Kapitola 1

Úvod

Stručný obsah kapitoly.

- Induktivní definice a důkaz indukcí. $\mathcal{F}$-uzávěr a $\mathcal{F}$-odvození.
- Notace a signatury, struktury pro signaturu.
- Obor designátorů $\underline{\mathrm{D}}(\mathcal{S})$; tvrzení o jednoznačnosti, o výskytech, o substituci.
- Hodnota designátoru ve struktuře. Konstrukce rekurzí.

1.1 Základní pojmy

1.1.1. Sekvence. n-ární funkce a relace.

Sekvence je konečná posloupnost; predikát $\mathrm{Seq}(x)$ nechť značí „x je sekvence“. Sekvenci lze v teorii množin případně v nějakém jejím fragmentu definovat takto:

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

Základní pojmy o sekvencích 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

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

Místo $(x)_y$ se píše také, nevede-li to k nedorozumění, symbol

$$x_y.$$

Místo sekvence délky n můžeme říkat n-sekvece. n-sekvenci x značíme jako

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

kde $x_i = (x)_i$. Značíme ji též $\overline{x}$; pruh graficky zdůrazňuje, že jde o sekvenci.

V teorii množin se definují n-tice (uspořádané) tak, že uspořádaná dvojice (x, y) je $\{\{x\}, \{x, y\}\}$ a $(n+1)$-tice s $n \geq 2$ jsou právě tvaru (u, y), kde u je nějaká n-tice. Dále 0-tice je jen $\emptyset$, 1-tice jsou právě tvaru $\{x\}$. (Metodicky se nejprve zavede pojem uspořádané dvojice, pomocí něj pojem relace a funkce a pomocí funkcí a pojmu přirozeného čísla pak sekvence jako v (1.1).)

Je vzájemně jednoznačná korespondence $'$ (funkce) mezi všemi sekvencemi a ticemi taková, že $\emptyset' = \emptyset$ a $\langle x \rangle' = \{x\}$ a pro $n \geq 2$ a $(n+1)$-sekvenci s tvaru $t \smile \langle y \rangle$ je $s' = (t', y)$. Pomocí $'$ n-sekvence a n-tice přirozeně ztotožňujeme.

Symbol z^n značí množinu všech n-tic s členy v z; můžeme díky ztotožnění n-sekvencí a n-tic psát místo z^n také ${}^n z$, neboť, symbol ${}^x y$ značí množinu všech funkcí z x do y. Často se ztotožňuje z^1 se z. Je dále $z^0 = \{\emptyset\}\,(= {}^0 z)$. Množinu všech sekvencí s hodnotami v z značíme z^*; tedy $z^* = \bigcup_{n \in \mathbb{N}} z^n$.

Symbol $f : x \to y$ značí, že f je funkce s definičním oborem $\mathrm{dom}(f) = x$ a oborem hodnot $\mathrm{rng}(f) \subseteq y$; je to funkce z x do y. Pro $a \in \mathrm{dom}(f)$ je $f(a)$ hodnota f v a. Pro $n \geq 1$ o funkci f resp. relaci r říkáme, že je n-ární, je-li dom(f) množina n-tic resp. r je množina n-tic. Když f je n-ární a $\langle a_0, \dots, a_{n-1}\rangle \in$ dom(f), píšeme $f(a_0, \dots, a_{n-1})$ místo $f(\langle a_0, \dots, a_{n-1}\rangle)$. Když r je n-ární, píšeme také $r(x_0, \dots, x_{n-1})$ místo $\langle x_0, \dots, x_{n-1}\rangle \in r$. Funkce f je nulární, když dom$(f) = \{\emptyset\}$. Funkce $f : x^n \to x$ je n-ární operace (též funkce) na x. Množina $r \subseteq x^n$ s $n > 0$ je n-ární relace na (též v) x. Pro funkce f, g je $fg = \{\langle x, f(g(x))\rangle;\ x \in \mathrm{dom}(g), g(x) \in \mathrm{dom}(f)\}$.

$x \times y = \{(a, b);\ a \in x, b \in y\}$ je kartézský součin x a y. Díky ztotožnění n-sekvencí a n-tic můžeme psát $x \times y = \{\langle a, b\rangle;\ a \in x, b \in y\}$ a $z^n \times y = \{s\smile b;\ s \in z^n, b \in y\}$.

Induktivní definice

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

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

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

$\mathcal{F}$-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 $\langle x_1, \dots, x_n\rangle \in X^n \cap \mathrm{dom}(F)$, $F \in \mathcal{F}$.

