(\kappa, \mathrm{DeLO}) = 1$ *resp.* 2^κ *pro* $\kappa = \omega$ *resp.* κ *nespočetné. Speciálně je* DeLO *kompletní.*

2) DeLO *je* f-*homogenní, má tedy eliminaci kvantifikátorů a je modelově kompletní.*

3) $\langle \mathbb{Q}, \leq \rangle$ *je prvomodel teorie* DeLO.

4) *Teorie* DeLO *není otevřeně axiomatizovatelná.*

Důkaz. 1) Snadno se sestrojí rekurzí izomorfizmus dvou spočetných modelů teorie DeLO; DeLO je tedy ω-kategorická o odtud plyne kompletnost. Tvrzení pro κ nespočetné dává tvrzení 1.3.1 o neizomorfních lineárních uspořádáních.

2) Každé neprázdné konečné parciální vnoření mezi modely DeLO lze jasně bezprostředně prodloužit, DeLO je tedy koexistenční a tedy má eliminaci kvantifikátorů.

3) Je-li $\mathcal{A} \models \mathrm{DeLO}$, jasně lze $\langle \mathbb{Q}, \leq \rangle$ vnořit do $\mathcal{A}$ na nějaký podmodel $\mathcal{A}'$. Díky modelové kompletnosti je $\mathcal{A}' \prec \mathcal{A}$.

4) Podstruktura modelu otevřené teorie T je model T. Podstruktura $\langle \mathbb{N}, \leq \rangle$ modelu $\langle \mathbb{Q}, \leq \rangle$ teorie DeLO není model DeLO; tedy DeLO není ekvivalentní otevřené teorii. □

A.4 Aritmetiky.

Jazyk aritmetiky je $\langle \mathrm{S}, +, \cdot, 0, \leq \rangle$, $\mathcal{N} = \langle \mathbb{N}, \mathrm{S}, +, \cdot, 0, \leq \rangle$ je jeho model, zvaný standardní model aritmetiky. $\langle \mathrm{S}, +, 0 \rangle$ je jazyk (aditivní) Presburgerovy aritmetiky Pr, $\langle \mathbb{N}, \mathrm{S}, +, 0 \rangle$ je její standardní model. Pro $n \in \mathbb{N}$ je $\underline{n}$ term $\mathrm{S} \cdots \mathrm{S}0$, S aplikováno n-krát, nazývající se (n-tý) numerál; $\underline{0}$ je 0. nx značí term $x + \cdots + x$, + aplikováno n-krát.

Presburgerova aritmetika.

Pro $m, n \in \mathbb{N}$ platí:

$$\begin{array}{llll} \text{a)} & \mathrm{Pr} \vdash \underline{m} = 0 \;\Leftrightarrow\; m = 0 & \text{b)} & \mathrm{Pr} \vdash \underline{m} = \underline{n} \;\Leftrightarrow\; m = n \\ \text{c)} & \mathrm{Pr} \vdash \mathrm{S}\underline{m} = \underline{\mathrm{S}m} & \text{d)} & \mathrm{Pr} \vdash \underline{m} + \underline{n} = \underline{m+n} \end{array} \tag{A.3}$$

Přitom k důkazu stačí jen axiomy (Q1) – (Q4); není třeba indukce. Položka a) plyne pomocí (Q1), b) pomocí a) a (Q2), c) z definice numerálu, d) indukcí dle n pomocí c) , (Q3) a (Q4).

TVRZENÍ A.4.1. (Elementární dokazatelné formule v Pr.) *V Presburgerově aritmetice* Pr, *dokonce s použitím jen schematu indukce pro otevřené formule, je dokazatelné:*

1) a) $\mathrm{S}x + y = \mathrm{S}(x + y)$ b) $0 + x = x + 0$

2) a) $x + y = y + x$ b) $(x + y) + z = x + (y + z)$ c) $x + z = y + z \to x = y$.

Důkaz. 1) a) Indukcí podle y. $\mathrm{S}x + 0 = \mathrm{S}x = \mathrm{S}(x + 0)$ dle (Q3). Indukční krok: máme

$$\mathrm{S}x + \mathrm{S}y = \mathrm{S}(\mathrm{S}x + y) = \mathrm{SS}(x + y) = \mathrm{S}(x + Sy).$$

1. rovnost plyne z (Q4), 2. je indukční předpoklad, 3. dle (Q4).

b) Indukcí dle x. $0 + 0 = 0 + 0$. Indukční krok: máme

$$0 + \mathrm{S}x = \mathrm{S}(0 + x) = \mathrm{S}(x + 0) = \mathrm{S}x = \mathrm{S}x + 0.$$

1. rovnost plyne z (Q4), 2. dle indukčního předpokladu, 3. dle (Q3), 4. dle (Q3).

2) a) Předpokládáme 1). Dále indukcí dle x. $0+y=y+0$ platí díky 1). Indukční krok: $\mathrm{S}x+y=\mathrm{S}(x+y)=\mathrm{S}(y+x)=y+\mathrm{S}x$; 1. rovnost plyne z 1), 2. je indukční předpoklad, 3. plyne z (Q4).

b) Předpokládáme 1). Dále indukcí dle x. Pro $x=0$ to platí: $(0+y)+z=y+z=0+(y+z)$ užitím 1) a užitím (Q3). Indukční krok: $(\mathrm{S}x+y)+z=\mathrm{S}(x+y)+z=\mathrm{S}((x+y)+z)=\mathrm{S}(x+(y+z))=\mathrm{S}x+(y+z)$. 1. a 2. rovnost plyne z 1) a), 3. z indukčního předpokladu.

c) Snadno indukcí dle z užitím (Q3) pro $z=0$ a (Q4), (Q2) v indukčním kroku. □

Buď Pr° extenze Pr o definice

$$x<y\leftrightarrow(\exists z\neq 0)(x+z=y),\qquad P_n(x)\leftrightarrow(\exists y)(ny=x)\ (\text{„}n \text{ dělí } x\text{“})\text{ pro }1<n\in\mathbb{N}.\tag{A.4}$$

Pro $\mathcal{A}\models\mathrm{Pr}$ buď $\mathcal{A}^\circ$ jednoznačná expanze struktury $\mathcal{A}$, která je modelem Pr°. V Pr° je dokazatelné:

1) $<$ je ostré lineární diskrétní uspořádání s nejmenším prvkem 0 a bez největšího, $\mathrm{S}x$ je následník x v $<$ a dále je $<$ izotonní vůči $\mathrm{S},+$.

2) $\bigvee_{i<n}P_n(x+\underline{i})$ pro $1<n\in\mathbb{N}$. ($\mathbb{N}$-divizibilita).

Snadno se zjistí, že platí:

$$\text{Pro modely }\mathcal{A}\subseteq\mathcal{B}\text{ teorie Pr je }\mathcal{A}^\circ\subseteq\mathcal{B}^\circ.\tag{A.5}$$

VĚTA A.4.2. (Některé charakteristiky teorie Pr.)

1) a) *Teorie* Pr° *má eliminaci kvantifkátorů a je tedy modelově kompletní.*
   b) $\langle\mathbb{N},\mathrm{S},+,0\rangle^\circ$ *je algebraický prvomodel* Pr° *a tedy prvomodel a* Pr° *je kompletní.*

2) Pr *je kompletní, ekvivalentní s* $\mathrm{Th}(\langle\mathbb{N},\mathrm{S},+,0\rangle)$ *a* $\langle\mathbb{N},\mathrm{S},+,0\rangle$ *je její prvomodel.*

3) Pr *je modelově kompletní a nemá eliminaci kvantifikátorů.*

Důkaz. 1) a) Důkaz neuvádíme. b) Díky (A.3) zřejmě existuje vnoření $\langle\mathbb{N},\mathrm{S},+,0\rangle$ do modelu $\mathcal{A}$ teorie Q; z (A.5) je patrné, že to je vnoření i $\langle\mathbb{N},\mathrm{S},+,0\rangle^\circ$ do $\mathcal{A}^\circ$.

2) Protože konzervativní rozšíření Pr° teorie Pr je kompletní, je Pr kompletní. Teorie Pr má model $\langle\mathbb{N},\mathrm{S},+,0\rangle$, tedy je ekvivalentní s teorií tohoto modelu. Protože $\langle\mathbb{N},\mathrm{S},+,0\rangle^\circ$ je prvomodel Pr°, lze jej elementárně vnořit do $\mathcal{A}^\circ$ jakmile $\mathcal{A}\models\mathrm{Pr}$, tudíž je tím spíše $\langle\mathbb{N},\mathrm{S},+,0\rangle$ elementárně vnořen do $\mathcal{A}$.

3) Dokážeme, že Pr je modelově kompletní. Buďte $\mathcal{A}\subseteq\mathcal{B}$ modely Pr. Pak platí $\mathcal{A}^\circ\subseteq\mathcal{B}^\circ$ dle (A.5). Tudíž $\mathcal{A}^\circ\prec\mathcal{B}^\circ$ díky modelové kompletnosti Pr° a tedy i $\mathcal{A}\prec\mathcal{B}$.

Dokážeme, že Pr nemá eliminaci kvantifikátorů. Buď $\mathcal{A}$ nestandardní model Pr, $a\in A$ nestandardní prvek $\mathcal{A}$. Pak $f=\{\langle a+a,a+a+\underline{1}\rangle\}$ je parciální vnoření $\mathcal{A}$ do sebe. Atomická formule $\psi(x)$ teorie Pr je totiž ekvivalentní v Pr formuli tvaru $mx=\underline{n}$ s m,n přirozenými. Odtud je jasné, že $\mathcal{A}\models\psi[a+a]\Leftrightarrow\mathcal{A}\models\psi[a+a+1]$. Dále $\mathcal{A}\models(\exists y)(y+y=x)[a+a]$. Avšak $\mathcal{A}\not\models(\exists y)(y+y=x)[f(a+a)]$; Pr tedy není koexistenční a tedy nemá eliminaci kvantifikátorů. □

Hierarchie aritmetických formulí a množin.

A.4.3. Σ_n-, Π_n- a Δ_n-formule a množiny. Aritmetické množiny.

1. *Omezená formule* jazyka aritmetiky je formule jazyka aritmetiky, ve které je každá kvantifikace *omezená*, tj. tvaru $(Qx\le y)$, kde Q je kvantifikátor a x,y jsou různé. Taková formule je ekvivalentní formuli tvaru $(Q_1x_1\le y_1)\cdots(Q_nx_n\le y_n)\varphi$, kde Q_i jsou kvantifikátory a φ je otevřená formule.

2. Hierarchii Σ_n*-formulí* a Π_n*-formulí* jazyka aritmetiky definujeme indukcí:

• Σ_0-formule a Π_0-formule jsou právě omezené formule.

• Σ_n*-formule* resp. Π_n*-formule* jsou formule právě tvaru $(\exists\overline{x})\varphi$ resp. $(\forall\overline{x})\varphi$, kde φ je Π_{n-1}-formule resp. Σ_{n-1}-formule.

• Formule jazyka aritmetiky je Δ_n (*-formule*), je-li logicky ekvivalentní jak nějaké Σ_n-formuli tak nějaké Π_n-formuli.

Zcela stejně definujeme $\Sigma_{n,L}$-, $\Pi_{n,L}$- a $\Delta_{n,L}$*-formule* jazyka L obsahujícího $\le$.

3. Množina je Σ_n resp. Π_n resp. Δ_n (*-množina*), je-li to množina definovaná (s parametry či bez parametrů) nějakou Σ_n- resp. Π_n- resp. Δ_n-formulí ve standardním modelu $\mathbf{N}$. Obory

takových podmnožin $\mathbb{N}^k$ jsou uzavřeny na sjednocení a průnik. Komplement Σ_n- resp. Π_n-množiny je Π_n- resp. Σ_n-množina, komplement Δ_n-množiny je Δ_n-množina. Je-li $A \subseteq \mathbb{N}^k$ i její komplement Σ_n-množina, je to Δ_n-množina. Složení totálních funkcí, které jsou Δ_n, je Δ_n. Každá množina definovatelná v $\mathbf{N}$ je Σ_n a také Π_n pro nějaké n (díky tomu, že definující formuli můžeme vzít v prenexním tvaru); množiny definovatelné v $\mathbf{N}$ se nazývají *aritmetické*.

Robinsonova aritmetika.

TVRZENÍ A.4.4.

1) *Pro* $m, n \in \mathbb{N}$ *platí:*

   a) $\mathrm{Q} \vdash \underline{m} = 0 \quad \Leftrightarrow \quad m = 0$ b) $\mathrm{Q} \vdash \underline{m} = \underline{n} \quad \Leftrightarrow \quad m = n$
   c) $\mathrm{Q} \vdash \mathrm{S}\underline{m} = \underline{\mathrm{S}m}$ d) $\mathrm{Q} \vdash \underline{m} + \underline{n} = \underline{m+n}$ e) $\mathrm{Q} \vdash \underline{m} \cdot \underline{n} = \underline{m \cdot n}$

2) *V* Q *je dokazatelné pro* $m, n \in \mathbb{N}$.

   (q1) $x \leq \underline{m} \leftrightarrow x = \underline{0} \vee \cdots \vee x = \underline{m}$ (q2) $x \leq \underline{m} \vee \underline{m} \leq x$
   $x \leq y \leq \underline{m} \rightarrow x \leq \underline{m}$ $x \leq \underline{m} \leq y \rightarrow x \leq y$

   Speciálně: $\mathrm{Q} \vdash \underline{m} \leq \underline{n} \quad \Leftrightarrow \quad m \leq n.$

3) (O Σ_1-kompletnosti Robinsonovy aritmetiky.) *Pro* Σ_1*-formuli* $\varphi(x_1, \ldots, x_k)$ *a* $m_1, \ldots, m_k$ *z* $\mathbb{N}$ *je*
$$\mathrm{Q} \vdash \varphi(\underline{m_1}, \ldots, \underline{m_k}) \;\Leftrightarrow\; \mathbf{N} \models \varphi[m_1, \ldots, m_k]. \tag{A.6}$$

Důkaz. 1) a) plyne pomocí (Q1), b) pomocí a) a (Q2), c) z definice numerálu, d) indukcí dle n pomocí c) , (Q3) a (Q4), e) obdobně navíc pomocí (Q5) a (Q6).

2) (q1) Indukcí podle m. Pro $m = 0$ to platí, neboť zřejmě $\mathrm{Q} \vdash x \leq 0 \leftrightarrow x = 0$. Nechť to platí pro m. Pak v Q máme: $x \leq \underline{m+1}$ právě když $z + x = \mathrm{S}\underline{m}$ pro nějaké z. Pokud $x \neq 0$, máme $x = \mathrm{S}x'$ pro nějaké x' a díky (Q4), (Q2) tedy $z + x' = \underline{m}$, tj. $x' \leq \underline{m}$ a dle indukčního předpokladu je $x' = \underline{p}$ pro nějaké $p \leq m$. Tedy $x = \mathrm{S}\underline{p}$ a máme $x = \underline{q}$ pro nějaké $q \leq m + 1$. (q2) plyne snadno indukcí dle m, užijeme-li (q1). Zbývající dvě implikace plynou snadno užitím (q1), (q2).

3) Indukcí podle složitosti termu t se dokáže $\mathrm{Q} \vdash t(\underline{n_1}, \ldots, \underline{n_k}) = \underline{t^{\mathbb{N}}[n_1, \ldots, n_k]}$ užitím 1). Indukcí podle složitosti a užitím 1) a speciálního tvrzení z 2) dále dokážeme (A.6) pro φ omezenou; v případě omezené kvantifikace užijeme $(q1)$ z 2). Snadno se provede krok pro $\exists$. $\square$

TVRZENÍ A.4.5. (Některé charakteristiky Robinsonovy aritmetiky Q.)

1) *Teorie* Q *není kompletní.*

2) Q *není otevřeně axiomatizovatelná.*

3) *Jednoduchá bezesporná extenze* T *teorie* Q *taková, že* $\mathbf{N} \models T$*, má algebraický prvomodel* $\mathbf{N}$.

4) *Buď* T *jednoduchá bezesporná extenze teorie* Q *taková, že* $\mathbf{N} \models T$ *a* T *není ekvivalentní s* $\mathrm{Th}(\mathbf{N})$. *Pak* T *není modelově kompletní a tedy nemá eliminaci kvantifikátorů.*

Důkaz. 1) V Q není např. dokazatelné $(\forall x, y)(x \leq y \vee y \leq x)$, platí to však v $\mathbf{N}$. Buď totiž $A = \mathbb{N} \cup \mathbb{Z}\{x, y\}$, kde $\mathbb{Z}\{x, y\}$ jsou nenulové polynomy v proměnných x, y nad $\mathbb{Z}$ s kladnými koeficienty u mocnin s největší sumou exponentů.

Zřejmě je A uzavřeno na sčítání $+$ a násobení $\cdot$ polynomů. Definujme $S : A \to A$ tak, že $S(a) = a+1$ a relaci $\preceq \subseteq A^2$ tak, že $a \preceq b \Leftrightarrow c+a = b$ pro nějaké $c \in A$. Pak $\langle A, S, +, \cdot, 0, \preceq \rangle \models \mathrm{Q}$ a prvky x, y jsou $\preceq$-nesrovnatelné, neboť $c+x = y \Leftrightarrow c = y-x$ a $y-x \notin A$. Tedy $\mathrm{Q} \not\models x \leq y \vee y \leq x$.

2) Buď $\mathcal{A}$ vlastní elementární extenze $\mathbf{N}$; je $\mathbf{N} \models \mathrm{Q}$. Buď $a \in A - \mathbb{N}$. Pak podstruktura $\mathcal{B} = \mathcal{A}\langle a \rangle \subseteq \mathcal{A}$ není model Q. Každý prvek z B je totiž tvaru $t[a]$ pro nějaký term t. Snadno se dokáže indukcí dle složitosti t: $t[a] \in \mathbb{N}$ nebo $a \leq^A t[a]$. Tudíž neexistuje $b \in B$ s $S^A(b) = a$. (Pokud $S^A(b) = a$, tak $b <^A a$, $b \notin \mathbb{N}$.) Avšak $\mathrm{Q} \vdash x \neq 0 \rightarrow (\exists y)(\mathrm{S}y = x)$.

3) Buď $\mathcal{A} \models T$. Definujme $h : \mathbb{N} \to A$ takto: $h(n) = (\underline{n})^A$ $(= S^A \cdots S^A(0^A)$, S^A aplikováno n-krát). Pak je to hledané vnoření, neboť $\mathrm{Q} \vdash \mathrm{S}(\underline{n}) = \underline{\mathrm{S}n}$, $\mathrm{Q} \vdash \underline{m} \diamond \underline{n} = \underline{m \diamond n}$, kde $\diamond$ je $+$ nebo $\cdot$ a $\mathrm{Q} \vdash \underline{m} \leq \underline{n} \Leftrightarrow m \leq n$.

4) Protože T má algebraický prvomodel $\mathbf{N}$, má předpoklad modelové kompletnosti T za následek, že standardní model aritmetiky $\mathbf{N}$ je prvomodel T a tedy T je kompletní a ekvivalentní s $\mathrm{Th}(\mathbf{N})$. □

POZNÁMKA A.4.6. Následující extenze Q jsou bezesporné (tj. mají model):

$$\mathrm{Q} \cup \{\leq \text{ je tranzitivní, není reflexivní}\},$$
$$\mathrm{Q} \cup \{+ \text{ je komutativní, } \cdot \text{ není komutativní}\},\ \mathrm{Q} \cup \{+ \text{ není komutativní}\}.$$

VĚTA A.4.7. (O nerozhodnutelnosti a nekompletnosti.) *Bezesporná teorie rozšiřující Robinsonovu aritmetiku* Q *je nerozhodnutelná a je-li navíc rekurzivně axiomatizovaná, není kompletní.*

Důsledky:

Nechť $\mathrm{Sent}_{L(\mathrm{Q})}$ *resp.* Th_Q *resp.* nTh_Q *značí množinu sentencí resp. dokazatelných sentencí resp. negací dokazatelných sentencí teorie* Q. *Pak*

a) Th_Q *je* Σ_1 *a není* Δ_1, b) $\mathrm{Sent}_{L(\mathrm{Q})} - (\mathrm{Th}_\mathrm{Q} \cup \mathrm{nTh}_\mathrm{Q})$ *je* Π_1 *a není* Δ_1.

Peanova aritmetika.

TVRZENÍ A.4.8. (Elementární teorémy P.) *V Peanově aritmetice* P, *dokonce v jednoduché extenzi* Q *o schema indukce pro otevřené formule, je dokazatelné:*

1) a) $\mathrm{S}x + y = \mathrm{S}(x+y)$ b) $0 + x = x + 0$
2) a) $x + y = y + x$ b) $(x+y)+z = x+(y+z)$
3) a) $0 \cdot x = 0$ b) $\mathrm{S}x \cdot y = xy + y$ c) $xy = yx$
4) a) $(x \neq 0 \vee y \neq 0) \to x + y \neq 0$ b) $x \neq 0 \to y \neq x + y$
5) a) $x \leq x$ & $(x \leq y \,\&\, y \leq x \to x = y)$ & $(x \leq y \,\&\, y \leq z \to x \leq z)$ b) $x \leq y \vee y \leq x$
(Tj. $\leq$ je lineární uspořádání.)

Důkaz. Formule z 1) a 2) jsou dokazatelné i v Presburgerově aritmetice; viz A.4.1.

3) a) Indukcí dle x. Platí $0 \cdot 0 = 0$ dle (Q5). Indukční krok: $0 \cdot \mathrm{S}x = 0 \cdot x + 0 = 0$ užitím (Q6) a (Q5).

b) Předpokládáme 1) a), 2). Indukcí dle y. Je $\mathrm{S}x \cdot 0 = 0 = x \cdot 0 + 0$ užitím (Q5), (Q6). Indukční krok: $\mathrm{S}x \cdot \mathrm{S}y = \mathrm{S}(\mathrm{S}x \cdot y + x) = \mathrm{S}((xy + y) + x) = \mathrm{S}((xy + x) + y) = \mathrm{S}(x \cdot \mathrm{S}y + y) = x \cdot \mathrm{S}y + \mathrm{S}y$. 1. rovnost dává (Q6), (Q4), 2. plyne z indukčního předpokladu, 3. plyne užitím 1) a), 2), 4. pomocí (Q6) a 5. pomocí (Q4).

c) Předpokládáme, že již máme dokázané 3) a), 3) b), 1) a). Indukcí dle x. Je $0 \cdot y = 0 = y \cdot 0$ užitím 3) a) a (Q5). Indukční krok: $\mathrm{S}x \cdot y = xy + y = yx + y = y \cdot \mathrm{S}x$. 1. rovnost platí dle 3) b), 2. plyne z indukčního předpokladu, 3. z (Q6). 4), 5) již nedokazujeme. □

TVRZENÍ A.4.9. (Některé charakteristiky Peanovy aritmetiky P.)

1) $\mathbf{N}$ *je algebraický prvomodel* P.
2) *Buď* $\mathcal{A} \models \mathrm{P}$, $X \subseteq A$. *Pak* $\mathcal{A}_{(X)} \prec \mathcal{A}$, *kde univerzum* $\mathcal{A}_{(X)}$ *je množina definovatelných prvků v* $\mathcal{A}$ *nad* X, *tj.* $A_{(X)} = \{a \in A;\ \{a\} \in \mathrm{Df}^1(X, \mathcal{A})\}$.

   Důsledek: Pro $\mathcal{A} \models \mathrm{P}$ *je* $\mathcal{A}_{(\emptyset)}$ *prvomodel teorie* $\mathrm{Th}(\mathcal{A})$.
3) P *není modelově kompletní a tedy nemá eliminaci kvantifikátorů.*
4) P *má kontinuum neekvivalentních jednoduchých kompletních extenzí.*
5) P *není otevřeně axiomatizovatelná.*

Důkaz. 1) Buď $\mathcal{A} \models \mathrm{P}$. Definujme $h : \mathbb{N} \to A$ takto: $h(n) = (\underline{n})^A$ $(= S^A \cdots S^A(0^A)$, S^A aplikováno n-krát). Pak to je vnoření $\mathbf{N}$ do $\mathcal{A}$.

2) $A_{(X)}$ je jasně uzavřeno na funkce struktury $\mathcal{A}$; tedy $\mathcal{A}_{(X)} \subseteq \mathcal{A}$. Snadno se dokáže platnost předpokladů Tarski-Vaughtova testu pro $\mathcal{A}_{(X)}$ a $\mathcal{A}$: pro neprázdnou množinu D z $\mathrm{Df}^1(A_{(X)}, \mathcal{A})$ je definován její nejmenší prvek nad X v $\mathcal{A}$, což je prvek z podstruktury $\mathcal{A}_{(X)}$, který test požaduje.

Důsledek. Buď $\mathcal{A}' \models \mathrm{Th}(\mathcal{A})$, tj. $\mathcal{A}' \equiv \mathcal{A}$. Pro $a \in A_{(\emptyset)}$ buď $\varphi(x)$ formule jazyka Peanovy aritmetiky definující $\{a\}$ v $\mathcal{A}$; pak definuje jisté $\{a'\}$ v $\mathcal{A}'$; položme $h(a) = a'$. Toto h je korektně definované a je to prosté zobrazení $A_{(\emptyset)}$ na $A'_{(\emptyset)}$. Stačí dokázat, že to je vnoření $\mathcal{A}_{(\emptyset)}$ do $\mathcal{A}'_{(\emptyset)}$. Pro n-ární funkční symbol F jazyka aritmetiky a $\langle a_0, \dots, a_n\rangle$ z A^{n+1} buď $F^A(a_0, \dots, a_{n-1}) = a_n$; máme dokázat, že $F^{A'}(a'_0, \dots, a'_{n-1}) = a'_n$. Nechť $\varphi_i(x_i)$ definuje $\{a_i\}$ v $\mathcal{A}$. Pak v $\mathcal{A}$ platí $\bigwedge_{i\le n}\varphi_i(x_i) \to F(x_0, \dots, x_{n-1}) = x_n$; poslední formule platí i v $\mathcal{A}'$ a tedy $F^{A'}(a'_0, \dots, a'_{n-1}) = a'_n$. Podobně, je-li R relační n-ární symbol, tak analogicky dostaneme $R^A(a_0, \dots, a_{n-1}) \Leftrightarrow R^{A'}(a'_0, \dots, a'_{n-1})$.

3) a) Kdyby P byla modelově kompletní, díky existenci algebraického prvomodelu $\mathbf{N}$ by byla kompletní – spor s A.4.7.

4) Užijeme tvrzení: Každá bezesporná extenze aritmetiky P o konečně axiomů je nerozhodnutelná a tedy nekompletní. (Je to důsledek věty o nerozhodnutelnosti a nekompletnosti.) Pro každý vrchol σ stromu $\langle\bigcup_{n\in\mathbb{N}} {}^n2, \subseteq\rangle$ sestrojíme bezespornou jednoduchou extenzi T_σ teorie P o konečně axiomů takto: Buď $T_\emptyset$ teorie P. Máme-li T_σ, buď φ_σ nezávislá sentence teorie T_σ. Buď $\varphi_{\sigma\text{-}0}$ formule $\neg\varphi_\sigma$ a $\varphi_{\sigma\text{-}1}$ formule φ_σ; buď $T_{\sigma\text{-}i} = T_\sigma \cup \{\varphi_{\sigma\text{-}i}\}$. ($\sigma\text{-}i$ značí $\sigma \cup \{\langle n, i\rangle\}$, kde $n = \mathrm{dom}(\sigma)$.) Pro $f \in {}^{\mathbb{N}}2$ buď T_f extenze P právě o axiomy $\varphi_{f\restriction n}$ s $n \in \mathbb{N}$ (tj. $T_f = \bigcup_{n\in\mathbb{N}} T_{f\restriction n}$). Pro $f \neq g \in {}^{\mathbb{N}}2$ a nejmenší n s $f(n) \neq g(n)$ je v jedné z teorií T_f, T_g formule $\varphi_{f\restriction n+1}$, právě když je v druhé její negace.

5) Buď $\mathcal{A}$ model P, který je vlastní extenzí $\mathbf{N}$. Buď $a \in A - \mathbb{N}$. Pak podstruktura $\mathcal{B} = \mathcal{A}\langle a\rangle \subseteq \mathcal{A}$ není model P. Každý prvek z B je totiž tvaru $t[a]$ pro nějaký term t. Snadno se dokáže indukcí dle složitosti t: $t[a] \in \mathbb{N}$ nebo $a \le^A t[a]$. Tudíž neexistuje $b \in B$ s $S^A(b) = a$. (Pokud $S^A(b) = a$, tak $b <^A a$, $b \notin \mathbb{N}$.) Avšak $\mathrm{P} \vdash x \neq 0 \to (\exists y)(\mathrm{S}y = x)$. □

A.5 Teorie vektorových prostorů.

TVRZENÍ A.5.1. (Izomorfní spektrum vektorových prostorů.) *Buď F těleso, $\mathcal{A}$ vektorový prostor nad F a T teorie vektorových prostorů nad F. ($\lambda(\le)$ je počet velikostí nejvýše rovných λ.)*

1) *Buď $|F| < \omega$. Je-li* $\dim(\mathcal{A}) = n$, *je* $|A| = |F|^n$. *Je-li* $\dim(\mathcal{A}) \ge \omega$, *je* $|A| = \dim(\mathcal{A})$.

$$\textit{Důsledek: } \mathrm{I}(\lambda, T) = \begin{cases} 0 & \textit{když } |F|^n \neq \lambda < \omega \textit{ pro každé } n < \omega \\ 1 & \textit{když } |F|^n = \lambda \textit{ pro nějaké } n < \omega \\ 1 & \textit{když } \lambda \ge \omega. \end{cases}$$

2) *Buď $|F| \ge \omega$. Je-li* $0 < \dim(\mathcal{A}) \le |F|$, *je* $|A| = |F|$. *Je-li* $\dim(\mathcal{A}) > |F|$, *je* $|A| = \dim(\mathcal{A})$.

$$\textit{Důsledek: } \mathrm{I}(\lambda, T) = \begin{cases} 0 & \textit{když } 1 < \lambda < |F| \\ \lambda(\le) & \textit{když } \lambda = |F| \\ 1 & \textit{když } \lambda > |F|. \end{cases}$$

Důkaz. Tvrzení o $\mathcal{A}$ plynou z elementárních vlastností vektorových prostorů. Zbývá objasnit pro $|F| \ge \omega$ důsledek $\mathrm{I}(\lambda, T) = \lambda(\le)$, když $\lambda = |F|$. V tomto případě je počet dimenzí uvažovaných modelů, z nichž každá určuje jeden izomorfní typ, roven počtu nenulových kardinálních čísel nejvýše rovných λ; těch je právě $\lambda(\le)$. □

TVRZENÍ A.5.2. (Vlastnosti teorie nekonečných vektorových prostorů.) *Buď T teorie nekonečných vektorových prostorů nad tělesem F. Pak:*

1) *T je λ-kategorická pro každý nekonečný kardinál $\lambda > |F|$ a tedy i kompletní.*

2) *T má eliminaci kvantifikátorů a je tedy i modelově kompletní.*

3) *T je* f*-homogenní, právě když je F konečné.*

Důkaz. 1) Plyne z A.5.1.

2) Dokážeme, že T je 1-koexistenční. Buďte $\mathcal{A}$, $\mathcal{B}$ modely T a f neprázdné konečné parciální vnoření $\mathcal{A}$ do $\mathcal{B}$. Nechť $(\exists y)\chi(x_0, \dots, x_{n-1}, y)$ je 1-primitivní formule, kde χ je elementární konjunkce bez újmy na obecnosti tvaru

$$\bigwedge_{j<m} \sum_{i<n} r_{j,i} x_i + r_j y \diamond_j 0$$

s $r_{j,i}, r_j$ z F, $r_j \neq 0$ a $\diamond_j$ buď $=$ nebo $\neq$. Nechť $\mathcal{A} \models \chi[a_0, \dots, a_{n-1}, d]$ pro nějaké $a_0, \dots, a_{n-1}$ z $\mathrm{dom}(f)$ a $d \in A$; hledáme $d' \in B$ s $\mathcal{B} \models \chi[f(a_0), \dots, f(a_{n-1}), d']$. Je-li $d = -\frac{1}{r_j} \sum_{i<n} r_{j,i} a_i$ pro nějaké $j < m$, buď $d' = -\frac{1}{r_j} \sum_{i<n} r_{j,i} f(a_i)$. Jinak za d' vyberme nějaký prvek z nekonečné množiny $A' \subseteq B$ prvků různý od všech prvků tvaru $-\frac{1}{r_j} \sum_{i<n} r_{j,i} f(a_i)$ s $j < m$. Pak má d' požadované vlastnosti.

3) Buďte $\mathcal{A}$, $\mathcal{B}$ modely T. Je-li F konečné, mají $\mathcal{A}$, $\mathcal{B}$ nekonečnou dimenzi a tedy lze každé neprázdné konečné parciální vnoření $\mathcal{A}$ do $\mathcal{B}$ bezprostředně prodloužit. Je-li F nekonečné, nechť $\mathcal{A}$ má dva generátory a_0, a_1 a $\mathcal{B}$ jen jeden b_0. Zobrazení $f = \{\langle a_0, b_0 \rangle\}$ nelze prodloužit do a_1. □

A.6 Teorie $\mathrm{CE_k}(\infty)$, $\mathrm{C'E}_\omega$.

TVRZENÍ A.6.1. (Vlastnosti teorie $\mathrm{CE_k}(\infty)$.)
Buď $1 \leq k \in \mathbb{N}$ a označme teorii $\mathrm{CE_k}(\infty)$ jako T.

1) *Pro ekvivalenci E na k nechť T_E je $\langle c_i \rangle_{i \in k}$-teorie s axiomy*
$$T \cup \{c_i = c_j;\ \langle i,j \rangle \in E\} \cup \{c_i \neq c_j;\ \langle i,j \rangle \notin E\}.$$
Ekvivalencí na k existuje právě $B(k)$, kde $B(k)$ je k-té Bellovo číslo.
   a) *Pro $\mathcal{A}, \mathcal{B} \models T_E$ téže kardinality je $\mathcal{A} \cong \mathcal{B}$; speciálně je T_E kompletní.*
   b) *Jednoduchá kompletní extenze teorie T je až na ekvivalenci teorií právě některé T_E.*
   c) $\mathrm{I}(\kappa, T) = B(k)$ *pro každou nekonečnou kardinalitu κ.*
2) a) *T je* f*-homogenní a má tedy eliminaci kvantifikátorů a je modelově kompletní.*
   b) *Pro $k = 1$ je T kompletní a má prvomodel.*
   c) *Pro $k \geq 2$ není T kompletní a tedy nemá algebraický prvomodel.*

Důkaz. 1) a) platí evidentně. b) Buď T' nějaká kompletní jednoduchá extenze T. Buď E taková ekvivalence na k, že $\langle i,j \rangle \in E \Leftrightarrow T' \vdash c_i = c_j$. Díky kompletnosti T' máme $\langle i,j \rangle \notin E \Leftrightarrow T' \vdash c_i \neq c_j$, tedy $T_E \subseteq \mathrm{Th}(T')$, tedy i $\mathrm{Th}(T_E) \subseteq \mathrm{Th}(T')$. Platí i opačná inkluze, neboť pro sentenci φ s $T' \vdash \varphi$ nutně $T_E \vdash \varphi$, protože jinak $T' \vdash \varphi, \neg\varphi$. c) plyne ihned z a) a b).

2) a) Jasně lze neprázdné konečné parciální vnoření mezi modely T bezprostředně prodloužit a tedy a) platí.

b) Pro $k = 1$ je $B(k) = 1$ a T je tedy kompletní. Model $\langle \mathbb{N}, 0 \rangle$ je zřejmě algebraický prvomodel a v důsledku eliminace kvantifikátorů to je prvomodel.

c) Pro $k \geq 2$ je $B(k) \geq 2$ a T tedy není kompletní. Kdyby měla T algebraický prvomodel, byl by to prvomodel a T by byla kompletní. □

TVRZENÍ A.6.2. (Vlastnosti teorie $\mathrm{C'E}_\omega$ spočetně různých konstant.) *Označme T teorii $\mathrm{C'E}_\omega$.*

1) a) $\mathrm{I}(\omega, T) = \omega$ *a* $\mathrm{I}(\kappa, T) = 1$ *pro $\kappa > \omega$. Tudíž je T kompletní.*
   b) *T není konečně axiomatizovatelná.*
2) a) *T je* 1*-koexistenční a tedy má eliminaci kvantifikátorů a je modelově kompletní. Dále je $\langle \mathbb{N}, n \rangle_{n \in \mathbb{N}}$ její prvomodel.*
   b) *Teorie T není* f*-homogenní.*

Důkaz. 1) a) je jasné. b) Konečná část $T' \subseteq T$ má jasně model, který není modelem T. Tudíž T není konečně axiomatizovatelná.

2) a) Dokážeme, že T je 1-koexistenční. Buď f neprázdné konečné parciální vnoření modelu $\mathcal{A}$ teorie T do modelu $\mathcal{B}$ teorie T. Buď $\overline{a}$ prosté očíslování $\mathrm{dom}(f)$, $\mathrm{l}(\overline{a}) = n$, $\chi(x_0, \dots, x_{n-1}, y)$ elementární konjunkce a $a \in A$ s $\mathcal{A} \models \chi[\overline{a}, a]$. Máme najít $b \in B$ s $\mathcal{B} \models \chi[f\overline{a}, b]$. Konjunkty χ obsahující y jsou bez újmy na obecnosti atomické tvaru $y = x_i$, $y = c_k$ a jejich negace. Je-li nějaký atomický, je jím b jednoznačně určeno. Nechť jsou všechny negace atomických. Protože jich je konečně mnoho, najdeme v nekonečné množině B prvek b, který je všechny splňuje v $\mathcal{B}$.

Protože je T 1-koexistenční, má eliminaci kvantifikátorů a je modelově kompletní. Tvrzení o prvomodelu plyne z toho, že $\langle \mathbb{N}, n\rangle_{n\in\mathbb{N}}$ je jasně algebraický prvomodel T.

b) $\mathcal{A} = \langle \mathbb{N}, 2k\rangle_{k\in\mathbb{N}}$, $\mathcal{B} = \langle \mathbb{N}, k\rangle_{k\in\mathbb{N}}$ jsou modely T. Parciální vnoření $f = \{\langle 0, 0\rangle\}$ nelze bezprostředně rozšířit do 1. Je-li totiž $f' = f \cup \langle 1, b\rangle$, je $b = c_k^B$ pro nějaké i, tudíž platí $\mathcal{B} \models (x = c_k)[b]$. Avšak $\mathcal{A} \not\models (x = c_k)[1]$ a f' tedy není parciální vnoření $\mathcal{A}$ do $\mathcal{B}$. □

A.7 Teorie unárního predikátu.

TVRZENÍ A.7.1. (Vlastnosti teorií UE, UE(m, n).)

1) a) *Jednoduchá kompletní extenze teorie* UE *je až na ekvivalenci teorií právě teorie* UE(m, n) *s* $m, n \in \mathbb{N} \cup \{\infty\}$, $m + n \neq 0$.

   b) *Teorie* UE *není modelově kompletní a tedy nemá eliminaci kvantifikátorů.*

2) a) *Každá teorie* UE(m, n) *s* $m, n \in \mathbb{N} \cup \{\infty\}$ *a* $m + n \neq 0$ *je* f-*homogenní a má tedy eliminaci kvantifikátorů a je modelově kompletní.*

   b) *Pro* $m, n \in \mathbb{N} \cup \{\infty\}$ *s* $m + n = \infty$ *a* $\kappa \geq \omega$ *je*

$$\mathrm{I}(\kappa, \mathrm{UE}(m, n)) = \begin{cases} 1 & \text{když } m < \infty \text{ nebo } n < \infty, \\ 2 \cdot \kappa(<, \infty) + 1 & \text{jinak.} \end{cases}$$

Důkaz. 1) a) Každá teorie UE(m, n) je kompletní. Když totiž $m + n < \infty$, má UE(m, n) až na izomorfizmus právě jeden model (a to velikosti $m + n$); tedy je kompletní. Když $m + n = \infty$, má UE(m, n) až na izomorfizmus právě jeden model velikosti ω; tedy je kompletní.

Je-li T jednoduchá kompletní extenze teorie UE, tak UE$(m, n) \subseteq \mathrm{Th}(T)$ pro nějaké $m, n \in \mathbb{N} \cup \{\infty\}$. Díky kompletnosti UE$(m, n)$ a T je nutně $\mathrm{Th}(\mathrm{UE}(m, n)) = \mathrm{Th}(T)$.

b) Podstruktura modelu teorie UE je její model T; odtud plyne, že UE není modelově kompletní a tudíž nemá eliminaci kvantifikátorů.

2) a) Snadno se zjistí, že neprázdné konečné parciální vnoření mezi modely UE(m, n) lze bezprostředně prodloužit.

b) Případ $m < \infty$ nebo $n < \infty$ je jasný. Buď $m = \infty = n$, $\kappa \geq \omega$. Model $\mathcal{A} = \langle A, U^A\rangle \models$ UE(m, n) velikosti κ je až na izomorfizmus určen dvojicí $\langle |U^A|, |A - U^A|\rangle = \langle m, n\rangle$, $m, n \leq \kappa$ a nekonečné. Jsou možné právě jen případy: $m < \kappa$, $n = \kappa$; $m = \kappa$, $n < \kappa$; $m = \kappa = n$. Těch je právě $2 \cdot \kappa(<, \infty) + 1$. □

A.8 Teorie bijekcí.

TVRZENÍ A.8.1. (Vlastnosti teorie BI.)

1) *Pro teorii* BI *platí:*
   a) $\mathrm{I}(\kappa, \mathrm{BI})$ *je* 0 *pro* $\kappa \in \mathbb{N}$ *liché,* 1 *jinak.*
   b) *Má spočetně neekvivalentních jednoduchých kompletních extenzí, a to právě:*
   $$\mathrm{BI}(2n) \text{ s } 0 < n \in \mathbb{N}, \qquad \mathrm{BI}(\infty).$$
   c) *Není otevřeně axiomatizovatelná.*
   d) *Není modelově kompletní.*
   e) *Má algebraický prvomodel; je jím dvouprvkový model.*

2) *Pro teorii* BI(∞) *platí:*
   a) *Není ani konečně ani otevřeně axiomatizovatelná.*
   b) *Je* f-*homogenní a tedy má eliminaci kvantifikátorů a je modelově kompletní.*
   c) *Má prvomodel* $\langle \mathbb{N}, U, P\rangle$, *kde* $U = \{2n;\, n \in \mathbb{N}\}$, $P = \{\langle 2n, 2n + 1\rangle;\, n \in \mathbb{N}\}$.

Důkaz je snadný. □

A.8.2. **Teorie** BII.

Označme BII teorii v jazyce $L^{\mathrm{BII}} = \langle U, V, P, R\rangle$ s rovností, kde U, V jsou unární a P, R binární relační symboly, přičemž axiomatika vyjadřuje:

(a) „existuje nekonečně prvků", (b) „U, V jsou disjunktní",
(c) „P je prosté zobrazení U na V", (d) „R je prosté zobrazení $U \cup V$ na komplement $U \cup V$".

Buď $\mathcal{A} \models$ BII. Množinu definovanou bez parametrů v $\mathcal{A}$ formulí $(\exists y)(U(y)\ \&\ R(y,x))$ resp. $(\exists y)(V(y)\ \&\ R(y,x))$ označme

$$U_R^A \text{ resp. } V_R^A. \tag{A.7}$$

Zřejmě platí:

$$|U^A| = |V^A| = |A - (U^A \cup V^A)| = |A| = |U_R^A| = |V_R^A|, \tag{A.8}$$
$$U_R^A \cap V_R^A = \emptyset, \qquad U_R^A \cup V_R^A = A - (U^A \cup V^A). \tag{A.9}$$

LEMMA A.8.3. *Buďte $\mathcal{A}$, $\mathcal{B}$ modely* BII *téže velikosti. Pak prosté zobrazení X^A na X^B, kde X je U, V, U_R nebo V_R, lze rozšířit jednoznačně do izomorfizmu $\mathcal{A}$ a $\mathcal{B}$.*

Důkaz. Buď h prosté zobrazení X^A na X^B a X buď U. Zobrazení h se rozšíří do hledaného izomorfizmu jednoznačně: $h(P^A(a)) = P^B(h(a))$ pro $a \in U^A$, $h(R^A(a)) = R^B(h(a))$ pro $a \in U^{A'} \cup V^A$. Přitom $P^{\cdots}(a)$ značí b takové, že $P^{\cdots}(a,b)$ a podobně pro $R^{\cdots}$.

Zcela obdobně je tomu, když X je V, U_R nebo V_R. □

TVRZENÍ A.8.4. (Vlastnosti BII.) *Teorie* BII *má následující vlastnosti:*

1) *Je kategorická v každé nekonečné velikosti a tudíž je kompletní a má prvomodel.*
2) a) *Je modelově kompletní.*
   b) *Nemá eliminaci kvantifikátorů.*
3) a) *Není konečně axiomatizovatelná.*
   b) *Není otevřeně axiomatizovatelná.*
4) *Buď $\mathcal{A} \models$* BII. *Atomy algebry* $\mathrm{Df}^1(\emptyset, \mathcal{A})$ *jsou právě*
$$U^A,\ V^A,\ U_R^A,\ V_R^A.$$
5) *Buď* BII° *extenze* BII *o následující definice predikátových symbolů U_R, V_R:*
$$U_R(x) \leftrightarrow (\exists y)(U(y)\ \&\ R(y,x)), \qquad V_R(x) \leftrightarrow (\exists y)(V(y)\ \&\ R(y,x)).$$
   Teorie BII° *je* f-*homogenní.*

Důkaz. 1) Jsou-li $\mathcal{A}$, $\mathcal{B}$ modely teorie BII téže velikosti, sestrojíme pomocí (A.8) snadno izomorfizmus $\mathcal{A}$ a $\mathcal{B}$. Tudíž je BII kategorická v každé nekonečné velikosti. Odtud plyne, že je BII kompletní. Každý model teorie BII má dle Löwenheim-Skolemovy věty spočetný elemetární podmodel a ten je díky ω-kategoričnosti jediný až na izomorfizmus; je to tedy prvomodel.

2) a) Buďte $\mathcal{A} \subseteq \mathcal{B}$ modely BII, $\varphi(\overline{x})$ nějaká L^{BII}-formule, $\overline{a} \in A^{\mathrm{l}(\overline{a})}$; dokazujeme $\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}]$. Buďte $\mathcal{A}'$, $\mathcal{B}'$ dle Löwenheim-Skolemovy věty takové, že $\mathcal{A} \prec \mathcal{A}'$, $\mathcal{B} \prec \mathcal{B}'$, $|B| < |A'| = |B'|$. Protože $|U^{A'}| = |U^{B'}| = |A'|$ a podobně pro V a W, existuje dle A.8.3 izomorfizmus h struktury $\mathcal{A}'$ a $\mathcal{B}'$, identický na A. Pak máme

$$\mathcal{A} \models \varphi[\overline{a}] \Leftrightarrow \mathcal{A}' \models \varphi[\overline{a}] \Leftrightarrow \mathcal{B}' \models \varphi[h\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[h\overline{a}] \Leftrightarrow \mathcal{B} \models \varphi[\overline{a}].$$

b) Ukážeme, že BII není 1-koexistenční. Buďte $\mathcal{A}$, $\mathcal{B}$ modely BII, $a \in W^A - R^A[V^A]$, $b \in W^B - R^B[U^B]$. Pak $f = \{\langle a, b\rangle\}$ je parciální vnoření $\mathcal{A}$ do $\mathcal{B}$. Platí: $\mathcal{A} \models \chi(x)[a]$, kde $\chi(x)$ je $R(y,x)\ \&\ U(x)$. Avšak $\mathcal{B} \not\models \chi(x)[f(a)]$.

3) a) Sporem. Pokud by BII byla konečně axiomatizovatelná, bylo by možné nahradit schema „existuje nekonečně prvků" formulí „existuje alespoň n prvků" s jistým $n \in \mathbb{N}$. Pak by existoval konečný model takové axiomatiky, což je spor.

b) Každý model teorie BII má čtyřprvkovou podstrukturu; ta není modelem BII a tudíž BII není otevřeně axiomatizovatelná.

4) Stačí dokázat, že žádná z uvedených čtyř množin X^A nemá vlastní neprázdnou podmnožinu Y definovanou bez parametrů v $\mathcal{A}$. Pokud je $\emptyset \neq Y \subsetneq X^A$ existuje, $a \in Y$, $b \in X^A - Y$ a prosté zobrazení f množiny X^A na X^B s $f(a) = b$. Podle A.8.3 existuje automorfizmus h struktury $\mathcal{A}$ rozšiřující f; pak není $h[Y] = Y$, tudíž Y není definovaná bez parametrů v $\mathcal{A}$.

5) Buď f neprázdné konečné parciální vnoření modelu $\mathcal{A}$ teorie BII do modelu $\mathcal{B}$ teorie BII, nechť $\chi(x_0, \ldots, x_{n-1}, y$ je elementární konjunkce jazyka L^{BII} a $a_0, \ldots, a_{n-1}$ jsou z dom(f) a d z A splňuje $\mathcal{A} \models \chi(x_0, \ldots, x_{n-1})[a_0, \ldots, a_{n-1}, d]$; hledáme $d' \in B$ tak, aby platilo $\mathcal{B} \models \chi(x_0, \ldots, x_{n-1})[f(a_0), \ldots, f(a_{n-1}), d']$. Je-li některý konjunkt z χ tvaru $x_i = y$, $P(x_i, y)$, $P(y, x_i)$, $R(x_i, y)$, $R(y, x_i)$, je prvek d' jednoznačně určen. V opačném případě je třeba volit d' tak, aby splňoval konečně mnoho negací atomických formulí uvedených tvarů o prvcích $f(a_i)$ v $\mathcal{B}$; to díky nekonečnosti množin U^B, V^B, U_R^B, V_R^A lze. $\square$

POZNÁMKA A.8.5. To, že BII nemá eliminaci kvantifikátorů, můžeme dokázat i následovně.

Buď $\mathcal{A} \models$ BII. Pak algebra podmožin A, definovaných bez parametrů v $\mathcal{A}$ nějakou otevřenou formulí s jedinou proměnnou, je jasně generovaná množinami U^A, V^A, $A - (U^A \cup V^A)$(které jsou jejími atomy a tedy je to algebra osmiprvková). Speciálně množina $\{a \in A;\ (\exists y)(U(y)\ \&\ R(y, x))[a]\}$ není v této algebře; tudíž $(\exists y)(U(y)\ \&\ R(y, x))$ není v BII ekvivalentní žádné otevřené formuli.

A.9 Poznámky.

Příloha B

Nerozhodnutelnost

B.1 Základní pojmy.

Základním cílem je zjistit složitost množiny Th_T všech dokazatelných sentencí dané teorie T, zejména zda je dána algoritmicky, čili je rekurzivní; je-li, budeme říkat, že je T rozhodnutelná, v opačném případě pak nerozhodnutelná.

Není-li řečeno jinak, rozumíme dále čísly přirozená čísla. Rekurzivní funkce jsou číselné totální funkce definované induktivně v B.1.2, rekurzivní relace jsou pak ty, jejichž charakteristické funkce jsou rekurzivní. Jsou to právě číselné totální funkce a relace, definované Δ_1-formulí aritmetiky ve standardním modelu $\mathcal{N}$ přirozených čísel – viz B.1.3. Mluví se pak o induktivním či aritmetickém modelu rekurzivních funkcí a relací. Dalším modelem je pak turingovský, poskytující tyto funkce a relace pomocí Turingových strojů.

Množinu Th_T lze mít dánu jako číselnou na základě „číselné prezentace“ základní syntaxe teorie T. Základními syntaktickými pojmy rozumíme ty, které nakonec dovolí definovat Th_T. Číselná prezentace je taková, že symboly jazyka uvažované teorie jsou dány jako přirozená čísla, konečné sekvence symbolů, konečné sekvence takových konečných sekvencí atd. jsou (zakódovány) jako přirozená čísla a dále relevantní syntaktické predikce a operace jsou dány jako predikce a operace s přirozenými čísly. Takovou prezentaci lze mít v jisté expanzi $\mathcal{N}^\wedge$ standardního modelu $\mathcal{N}$ přirozených čísel o vhodně definované funkce a predikáty. Mezi nimi budou takové, které prezentují „kalkulus (konečných) sekvencí“, tj. pojem „být sekvencí“ a dále běžné operování se sekvencemi, jako získání délky, konkatenace, vytvoření (kódu) sekvence $\langle x_1, \ldots, x_n\rangle_n$ atd.

Když např. $\mathrm{Vr} : \mathbb{N} \to \mathbb{N}$ je definovaná prostá číselná funkce a $\mathrm{Vr}(n)$ prezentuje n-tou proměnnou v_n, dále číslo $=^\bullet$ resp. $+^\bullet$ prezentuje symbol $=$ resp. binární funkční symbol $+$, tak $\langle =^\bullet, \mathrm{Vr}(1), \mathrm{Vr}(1)\rangle_3$ prezentuje atomickou formuli $v_1 = v_1$, $\langle +^\bullet, \mathrm{Vr}(1), \mathrm{Vr}(2)\rangle_3$ prezentuje term $v_1 + v_2$. Dále dvojice relací $\mathcal{F}(x)$, $Ar_{\mathcal{F}}$ s $\mathcal{F}(x) \leftrightarrow x = +^\bullet$, $Ar_{\mathcal{F}}(x) \leftrightarrow x = \langle +^\bullet, 2\rangle_2$ prezentuje jazyk $L = \langle + \rangle$, kde $+$ je binární funkční symbol. Predikáty Term_L či Fm_L jsou definovány induktivně; protože v „prezentační struktuře“ $\mathcal{N}^\wedge$ platí axiomy indukce, jsou uvedené predikáty rovněž prezentovány v $\mathcal{N}^\wedge$. Podobně tam je i syntaktická operace „výsledek substituce termu za proměnnou do formule“ a všechny další predikce a operace ze základní syntaxe. Stručně řečeno: „prezentační struktura“ umožňuje rozvíjet základní syntax jazyka v ní prezentovaného tak, jak se to provádělo v „přirozené prezentaci“ (metamatematiky) dosud. Dokonce to lze učinit v rámci teorie $S^\wedge$, která je $\mathcal{N}^\wedge$ modelem; mluvíme pak o „aritmetické prezentaci“ či „aritmetizaci“ základní syntaxe v „prezentační teorii“ $S^\wedge$. Viz B.1.5.

Hierarchie aritmetických formulí a aritmetické množiny.

Připomeňme, že jazyk aritmetiky je $\langle \mathrm{S}, +, \cdot, 0, \leq\rangle$. Jazyk obsahující S a 0 se nazývá numerický a teorie v něm numerická. Pro $n \in \mathbb{N}$ a je $\underline{n}$ term $\mathrm{S}\cdots\mathrm{S}0$, S aplikováno n-krát; nazývá se (n-tý) numerál a $\underline{0}$ je 0. Pro term t značí nt term $t + \cdots + t$, $+$ aplikováno $(n-1)$-krát.

B.1.1. Σ_n-, Π_n- a Δ_n-formule a množiny. Aritmetické množiny.

1. *Omezená formule* jazyka aritmetiky je formule jazyka aritmetiky, ve které je každá kvantifikace *omezená*, tj. tvaru $(Qx \leq y)$, kde Q je kvantifikátor a x, y jsou různé. Taková formule je ekvivalentní formuli tvaru $(Q_1 x_1 \leq y_1) \cdots (Q_n x_n \leq y_n)\varphi$, kde Q_i jsou kvantifikátory a φ je otevřená formule.

2. Hierarchii Σ_n*-formulí* a Π_n*-formulí* jazyka aritmetiky definujeme indukcí:

• Σ_0-formule a Π_0-formule jsou právě omezené formule.

• Σ_n*-formule* resp. Π_n*-formule* jsou formule právě tvaru $(\exists \overline{x})\varphi$ resp. $(\forall \overline{x})\varphi$, kde φ je Π_{n-1}-formule resp. Σ_{n-1}-formule.

• Formule jazyka aritmetiky je Δ_n (*-formule*), je-li logicky ekvivalentní jak nějaké Σ_n-formuli tak nějaké Π_n-formuli.

Je-li Γ některý ze symbolů Σ_n, Π_n, Δ_n, značí Γ také množinu všech Γ-formulí. Je-li navíc T teorie resp. struktura v jazyce L rozšiřujícím jazyk aritmetiky, je $(\Gamma)^T$ resp. $(\Gamma)^{\mathcal{A}}$ množina všech Γ*-formulí v T* resp. *v* $\mathcal{A}$, tj. takových, které jsou ekvivalentní v T resp. v $\mathcal{A}$ nějaké Γ-formuli. Pro T prázdnou píšeme jen $(\Gamma)^L$ a je-li L jazyk aritmetiky, můžeme psát též jen Γ. Zcela stejně definujeme $\Sigma_{n,L}$-, $\Pi_{n,L}$- a $\Delta_{n,L}$*-formule* jazyka L obsahujícího $\leq$, dále $(\Sigma_{n,L})^T$ či $(\Sigma_{n,L})^{\mathcal{A}}$ atd.

3. Říká se, že množina je Σ_n resp. Π_n resp. Δ_n (*-množina*), je-li to množina definovaná (s parametry či bez parametrů) nějakou Σ_n- resp. Π_n- resp. Δ_n-formulí ve standardním modelu $\mathbf{N}$. Obory takových podmnožin $\mathbb{N}^k$ jsou uzavřeny na sjednocení a průnik. Komplement Σ_n- resp. Π_n-množiny je Π_n- resp. Σ_n-množina, komplement Δ_n-množiny je Δ_n-množina. Je-li $A \subseteq \mathbb{N}^k$ i její komplement Σ_n-množina, je to Δ_n-množina. Složení totálních funkcí, které jsou Δ_n, je Δ_n. Každá množina definovatelná v $\mathbf{N}$ je Σ_n a také Π_n pro nějaké n (díky tomu, že definující formuli můžeme vzít v prenexním tvaru); množiny definovatelné v $\mathbf{N}$ se nazývají *aritmetické*. Označme ještě

$$^{\mathbb{N}}\Sigma_n \text{ resp. } ^{\mathbb{N}}\Pi_n \text{ resp. } ^{\mathbb{N}}\Delta_n \tag{B.1}$$

množinu všech podmnožin $\mathbb{N}$, definovaných v $\mathbf{N}$ nějakou Σ_n- resp. Π_n- resp. Δ_n-formulí. Platí pro $n \in \mathbb{N}$:

$$^{\mathbb{N}}\Sigma_0 = {}^{\mathbb{N}}\Pi_0 = {}^{\mathbb{N}}\Delta_0 \subseteq {}^{\mathbb{N}}\Delta_n = {}^{\mathbb{N}}\Sigma_n \cap {}^{\mathbb{N}}\Pi_n \subseteq {}^{\mathbb{N}}\Sigma_n \cup {}^{\mathbb{N}}\Pi_n \subseteq {}^{\mathbb{N}}\Delta_{n+1}.$$

Rekurzivní funkce a relace.

B.1.2. Obor *rekurzivních funkcí* je nejmenší obor číselných funkcí (tj. tvaru $F : \mathbb{N}^n \to \mathbb{N}$ s nenulovým $n \in \mathbb{N}$), který obsahuje funkce $\mathrm{S}, \mathrm{I}_i^n, +, \cdot, \mathrm{K}_<$ (tzv. *základní rekurzivní funkce*: $\mathrm{S}(x) = x + 1$, $\mathrm{I}_i^n(x_1, \ldots, x_n) = x_i$ (pro $1 \leq i \leq n$), $\mathrm{K}_< : \mathbb{N}^2 \to 2$ s $\mathrm{K}_<(x, y) = 0$ resp. $1 \Leftrightarrow x < y$ resp. jinak – $\mathrm{K}_<$ je charakteristická funkce relace $<$) a je uzavřený na skládání a *speciální μ-operaci*, která funkci $G : \mathbb{N}^{n+1} \to \mathbb{N}$ s $(\forall \overline{z})(\exists x)G(\overline{z}, x) = 0$ přiřadí funkci $\mu x G(\overline{a}, x) = \min\{b;\, G(\overline{a}, b) = 0)\}$. Číselná relace či množina (tj. nějaké $S \subseteq \mathbb{N}^n$) je *rekurzivní*, je-li její charakteristická funkce rekurzivní, a je *rekurzivně spočetná*, stručně r.s., existuje-li rekurzivní relace R tak, že $S(\overline{a}) \leftrightarrow (\exists x)R(\overline{a}, x)$ platí pro každé $\overline{a} \in \mathbb{N}^n$, tj. je-li to definiční obor nějaké rekurzivní relace. *Komplement* relace $R \subseteq \mathbb{N}^n$ je $\mathbb{N}^n - R$, stručně též $-R$.

TVRZENÍ B.1.3.

1) a) *Totální číselná funkce je rekurzivní, právě když je Δ_1, právě když je Σ_1.*
   b) *Číselná relace je rekurzivní, právě když je Δ_1*

2) a) *Číselná relace je rekurzivně spočetná, právě když je Σ_1.*
   b) (O komplementu.) *Je-li číselná množina i její komplement r.s., je to rekurzivní množina.*

Důkaz. Důkazy 1) a), b), 2) a) neuvádíme, nejsou však obtížné. 2) b) je triviální důsledek. □

Platí tedy:

obor všech rekurzivních podmnožin $\mathbb{N} = {}^{\mathbb{N}}\Delta_1 \subseteq {}^{\mathbb{N}}\Sigma_1 =$ obor všech r.s. podmnožin $\mathbb{N}$.

PŘÍKLADY B.1.4.

1. Vlastnosti „y je dělitel x“, „x je prvočíslo“ jsou Δ_1 v $\mathbf{N}$.
2. Každá konečná podmnožina $\mathbb{N}$ je spočetná. Množina $Prv \subseteq \mathbb{N}$ všech prvočísel je rekurzivní.

Aritmetická a číselná prezentace syntaxe.

B.1.5. Specifikace „prezentační teorie $S\hat{}$“ a „prezentační struktury“ $\mathfrak{N}\hat{}$.
S je jednoduchá extenze aritmetiky $\mathrm{I}\Sigma_1$ ($=$ Q $\cup$ schema indukce pro Σ_1-formule) s $\mathfrak{N} \models S$,
$S\hat{}$ je extenze S o všechny Δ_1-definice.
$\mathfrak{N}\hat{}$ je přirozená expanze $\mathfrak{N}$ do modelu $S\hat{}$.

B.1.6. **Vlastnosti $S\hat{}$.**

Teorie $S\hat{}$ je „Δ_1-plná“ (co do obsažnosti a konstrukčnosti), tj. platí následující a) – c):

a) i) $\Sigma_{1,L(S\hat{})}[\Pi_{1,l(S\hat{})}]$-formule je v $S\hat{}$ ekvivalentní $\Sigma_1[\Pi_1]$-formuli. ii) $\Delta_{1,L(S\hat{})}$-definice poskytuje již existující symbol teorie $S\hat{}$. iii) Obor Σ_1- a Π_1-formulí teorie $S\hat{}$ je uzavřen v $S\hat{}$ na konjunkce, disjunkce, omezené kvantifikace $(Qx \leq t)$ s termem t, Δ_1-formule pak i na negaci. iv) Platí každý axiom indukce pro Σ_1-formule teorie $S\hat{}$.

b) V $S\hat{}$ je „kalkulus sekvencí“, tj. predikátový symbol $\mathrm{Seq}(x)$ (x je konečná sekvence), funkční symboly $\mathrm{lh}(x)$ (délka x), $(x)_y$ (y-tý člen x), $x{\restriction}y$ (zkrácení x na délku y), $x\smile y$ (konkatenace x a y), n-ární funkční symboly $\langle x_1,\ldots,x_n\rangle_n$, stručně $\langle x_1,\ldots,x_n\rangle$, s $n\in\mathbb{N}$ a $\langle\rangle_0 = 0$; $\langle x_1,\ldots,x_n\rangle_n$ je kód n-tice $x_1,\ldots,x_n$. Vše má (v $S\hat{}$ dokazatelně) předpokládané vlastnosti. Platí např. $\mathrm{Seq}(\langle x_1,\ldots,x_n\rangle_n)$, $\mathrm{lh}(\langle x_1,\ldots,x_n\rangle_n) = n$, $\mathrm{lh}(x) \leq x$, $(x)_y \leq x$, $(\exists y > x)\neg\mathrm{Seq}(y)$. V $S\hat{}$ je unární funční symbol BS takový, že platí „s je sekvence délky $\leq x$ prvků $\leq x$“ $\rightarrow s \leq \mathrm{BS}(x)$.

O konstrukci uvedených pojmů. Základem je funkční symbol $(\,,)$ uspořádaná dvojice, kde $(x,y) = z \leftrightarrow \underline{2}z = (x+y+\underline{1})(x+y)+\underline{2}x$, a jisté elementární poznatky o dělitelnosti v $\mathrm{I}\Sigma_1$, umožňující konstrukci tzv. Gödelovy β-funkce s vlastnostmi: $\beta(x,y) \leq x \dot{-} \underline{1}$, $(\exists x)(\forall i \leq n)(\beta(x,i) = F(i,\overline{p}))$, když $F(i,\overline{p})$ je funkční symbol z $S\hat{}$, přičemž proměnné x, n nejsou mezi proměnnými $i, \overline{p}$. Pak se definuje např. $\mathrm{lh}(x) = \beta(x,0)$, $(x)_y = \beta(x, y+\underline{1})$,

$$\mathrm{Seq}(x) \leftrightarrow (\forall y < x)(\mathrm{lh}(y) \neq \mathrm{lh}(x) \vee (\exists u < \mathrm{lh}(x))((y)_u \neq (x)_u)).$$

c) i) Rekurzí sestrojená funkce je v $S\hat{}$, je-li „konstruující“ funkce z $S\hat{}$.

ii) Je-li notace $\underline{\mathcal{F}}$ v $S\hat{}$ (tj. $\mathcal{F}$, $Ar_{\mathcal{F}}$ jsou v $S\hat{}$), je obor $\mathrm{D}(\mathcal{F})$ designátorů v $S\hat{}$.

(*Důkaz* ii). Obor $\mathrm{D}(\mathcal{F})$ designátorů je definován formulí $(\exists u)$(„u je odvození v $\underline{\mathcal{F}}$“ & $x = (u)_{\mathrm{lh}(u)\dot{-}1}$), kde „$u$ je odvození v $\underline{\mathcal{F}}$“ je definováno $\Delta_{1,L(S\hat{})}$-formulí, jak se snadno zjistí. Zřejmě lze $(\exists u)$ nahradit $(\exists u \leq \mathrm{BS}(x))$. Tedy uvedená definice je $\Delta_{1,L(S\hat{})}$ a tudíž $\mathrm{D}(\mathcal{F})$ je v $S\hat{}$. $\Box$)

B.1.7. **Prezentace základní syntaxe v $S\hat{}$ a $\mathfrak{N}\hat{}$. Rekurzivně axiomatizovaná teorie.**

• Logické symboly se prezentují jako různé konstantní termy $\neg^\bullet, \rightarrow^\bullet, v^\bullet, \forall^\bullet, =^\bullet$ tvaru $\underline{n}$ s (technickou podmínkou) $\neg\mathrm{Seq}(\underline{n})$. V $S\hat{}$ je funkční symbol $\mathrm{Vr}(x) = \langle v^\bullet, x\rangle$, prezentující x-tou proměnnou, relační symbol $\mathrm{Var}(y) \leftrightarrow (\exists x < y)(y = \mathrm{Vr}(x))$, značící „$y$ je proměnná“, relační symbol $\mathrm{Gqs}(z) \leftrightarrow (\exists y < z)(\mathrm{Var}(y)\ \&\ (z = \langle\forall^\bullet, y\rangle))$, značící „$z$ je obecná kvantifikace“.

Jazyk L je v $S\hat{}$ dán nějakými symboly $\mathcal{R}, Ar_{\mathcal{R}}, \mathcal{F}, Ar_{\mathcal{F}}$ teorie $S\hat{}$; přitom $\mathcal{R}, \mathcal{F}$ jsou disjunktní a neobsahují žádný mimologický symbol a $\mathcal{R}(x) \rightarrow \neg\mathrm{Seq}(x)$, $\mathcal{F}(x) \rightarrow \neg\mathrm{Seq}(x)$. $\mathcal{R}(x)$ resp. $Ar_{\mathcal{R}}(x)$ značí, že „x je relační symboly L“ resp. „četnosti $Ar_{\mathcal{R}}(x)$“ a podobně pro $\mathcal{F}$. Díky c) ii) máme též v $S\hat{}$ obor L-termů resp. L-formulí, daný jako predikátový symbol Term_L resp. Fm_L. Je jen technickým problémem zjistit, že potřebné syntaktické predikce a operace, jako např. „x je volná proměnná v y“, „x je sentence“, „z je substituovatelné za y do x“, „výsledek substituce termu z za proměnnou y do formule x“ jsou v $S\hat{}$, symbolicky po řadě značené následovně:

$$\mathrm{Fr}_L(x,y),\ \mathrm{Sent}_L(x),\ \mathrm{Substl}_L(x,y,z),\ \mathrm{Sub}_L(x,y,z),\ \mathrm{LAx}_L.$$

Pro numerický jazyk je v $S\hat{}$ i $\mathrm{Num}(x)$, poskytující x-tý numerál. Sumárně řečeno: Je-li jazyk v $S\hat{}$, je jeho základní syntax v $S\hat{}$. Index L v symbolech Term_L, Fm_L atd. často pro přehlednost vynecháváme.

L-teorie T je dále dvojice L, Ax_T, kde Ax_T je nový predikátový symbol s $\mathrm{Ax}_T(x) \rightarrow \mathrm{Fm}_L(x)$, představující axiomatiku T. Označme $\varphi^{Prf}_{\mathrm{Ax}_T}$ formuli (B.2), zachycující vztah „y je důkaz x v T“:

$$\begin{aligned}&\mathrm{Seq}(y)\&\ \mathrm{lh}(y) \neq 0\ \&\ (y)_{\mathrm{lh}(y)-1} = x\ \&\ (\forall u < \mathrm{lh}(y))(\mathrm{LAx}((y)_u) \vee \mathrm{Ax}_T((y)_u) \vee \\ &\quad (\exists v, w < u)\ ((y)_v = \langle\rightarrow^\bullet, (y)_w, (y)_u\rangle \vee (\exists z < (y)_u)(\mathrm{Gqs}(z)\ \&\ (y)_u = \langle z, (y)_v\rangle)))).\end{aligned} \tag{B.2}$$

Buď $S\hat{}(T)$ extenze $S\hat{}$ o definice $\mathrm{Prf}_T(x,y) \leftrightarrow \varphi^{Prf}_{\mathrm{Ax}_T}(x,y)$, $\mathrm{Th}_T(x) \leftrightarrow (\exists y)\mathrm{Prf}_T(x,y)\ \&\ \mathrm{Sent}(x)$ a $\mathrm{nTh}_T(x) \leftrightarrow \mathrm{Th}_T(\langle\neg^\bullet, x\rangle)$; $S\hat{}(T)$ poskytuje aritmetickou prezentaci základní syntaxe teorie T.

• Je-li O symbol jazyka $L(S\hat{})$, označme $\grave{O}$ jeho sémantickou interpretaci v $\mathfrak{N}\hat{}$. Máme pak např. číselnou prezentaci $\grave{\mathrm{Fm}}_L$ množiny formulí jazyka L z $S\hat{}$; její prvky jsou „číselné kódy“

formulí jazyka L. Když ještě $Ax_T \subseteq {}^{\backprime}\mathrm{Fm}_L$, je dvojice ${}^{\backprime}L, Ax_T$ číselná prezentace nějaké L-teorie T, a $\langle \mathbf{N}^{\wedge}, Ax_T\rangle$ lze jednoznačně expandovat do modelu teorie $S^{\wedge}(T)$, který označme $\mathbf{N}^{\wedge}(T)$. Zde pak máme ${}^{\backprime}\mathrm{Th}_T$ jakožto číselnou prezentaci syntaktické predikce „být sentencí dokazatelnou v T“ a ${}^{\backprime}\mathrm{Th}_T \subseteq \mathbb{N}$. Symbol ${}^{\backprime}$ můžeme vynechat pro přehlednost, pokud to nevede k nedorozumění.

- Teorie (číselně prezentovaná) je *rekurzivně axiomatizovaná*, je-li její axiomatika rekurzivní.

POZNÁMKA o vyjadřování. Buď T v rekurzivním jazyce. Pak se o ní vyjádřujeme v „přirozené“ prezentaci a říkáme např. φ je sentence, $T \vdash \varphi$. Totéž vyjádříme v číselné prezentaci jako ${}^{\backprime}\mathrm{Sent}(\varphi)$, ${}^{\backprime}\mathrm{Th}_T(\varphi)$, chápeme-li již φ jako číselně prezentované (a tedy $\varphi \in \mathbb{N}$), a jako $\mathrm{Sent}(\underline{\varphi})$, $\mathrm{Th}(\underline{\varphi})$, jde-li o aritmetickou prezentaci. Někdy se pro názornost užívá symbol $\ulcorner\varphi\urcorner$ k označení číselné prezentace přirozeně prezentované formule φ. Je-li T numerická, tj. v jazyce obsahujícím 0, S, kdy lze mluvit o numerálech, tak pro φ tvaru $\varphi(v_0)$, má dobrý smysl formule $\varphi(v_0/\underline{\ulcorner\varphi\urcorner})$, stručněji $\varphi(\underline{\ulcorner\varphi\urcorner})$, nejpřehledněji jen $\varphi(\underline{\varphi})$, v numerické prezentaci pak $\mathrm{Sub}(\varphi, \mathrm{Var}(0), \mathrm{Num}(\varphi))$; vynechali jsme ${}^{\backprime}$.

B.1.8. **Rozhodnutelná a nerozhodnutelná teorie a jazyk.**
Teorie T v rekurzivním jazyce je *rozhodnutelná*, je-li Th_T rekurzivní; jinak je *nerozhodnutelná*. Rekurzivní jazyk L je *(ne)rozhodnutelný*, je-li (ne)rozhodnutelná prázdná L-teorie.

B.1.9. Shrnutí o „prezentační teorii“ $S^{\wedge}$ a „prezentační struktuře“ $\mathbf{N}^{\wedge}$.

- $S^{\wedge}$ je Δ_1-plná - viz B.1.7.
- V $S^{\wedge}$ je dána exaktně prezentace základní syntaxe jazyků z $S^{\wedge}$. Je-li T v jazyce z $S^{\wedge}$ a s axiomatikou Ax_T, je T a její základní syntax v $S^{\wedge}(T)$. (Když Ax_T je v $S^{\wedge}$, $S^{\wedge}(T)$ buď $S^{\wedge}$.)
- V expanzi $\mathbf{N}^{\wedge}$ je číselná prezentace základní syntaxe jazyků z $S^{\wedge}$. Každý rekurzivní jazyk a každá rekurzivní axiomatika v něm je v $\mathbf{N}^{\wedge}$. Když $Ax_T \subseteq {}^{\backprime}\mathrm{Fm}_L$ pro L z $S^{\wedge}$ je axiomatika T, je číselná prezentace základní syntaxe T v $\mathbf{N}^{\wedge}(T)$.

Poznamenejme, že v $\mathbf{N}^{\wedge}(T)$ jsou prezentovány i nerekurzivní jazyky a aritmetizaci lze realizovat bez předpokladu $S \models \mathbf{N}$.

B.2 Věty o nerozhodnutelnosti.

Dále uvažujeme jen teorie v rekurzivních jazycích a s rovností, není-li řečeno jinak.

TVRZENÍ B.2.1. (O složitosti Prf.) *Je-li teorie T rekurzivně axiomatizovaná, je* Prf_T *rekurzivní a* Th_T *i* nTh_T *jsou r.s.*

Kriteria rozhodnutelnosti a nerozhodnutelnosti.

Důkaz plyne ihned z tvaru formule $\varphi^{Prf}_{\mathrm{Ax}_T}(x,y)$, neboť Ax_T můžeme nahradit Δ_1- resp. Σ_1-formulí. □

B.2.2. **Rekurzivní kompletace.**
Relace $R \subseteq \mathbb{N}^2$ je *rekurzivní kompletace* teorie T, když

a) R je rekurzivní a pro $a \in \mathrm{dom}(R)$ je $R[a]$ axiomatika jednoduché kompletní extenze teorie T,
b) každá jednoduchá kompletní extenze teorie T je ekvivalentní teorii s axiomatikou tvaru $R[a]$.

Názorně lze říci, že rekurzivní kompletace teorie T je rekurzivně prezententovaný „slabý komplet“ T; oproti kompletu zde nevylučujeme ekvivalenci různých axiomatik $R[a]$, $R[a']$.

TVRZENÍ B.2.3. (Kriteria rozhodnutelnosti.)

1) *Rekurzivně axiomatizovaná kompletní teorie T je rozhodnutelná.*
2) (Kompletační kriterium rozhodnutelnosti.) *Rekurzivně axiomatizovaná teorie T mající rekurzivní kompletaci, je rozhodnutelná.*

Důkaz. 1) Protože Th_T je Σ_1 dle B.2.1, stačí dokázat, že $\mathbb{N} - \mathrm{Th}_T$ je Σ_1. Díky kompletnosti T v modelu $\mathbf{N}^{\wedge}(T)$ platí $\neg\mathrm{Th}_T(x) \leftrightarrow \mathrm{nTh}_T(x) \vee \neg\mathrm{Sent}(x)$ a vidíme, že $\mathbb{N} - \mathrm{Th}_T$ je Σ_1.

2) Předně Th_T je Σ_1 dle 1). Máme ještě dokázat, že $\mathbb{N} - \mathrm{Th}_T$ je Σ_1. Nechť Σ_1-formule $\alpha(z_0, z_1)$ definuje R a formule $\varphi^{Prf}_R(z_0, x, y)$ se získá z $\varphi^{Prf}_{\mathrm{Ax}_T}$ tak, že nahradíme $\mathrm{Ax}_T((y)_u)$ formulí

$\alpha(z_0, z_1/(y)_u)$. $\varphi_R^{Prf}(z_0, x, y)$ říká: „y je důkaz x v $R[z_0]$“. Z definice kompletace plyne platnost následující formule v $\mathbf{N}\hat{\ }(T)$: $\mathrm{Sent}(x)\ \&\ \neg\mathrm{Th}_T(x) \leftrightarrow \mathrm{Sent}(x)\ \&\ (\exists z_0, y)(\varphi_R^{Prf}(z_0, \langle \neg^\bullet, x\rangle, y))$. Formule vpravo od $\leftrightarrow$ je v $\mathbf{N}\hat{\ }(T)$ ekvivalentní Σ_1-formuli díky tvaru φ_R^{Prf}. Tudíž $\mathrm{Sent} - \mathrm{Th}_T$ je Σ_1 a tedy i $\mathbb{N} - \mathrm{Th}_T = (\mathrm{Sent} - \mathrm{Th}_T) \cup (\mathbb{N} - \mathrm{Sent})$ je Σ_1. □

B.2.4. **Metoda algoritmického překladu.**

Buďte T, T' teorie. Zobrazení $F : \mathrm{Sent}_T \to \mathrm{Sent}_{T'}$, které je Δ_1 (čili rekurzivní relací) je *algoritmický překlad* teorie T do T', jestliže pro každé $a \in \mathrm{Sent}_T$ je $\mathrm{Th}_T(a) \Leftrightarrow \mathrm{Th}_{T'}(F(a))$.

Je-li F algoritmický překlad T do T', zřejmě platí:

Je-li T nerozhodnutelná, je T' nerozhodnutelná.

TVRZENÍ B.2.5. (Kriteria nerozhodnutelnosti.)

1) *Buď $F : \mathrm{Sent}_T \to \mathrm{Sent}_{T'}$ s $F(\varphi) = \varphi^*$ dáno následující tabulkou.*

	Vztah T a T'	φ^*
a)	*T' je konzervativní extenze T.*	φ
b)	*T je konečná jednoduchá extenze T' o axiomy $\chi_1, \ldots, \chi_n$, jež jsou sentence.*	$(\chi_1\ \&\ \cdots\ \&\ \chi_n) \to \varphi$
c)	*T je extenze T' o konečně definice.*	*„překlad“ φ^* formule φ do L': $T \vdash \varphi \Leftrightarrow T' \vdash \varphi^*$*

Pak F je algoritmický překlad T do T' a tedy: Je-li T nerozhodnutelná, je T' nerozhodnutelná.

2) *Buď T' extenze T jen o nové konstantní symboly (a žádné nové mimologické axiomy). Pak T je nerozhodnutelná, právě když je T' nerozhodnutelná.*

Důkaz. 1) Zobrazení F je Δ_1, neboť konstrukce φ^* se odvolává jen na φ a konečně konkrétních formulí. Díky uvedenému vztahu mezi T a T' pak pro $L(T')$-sentenci máme $\mathrm{Th}_T(\varphi) \Leftrightarrow \mathrm{Th}_{T'}(F(\varphi))$.

2) T' je konzervativní extenze T, tudíž z rozhodnutelnosti T' plyne rozhodnutelnost T. Buď naopak T rozhodnutelná. Sentenci φ jazyka $L(T')$ přiřaďme algoritmicky formuli φ' získanou z φ nahrazením každého nového konstantního symbolu proměnnou $\mathrm{Vr}(\varphi + c)$, a dále buď φ^* generální uzávěr φ', opět jasně získaný algoritmicky; tedy je rekurzivní i funkce

$$F = \{\langle a, a^*\rangle;\ a \in \mathrm{Sent}_{L(T')}\} \cup \{\langle a, 0\rangle;\ a \in \mathbb{N} - \mathrm{Sent}_{L(T')}\}$$

Dle věty o konstantách je $T' \vdash \varphi \Leftrightarrow T \vdash \varphi^*$. Tudíž $\mathrm{Th}_{T'} = \mathrm{Sent}_{L(T')} \cap \mathrm{Th}_T(F)$ a množina vpravo je Δ_1 čili rekurzivní. Tedy je $\mathrm{Th}_{T'}$ rekurzivní a T' je rozhodnutelná. □

Věty o nerozhodnutelnosti.

B.2.6. **Reprezentovatelnost.**

Funkce $F : \mathbb{N}^n \to \mathbb{N}$ resp. relace $R \subseteq \mathbb{N}^n$ je *reprezentovaná* v numerické teorii T formulí $\varphi(x_1, \ldots, x_n, y)$ resp. $\psi(x_1, \ldots, x_n)$, platí-li pro každou n-tici $a_1, \ldots, a_n$ čísel:

$$T \vdash \varphi(\underline{a}_1, \ldots, \underline{a}_n, y) \leftrightarrow y = \underline{F(a_1, \ldots, a_n)} \text{ resp.}$$
$$R(a_1, \ldots, a_n) \Rightarrow T \vdash \psi(\underline{a}_1, \ldots, \underline{a}_n), \quad \neg R(a_1, \ldots, a_n) \Rightarrow T \vdash \neg\psi(\underline{a}_1, \ldots, \underline{a}_n).$$

Poznamenejme, že následující tvrzení můžeme ekvivalentně formulovat pomocí „rekurzivní“ místo „Δ_1(-množina)“ a „r.s.“ místo „Σ_1(-množina)“.

VĚTA B.2.7. (O Δ_1-neoddělitelnosti.) *Buď T bezesporná numerická teorie a nechť každá Δ_1-podmnožina $\mathbb{N}$ je reprezentovaná v T nějakou formulí. Pak platí:*

1) *Nechť $P \subseteq \mathbb{N}$ odděluje Th_T a nTh_T, tj. obsahuje jednu z uvedených množin a je disjunktní s druhou. Pak relace $E_P = \{\langle a, b\rangle \in \mathbb{N}^2;\ P(\mathrm{Sub}(a, \mathrm{Vr}(0), \mathrm{Num}(b)))\}$ kóduje všechny Δ_1-podmnožiny $\mathbb{N}$, tj.platí: Pro každou Δ_1-množinu $A \subseteq \mathbb{N}$ existuje $a \in \mathbb{N}$ s $A = E_P[a]$.*

2) *Th_T a nTh_T nelze oddělit Δ_1-množinou. Speciálně je T nerozhodnutelná.*

3) *Je-li T navíc rekurzivně axiomatizovaná, tak $\mathbb{N} - (\mathrm{Th}_T \cup \mathrm{nTh}_T)$ je Π_1 a není Σ_1.*

Důkaz. 1) Předně Th_T a nTh_T jsou disjunktní díky bezespornosti. (Neboť $\mathrm{Th}_T(n)$ a $\mathrm{nTh}_T(n)$ dává $\mathrm{Th}_T(m)$, kde m je konjunkce n a negace n.) Označme $\mathrm{Sub}(a, \mathrm{Vr}(0), \mathrm{Num}(b))$ jako $Sb(a,b)$. Nechť $P \subseteq \mathbb{N}$ odděluje Th_T a nTh_T; z důvodu symetrie můžeme předpokládat, že $\mathrm{Th}_T \subseteq P$. Pro Δ_1-definovanou množinu $A \subseteq \mathbb{N}$ existuje $L(T)$-formule a (tj. $\mathrm{Fm}(a)$) s jedinou volnou proměnnou $\mathrm{Vr}(0)$ tak, že $b \in A \Rightarrow \mathrm{Th}_T(Sb(a,b)) \Rightarrow P(Sb(a,b))$, $b \notin A \Rightarrow \mathrm{nTh}_T(Sb(a,b)) \Rightarrow \neg P(Sb(a,b))$. Tudíž $b \in A \Leftrightarrow E_P(a,b)$, tj. $E_P[a] = A$.

2) Když $P \subseteq \mathbb{N}$ odděluje Th_T a nTh_T a je Δ_1, je Δ_1 i $A = \{a \in \mathbb{N};\ \neg E_P(a,a)\}$. Pak existuje $a \in \mathbb{N}$ s $A = E_P[a]$. Speciálně máme $\neg E_P(a,a) \Leftrightarrow a \in A \Leftrightarrow E_P(a,a)$–spor.

3) Nyní Th_T i nTh_T jsou Σ_1 dle B.2.1. Když $\mathbb{N} - (\mathrm{Th}_T \cup \mathrm{nTh}_T)$ je Σ_1, tak je i $\mathbb{N} - \mathrm{Th}_T = \mathrm{nTh}_T \cup (\mathbb{N} - (\mathrm{Th}_T \cup \mathrm{nTh}_T))$ a tedy Th_T je Δ_1; to je ve sporu s 2). □

VĚTA B.2.8.

1) (O reprezentaci Δ_1 funkcí a relací v Robinsonově aritmetice Q.)
   a) *Každá totální funkce, která je Σ_1, je reprezentovaná v* Q *nějakou Σ_1-formulí.*
   b) *Každá relace, která je Δ_1, je reprezentovaná v* Q *nějakou Σ_1-formulí.*
2) (O nerozhodnutelnosti.) *Bezesporná teorie rozšiřující Robinsonovu aritmetiku* Q *je nerozhodnutelná a je-li navíc rekurzivně axiomatizovaná, není kompletní.*
3) Důsledky. a) Th_{Q} *je* Σ_1 *a není* Δ_1, $\quad \mathrm{Sent}_{L(\mathrm{Q})} - (\mathrm{Th}_{\mathrm{Q}} \cup \mathrm{nTh}_{\mathrm{Q}})$ *je* Π_1 *a není* Σ_1.
$$^{\mathbb{N}}\Delta_1 \subsetneq {}^{\mathbb{N}}\Sigma_1,\ {}^{\mathbb{N}}\Delta_1 \subsetneq {}^{\mathbb{N}}\Pi_1,\ {}^{\mathbb{N}}\Sigma_1 \neq {}^{\mathbb{N}}\Pi_1.$$
   b) *Jazyk aritmetiky je nerozhodnutelný.*

Důkaz. 1) Neuvádíme důkaz, není však obtížný. 2) Nerozhodnutelnost plyne ihned z B.2.7 a 1), nekompletnost v případě rekurzivní axiomatizovatelnosti pak ještě užitím B.2.3, 1). 3) a) plyne z 1) a B.2.7 3). Dokažme b) Teorie Q je extenze prázdné teorie T v jazyce aritmetiky; je to nerozhodnutelná jednoduchá extenze o konečně axiomů, tedy je T nerozhodnutelná dle B.2.5. □

TVRZENÍ B.2.9. *Bezesporná rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky* Q *má právě kontinuum neekvivalentních* JKE.

Důkaz. 1) Buď T uvažovaná teorie. Její bezesporná jednoduchá extenze o konečně axiomů je nerozhodnutelná a nekompletní dle B.2.8. Pro každý vrchol σ stromu $\langle \bigcup_{n\in\mathbb{N}} {}^{n}2, \subseteq \rangle$ sestrojíme bezespornou jednoduchou extenzi T_σ teorie T o konečně axiomů takto: Buď $T_\emptyset$ teorie T. Máme-li T_σ, buď φ_σ nezávislá sentence teorie T_σ. Buď $\varphi_{\sigma\text{-}0}$ formule $\neg\varphi_\sigma$ a $\varphi_{\sigma\text{-}1}$ formule φ_σ; buď $T_{\sigma\text{-}i} = T_\sigma \cup \{\varphi_{\sigma\text{-}i}\}$. ($\sigma\text{-}i$ značí $\sigma \cup \{\langle n, i\rangle\}$, kde $n = \mathrm{dom}(\sigma)$.) Pro $f \in {}^{\mathbb{N}}2$ buď T_f extenze T právě o axiomy $\varphi_{f\restriction n}$ s $n \in \mathbb{N}$ (tj. $T_f = \bigcup_{n\in\mathbb{N}} T_{f\restriction n}$). Pro $f \neq g \in {}^{\mathbb{N}}2$ a nejmenší n s $f(n) \neq g(n)$ je v jedné z teorií T_f, T_g formule $\varphi_{f\restriction n+1}$, právě když je v druhé její negace. Je-li konečně T'_f jednoduchá kompletní extenze teorie T_f, jsou T'_f s $f \in {}^{\mathbb{N}}2$ hledané teorie. □

TVRZENÍ B.2.10. (O r.s. axiomatizovatelnosti.) *Teorie s r.s. axiomatikou je ekvivalentní teorii s rekurzivní axiomatikou.*

Důkaz neuvádíme. □

Některá výše uvedená tvrzení platí tedy i s předpokladem r.s. axiomatizovatelnosti místo rekurzivní axiomatizovatelnosti.

Silná nerozhodnutelnost.

B.2.11. **Silně nerozhodnutelná struktura. Definovatelná struktura.**

1. Struktura $\mathcal{A}$ v rekurzivním jazyce je *silně nerozhodnutelná*, je-li nerozhodnutelná každá teorie, která ji má za model.

2. Buď $\mathcal{A}$ struktura pro jazyk konečné signatury. Struktura $\mathcal{A}$ je *definovatelná* ve struktuře $\mathcal{B}$, jestliže A je podmnožina B definovaná bez parametrů v $\mathcal{B}$ a každá relace nebo funkce z $\mathcal{A}$ je restrikcí na A nějaké relace nebo funkce definované bez parametrů v $\mathcal{B}$.

TVRZENÍ B.2.12. (O silně nerozhodnutelné struktuře.) *Je-li $\mathcal{A}$ silně nerozhodnutelná struktura definovatelná ve struktuře $\mathcal{B}$ pro jazyk konečné signatury, je $\mathcal{B}$ silně nerozhodnutelná struktura.*

Důkaz neuvádíme, není však obtížný. □

Příklady rekurzivních kompletací a silně nerozhodnutelných struktur.

PŘÍKLADY B.2.13. Následující teorie mají rekurzivní kompletaci:

1. Teorie čisté rovnosti PE, teorie hustého lineárního uspořádání DeLO*.

Důkaz. Rekurzivní kompletace PE je relace $R \subseteq \mathbb{N}^2$, kde pro $0 < n \in \mathbb{N}$ je $R[n]$ je jednoduchá extenze PE o jediný axiom „existuje právě n prvků“ a $R[0]$ je jednoduchá extenze PE o schema „existuje nekonečně prvků“. Teorie DeLO* má 4 jednoduché kompletní extenze a každá je jasně rekurzivně axiomatizovaná. □

2. Teorie algebraicky uzavřených těles ACF.

Důkaz. Komplet $\mathcal{K}$ teorie ACF je tvořen právě teoriemi ACF$_p$, kde p je prvočíslo nebo 0. Každé algebraicky uzavřené těleso je totiž i) nekonečné, ii) některé takové charakteristiky p, iii) každá teorie ACF$_p$ je kategorická v každé nespočetné kardinalitě a tudíž kompletní. Zřejmě lze $\mathcal{K}$ rekurzivně prezentovat. □

3. Teorie Booleových algeber BA. *Důkaz* neuvádíme.

PŘÍKLADY B.2.14. Struktury, které nejsou silně nerozhodnutelné.

1. Struktura $\langle A \rangle$ (s $A \neq \emptyset$) není silně nerozhodnutelná, neboť je modelem rozhodnutelné teorie čisté rovnosti.

2. Husté lineární uspořádání není silně nerozhodnutelná struktura, neboť je modelem rozhodnutelné teorie DeLO*.

3. Abelova grupa není silně nerozhodnutelná, neboť teorie Abelových grup je rozhodnutelná. Důkaz rozhodnutelnosti teorie Abelových grup neuvádíme; je dosti komplikovaný.

PŘÍKLADY B.2.15. Některé silně nerozhodnutelné struktury a nerozhodnutelné teorie.

1. $\underline{\mathbb{N}} = \langle \mathbb{N}, \mathrm{S}, +, \cdot, 0, \leq \rangle$ je silně nerozhodnutelná struktura.

Důkaz. Když $\underline{\mathbb{N}} \models T$, tak $T \cup \mathrm{Q}$ je bezesporná extenze Q a tedy je nerozhodnutelná; je to i jednoduchá extenze T o konečně axiomů, tudíž je T nerozhodnutelná dle kriteria nerozhodnutelnosti.

2. $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, -, \cdot, 0, 1 \rangle$ je silně nerozhodnutelná struktura.

Důsledek: Teorie okruhů, komutativních okruhů a oborů integrity jsou nerozhodnutelné.

Důkaz. $\mathbb{N}$ je definované v $\underline{\mathbb{Z}}$ formulí $(\exists x_1, x_2, x_3, x_4)(x = x_1x_1 + x_2x_2 + x_3x_3 + x_4x_4)$ dle Lagrangeovy věty, tedy struktura $\underline{\mathbb{N}}$ je definovatelná v $\underline{\mathbb{Z}}$, tudíž je $\underline{\mathbb{Z}}$ silně nerozhodnutelná dle věty o silně nerozhodnutelné struktuře.

3. $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, -, \cdot, 0, 1 \rangle$ je silně nerozhodnutelná struktura.

Důsledek: Teorie těles a teorie těles charakteristiky 0 jsou nerozhodnutelné.

Důkaz. Dle výsledku J. Robinsonové je $\mathbb{Z}$ definovatelné v $\underline{\mathbb{Q}}$. Tudíž $\underline{\mathbb{Z}}$ je definovantelné v $\underline{\mathbb{Q}}$ a je tedy $\underline{\mathbb{Q}}$ silně nerozhodnutelná struktura.

B.2.16. Tabulka B.1 uvádí některé teorie či jazyky s rovností se silně nerozhodnutelným modelem. Struktura $\langle \mathrm{Perm}(\mathbb{Z}), \cdot, \mathrm{Id} \rangle$ je silně nerozhodnutelná nekomutativní grupa, přičemž $\mathrm{Perm}(\mathbb{Z})$ je množina všech bijekcí $\mathbb{Z}$. Žádná Abelova grupa není silně nerozhodnutelná, neboť teorie Abelových grup je rozhodnutelná. Další podrobnosti neuvádíme.

Teorie se silně nerozh. modelem
Teorie grup
Teorie obyčejných grafů
Teorie svazů, teorie uspořádání

Jazyk se silně nerozh. modelem	
$\langle R \rangle$,	R kvaternární relace
$\langle R \rangle$,	R binární relace
$\langle F, G \rangle$,	F, G unární funkce

Tabulka B.1: Teorie a jazyky se silně nerozhodnutelným modelem.

B.2.17. V tabulce B.2 plyne kompletnost DiLO pomocí extenze DiLO$^\circ$ o predikce $x <_n y$ s $n \in \mathbb{N}$, značící $x \leq y$ & „mezi x a y je právě n prvků“; DiLO$^\circ$ má eliminaci kvantifikátorů a prvomodel. Kompletnost DeLO plyne z ω-kategoričnosti. Kompletnost SC$_0$ plyne díky kategoričnosti v každé nespočetné kardinalitě a užitím kategorického kriteria kompletnosti. Kompletnost Pr a RCF plyne podobnými postupy jako v případě DiLO, důkaz je však výrazně náročnější; detaily neuvádíme. Kompletnost ACF_0 plyne z kategoričnosti v každé nespočetné kardinalitě; detaily neuvádíme. Uvedená neexistence rekurzivních axiomatik pro $\mathrm{Th}(\mathcal{A})$ plyne ze silné nerozhodnutelnosti struktur $\mathcal{A}$; klíčem je silná nerozhodnutelnost $\mathbf{N}$ a její definovatelnost v ostatních dvou. Nearitmetičnost Th_T plyne z nearitmetitmetičnosti Th_T pro $T = \mathrm{Th}(\mathbf{N})$ (užitím nedefinovatelnosti pravdy); detaily neuvádíme.

$\mathcal{A}$	Rekurzivní axiomatika T ekvivalentní s $\mathrm{Th}(\mathcal{A})$	Th_T
$\langle \mathbb{Z}, \leq \rangle$	DiLO	rekurzivní
$\langle \mathbb{Q}, \leq \rangle$	DeLO	rekurzivní
$\langle \mathbb{N}, \mathrm{S}, 0 \rangle$	SC_0	rekurzivní
$\langle \mathbb{N}, \mathrm{S}, +, 0 \rangle$	Pr	rekurzivní
$\langle \mathbb{N}, \mathrm{S}, +, \cdot, 0, \leq \rangle$	neexistuje	nearitmetická
$\langle \mathbb{Z}, +, -, \cdot, 0, 1 \rangle$	neexistuje	nearitmetická
$\langle \mathbb{Q}, +, -, \cdot, 0, 1 \rangle$	neexistuje	nearitmetická
$\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$	RCF	rekurzivní
$\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$	ACF_0	rekurzivní

Tabulka B.2: Rekurzivní axiomatika teorie $T = \mathrm{Th}(\mathcal{A})$ a složitost Th_T.

První Gödelova věta.

VĚTA B.2.18.

1) (Diagonální lemma.) *Buď T rozšíření teorie* Q. *Pak pro formuli $\varphi(v_0)$ teorie T existuje její sentence φ^* tak, že $T \vdash \varphi^* \leftrightarrow \varphi(\underline{\varphi^*})$.*
2) *V bezesporném rozšíření T teorie* Q *neexistuje definice pravdy.*

   Přitom formule $\tau(x)$ teorie T je definice pravdy v T, *jestliže pro každou sentenci φ teorie T platí $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.*
3) $\mathrm{Th}(\mathbf{N})$ *není aritmetická množina.*

Důkaz. 1) Existuje formule $\psi(v_0)$ tak, že $T \vdash \psi(\underline{\chi}) \leftrightarrow \varphi(\underline{\chi(\underline{\chi})})$ platí pro každou $L(T)$-formuli $\chi(v_0)$. Stačí pak vzít $\psi(\underline{\psi})$ za φ^*. Najdeme ψ. Funkce $D(x) = \mathrm{Sub}(x, \mathrm{Vr}(0), \mathrm{Num}(x))$ je Δ_1; buď $\delta(v_0, v_1)$ nějaká Σ_1-formule reprezentující D v Q; pak je $\mathrm{Q} \vdash (\forall v_1)(\delta(\underline{\chi}, v_1) \leftrightarrow v_1 = \underline{\chi(\underline{\chi})})$ pro každou L(T)-formuli $\chi(v_0)$. Hledané ψ je formule $(\exists v_1)(\delta(v_0, v_1) \mathbin{\&} \varphi(v_1))$.

2) Je-li $\tau(x)$ formule teorie T, existuje dle diagonálního lemmatu sentence φ s $T \vdash \varphi \leftrightarrow \neg\tau(\underline{\varphi})$; tedy τ nemůže být definicí pravdy v T.

3) Buď $T = \mathrm{Th}(\mathbf{N})$. Dále sporem: nechť $\tau(x)$ definuje $\mathrm{Th}(\mathbf{N})$. Pak je to definice pravdy v T, neboť pro sentenci φ jazyka aritmetiky máme $T \vdash \varphi \Leftrightarrow \varphi \in T \Leftrightarrow \mathbf{N} \models \tau(\underline{\varphi}) \Leftrightarrow \tau(\underline{\varphi}) \in T$, tj. $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$ – spor s 2). □

VĚTA B.2.19. (První Gödelova věta.) *Buď T bezesporné rekurzivně axiomatizované rozšíření* Q. *Pak existuje Π_1-sentence pravdivá v $\mathbf{N}$ a nedokazatelná v T.*

Podrobněji: Nechť Σ_1-formule $\Theta(x, y)$ definuje Prf_T *a ν je dle diagonálního lemmatu sentence, pro níž je $\mathrm{Q} \vdash \nu \leftrightarrow \neg(\exists y)\Theta(\underline{\nu}, y)$. Pak $T \nvdash \nu$, $\mathbf{N} \models \nu$ a ν je Π_1-formule v* Q. *Když navíc každá Σ_1-sentence dokazatelná v T platí v $\mathbf{N}$ (speciálně, když $\mathbf{N} \models T$), je ν nezávislá sentence teorie T.*

Důkaz. Nechť $T \vdash \nu$. Pak $\mathrm{Prf}_T(\nu, d)$ pro nějaké $d \in \mathbb{N}$. Tedy $\mathrm{Q} \vdash (\exists y)\Theta(\underline{\nu}, y)$; to plyne z tvrzení o Σ_1-kompletnosti Robinsonovy aritmetiky Q: pro Σ_1-formuli $\varphi(x_1, \dots, x_k)$ a $m_1, \dots, m_k$ z $\mathbb{N}$ je $\mathrm{Q} \vdash \varphi(\underline{m}_1, \dots, \underline{m}_k) \Leftrightarrow \mathbf{N} \models \varphi[m_1, \dots, m_k]$. Z definice ν máme $T \vdash \neg(\exists y)\Theta(\underline{\nu}, y)$ – spor. Dokážeme $\mathbf{N} \models \nu$. Nechť $\mathbf{N} \models \neg\nu$. Pak $\mathbf{N} \models \Theta(\underline{\nu}, \underline{d})$ pro nějaké $d \in \mathbb{N}$ a tedy $\mathrm{Prf}_T(\nu, d)$, tj. $T \vdash \nu$, což je ve sporu s již dokázaným. □

Literatura

[1] Chang, C.C., Keisler, H.J., Model theory, NHPC, 1973

[2] Hájek, P., Pudlák, P., Metamathematics of First-Order Arithmetic, Springer, 1998

[3] Hodges, W., Model Theory, Cambridge University Press, 1993

[4] Shelah S., Classification Theory, NHPC, 1990

[5] Shoenfield, J.R., Mathematical Logic, A. K. Peters, 2001

[6] Sochor, A., Klasická matematická logika, UK v Praze – Karolinum, 2001

[7] Švejdar, V., Logika neúplnost, složitost a nutnost, Academia, 2002

Rejstřík

$B\restriction a$, 13
$\underline{\mathrm{AV}}(T)$, 49
$\mathsf{Aut}(\mathcal{A})$, 37
BS, 111
$\mathrm{CA}(\mathbb{P})$, 65
$\Upsilon^{A}_{n,i}$, 36
Fm_L, 21
$\underline{\mathbb{K}}^m_n$, 52
$\mathrm{Kn}(T)$, 42
$\mathsf{M}(L)$, 25
$\mathsf{M}_\kappa(T)$, 29
$\mathsf{M}(T)$, 29
$\underline{\mathbb{J}}_n$, 52
$\mathbb{P}_L$, 31
SC, 52
SC_0, 52
$\mathrm{Th}(T)$, 24
$\mathrm{Th}(\mathcal{A})$, 34
Th_T, 24
$\mathrm{Thm}(T)$, 24
Thm_T, 24
$\mathrm{Tr}(T)$, 29
$\mathrm{Tru}(T)$, 29
$\underline{\mathcal{P}}(I)$, 11
$\approx_T$, 48
$\|L\|$, 20
$\|\mathcal{A}\|$, 25
$|x|$, 9
$\kappa(\diamond)$, $\kappa(\diamond, \infty)$, 9
$\underline{\mathbb{O}}^m_I$, 57
Δ_n, 99, 110
$\Delta^e(\mathcal{A})$, 86
$\mathcal{F}\langle X\rangle$, 8
$\perp$, 27, 61
$\mathrm{b}[\Gamma]$, 42
Fm^n_L, 22
$\mathcal{A}\langle X\rangle$, 26
$\rightarrow$, 20
$\mathrm{I}(\kappa, T)$, 38
κ_L, 25
$\mathrm{l}(\overline{x})$, 7
$\neg$, 20
$\models$
    $L \models$, 29
    $T \models$, 29
$\mathrm{nTr}(T)$, 29
Π_n, 99, 110
Σ_n, 99, 110
$\mathcal{A}' \mid L$, 26
$\mathcal{A} \prec \mathcal{B}$, 39
$\mathcal{A}\restriction Y$, 26
$\mathcal{B} \subseteq \mathcal{A}$, 25
$\top$, 27, 61
$\underline{\mathsf{Aut}}(\mathcal{A})$, 37
$\mathrm{var}(\varphi)$, 61
$h[\mathcal{A}]$, 37
JKE, 83
JKE, 41

homomorfní obraz struktury, 37

algebra
    booleovských funkcí, 65
    Cantorova nad $\mathbb{P}$, 65
    Lindenbaumova, 49
    modelů výroků teorie, 64
    výroků, 49
algoritmický překlad, 113
algoritmus
    CNF-, 64
antecedent, 21
aritmetika
    Peanova, 53
    Presburgerova, 53
    Robinsonova, 53
automorfizmus, 37
axiom
    $\forall$-zavedení, 24
    diskrétnosti, 54
    hustoty, 54
    substituce, 24
axiomatika, 24
axiomy
    logické, 24
    mimologické, 24

Booleova algebra, 10

booleovská kombinace, 42

definice pravdy, 116
definovat
  indukcí, 22
designátor, 21
designátor
  -ů struktura, 51
diagram
  elementární, 86
disjunkce, 22
disjunkt, 22
dokazovat
  indukcí, 22
důkaz, 24

ekvivalence, 22
ekvivalentní
  sémanticky, 48
elementární
  konjunkce, 43
  podstruktura, 39
  vnoření, 39
eliminace kvantifikátorů, 42
eliminace kvantifikátorů
  sémanticky, 42
epimorfizmus, 37
expanze, 26
extenze
  jednoduchá, 25
  konzervativní, 25
  o jména prvků, 28
  teorie, 25

faktorelace, 48
faktorfunkce, 48
faktorprojekce, 48
faktorstruktura, 48
formule, 21
formule
  $\triangle_L$- jazyka L, 80
  $\forall_{0,L}$-, 80
  $\forall_{n,L}$-, 80
  $\exists_{0,L}$-, 80
  $\exists_{n,L}$-, 80
  Σ_n,Π_n,Δ_n, 99, 110
  (právě) v proměnných, 22
  atomická, 20
  bezkvantifikátorová, 21
  dokazatelná, 24
  existenční, 80
  je lživá (v teorii), 29
  je pravdivá (v teorii), 29
  je pravdivá ve struktuře, 27
  je splněná, 27
  konzistentní, 24
  nevnořená atomická, 21
  nezávislá, 24
  omezená, 99, 110
  otevřená, 21
  platí, 27
  silnější, 24
  sémanticky konzistentní, 29
  sémanticky nezávislá, 29
  univerzální, 80
  varianta, 23
  vyvratitelná, 24
funkce
  booleovská, 65

generalizace, 24
generátory
  podstruktury, 26
grupa automorfizmů, 37

hodnocení ve struktuře, 26
hodnota
  designátoru, 51
  formule, 27
  termu, 26
homomorfizmus, 37
homomorfizmus
  striktní, 37

individuální konstanta, 29
induktivní definice, 8
instance, 23
izomorfizmus, 37
izomorfní vnoření, 37

jazyk, 20
jazyk
  extenze, 20
  kardinalita, 20
  nerozhodnutelný, 112
  numerický, 109
  s rovností, 20

kardinalita
  struktury, 25
klauzule, 61
komplet
  modelů, 42
  teorie, 42
kongruence, 47
konjunkce, 22
konjunkce
  elementární, 43
konjunkt, 22

- konsekvent, 21
- kvantifikátor
  - existenční, 22

- literál, 20, 61
- logické spojky
  - implikace, 20
  - negace, 20

- množina
  - Σ_n,Π_n,Δ_n, 99, 110
  - aritmetická, 100, 110
  - henkinovských konstant, 84
- množinová reprezentace, 64
- množinová reprezentace teorie, 73
- mocnina
  - Booleovy algebry, 11
- model
  - jazyka, 25
  - standardní aritmetiky, 53
  - teorie, 29
  - výrokového jazyka, 31
- modus ponens, 24
- monomorfizmus, 37

- notace, 21, 50
- notace
  - obecná, 20, 50

- oddělující klauzule, 69
- odvození
  - $\mathcal{F}$-, 8
- ohodnocení
  - proměnných, 26
  - proměnných parciální, 28

- poddesignátor, 21
- podformule, 21
- podstruktura, 25
- podstruktura
  - generovaná, 26
- pomocí reprezentantů, 48
- pravdivostní ohodnocení
  - prvovýroků, 31
- pravidla
  - dedukce, 24
- prenexní
  - operace, 79
  - tvar, 79
- produkt
  - algeber, 11
- projekce, 11
- proměnná
  - [ne]kvantifikovaná ve formuli, 22
  - patří formuli, 22
- proměnné
  - parametrické, 22
  - předmětné, 22
- překlad
  - dS, do T, 90

- r.s., 110
- redukce, 26
- redukt, 26
- rekurzivně spočetná, 110
- rekurzivní
  - funkce, 110
  - kompletace, 112
  - množina, relace, 110
- relativizace
  - Booleovy algebry, 13
- reprezentace
  - množinová formulí, 64
- reprezentovaná
  - funkce, relace, v teorii, 113
- rezoluční
  - operace, 73
  - uzávěr, 73
- rezoluční strom, 74
- rezolventa, 73

- signatura, 20
- spektrum
  - izomorfní teorie, 38
- spor, 24
- struktura
  - L-, pro L, 25
  - L-, triviální velikosti κ, 25
  - $\underline{\mathbb{K}}^m_n$, 52
  - $\underline{\mathbb{J}}_n$, 52
  - definovatelná, 114
  - designátorů, 51
  - formulí, 30
  - kanonická, 83, 84
  - konstantní, 83
  - silně nerozhodnutelná, 114
  - výrazů, 51
  - výroků, 61
- struktury
  - elementárně ekvivalentní, 34
- substituce
  - termu do formule, 23
- symboly
  - funkční, 20
  - mimologické, 20
  - relační, 20
- sémanticky
  - ekvivalentní teorie, 32
  - extenze teorie, 32

jednoduchá extenze, 32
kompletní teorie, 32
konzervativní extenze, 32
sporná teorie, 32
teorie axiomatizovatelná, 32

Tarski-Vaughtův test, 40
tautologie, 31
teorie, 24
teorie
DiLO, 54
$\mathbb{P}$-, 31
κ-kategorická, 38
f-homogenní, 43
bezesporná, 25
Booleových algeber, 53
ekvivalentní, 25
grafů, 54
grup, 55
henkinovská, 84
konečně axiomatizovatelná, 24, 25
modelově kompletní, 40
modulů, 56
nad $\mathbb{P}$, 31
nerozhodnutelná, 112
numerická, 109
náhodného grafu, 54
oborů integrity, 55
okruhů, 55
otevřená, 24
otevřeně axiomatizovatelná, 25
prázdná, 24
rozhodnutelná, 112
splnitelná, 31
sporná, 25
struktury, 34
těles, 56
uspořádání, 54
vektorových prostorů, 57
čisté rovnosti, PE, 25
část, 24
teorém, 24
term, 20
term
nevnořený, 21
substituovatelný, 23
těleso
archimedovské, 56
třída
obojetná, 69
otevřená, 69
uzavřená, 69

univerzum
struktury, 25
uzávěr
(generální) $\sim$ formule, 22
uzávěr X
$\mathcal{F}$-, 8

varianta formule, 23
výrok
splntelný, 31
výskyt, 21
výskyt
termu, 21