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 je seznam pravidel

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

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 z $\mathcal{F}\langle X\rangle$ prokazující, že každý prvek z $\mathcal{F}\langle X\rangle$ má vlastnost V, je schema

- každý prvek z X má vlastnost V,
- když každé $y_1, \dots, y_n$ z $\mathcal{F}\langle X\rangle$ má 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*, „každé $y_1, \dots, y_n$ má vlastnost V, jakmile $\langle y_1, \dots, y_n\rangle \in \mathrm{dom}(F)$“ je *indukční předpoklad* indukčního kroku 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) lze vynechat prvý řádek a ve druhém psát $\mathcal{F}'$ místo $\mathcal{F}$. Obdobně je tomu v (1.3).

TVRZENÍ 1.1.3. *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) $\mathcal{F}\langle X\rangle = \{y;\ y$ *je* $\mathcal{F}$*-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 je $\mathcal{F}$-odvození z X prvku z_i pro $i = 1, \ldots n$. Pak $s_1 \smile \cdots \smile s_n \smile y$ 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 $\mathcal{F}\langle X\rangle$. $\square$

1.2 Signatury a struktury

1.2.1. Notace a signatura.

1. *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* $\underline{\mathcal{S}}$. Když $Ar_\mathcal{S}(S) = 0$, říkáme, že S je *konstantní symbol*; značíme jej často písmenem c, c', c_i d, d', d_i apod. Obecná notace $\underline{\emptyset}$ se nazývá *prázdná*; ztotožňujeme ji s $\emptyset$.

Notace je obecná notace $\underline{\mathcal{S}}$, obsahující alespoň jeden konstantní symbol; tedy $0 \in Ar_\mathcal{S}[\mathcal{S}]$.

2. *Signatura* je $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$, kde $\underline{\mathcal{R}}$ je obecná notace s $0 \notin Ar_\mathcal{R}[\mathcal{R}]$, $\underline{\mathcal{F}}$ je obecná notace a $\mathcal{R} \cap \mathcal{F} = \emptyset$. Jsou-li $\underline{\mathcal{R}}$, $\underline{\mathcal{F}}$ prázdné, je to *prázdná signatura*; ztotožňujeme ji s $\emptyset$. Prvky z $\mathcal{R}$ resp. $\mathcal{F}$ jsou *relační* resp. *funkční symboly* uvažované signatury. Je-li symbol $=$ v $\mathcal{R}$, značí binární predikátový symbol rovnosti. Signatura $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$ je *relační* resp. *funkční*, když $\underline{\mathcal{F}}$ je prázdná resp. $\underline{\mathcal{R}}$ je prázdná; zapisujeme ji jako $\underline{\mathcal{R}}$ resp. $\underline{\mathcal{F}}$. Notaci chápeme jako funkční signaturu.

Je-li $\langle \mathcal{S}, Ar_\mathcal{S}\rangle$ obecná notace a $\mathcal{S} = \{S_0, \ldots, S_{m-1}\}$, zapisujeme ji také jako

$$\langle S_0, \ldots, S_{m-1}\rangle, \qquad S_0 \text{ je } k_0\text{-ární}, \ldots, S_{m-1} \text{ je } k_{m-1}\text{-ární},$$

kde $k_i = Ar_\mathcal{S}(S_i)$. Je-li $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$ signatura, $\mathcal{R} = \{R_0, \ldots, R_{m-1}\}$, $\mathcal{F} = \{R_0, \ldots, R_{n-1}\}$, zapisujeme ji jako

$$\langle R_0, \ldots, R_{m-1}, F_0, \ldots, F_{n-1}\rangle,$$

R_0 je k_0-ární, $\ldots$, R_{m-1} je k_{m-1}-ární, F_0 je l_0-ární, $\ldots$, F_{m-1} je l_{m-1}-ární,

kde $k_i = Ar_\mathcal{R}(R_i)$, $l_j = Ar_\mathcal{F}(F_j)$.

Jsou-li četnosti patrné z kontextu, nemusíme je uvádět.

1.2.2. Struktura, podstruktura a generovaná podstruktura.

1. *Struktura* je trojice $\mathcal{A} = \langle A, \mathcal{R}, \mathcal{F}\rangle$, kde A je neprázdná množina, $\mathcal{R}$ je soubor relací na A konečných kladných četností, $\mathcal{F}$ je soubor operací na A konečných četností. Říkáme také, že prvky z $\mathcal{R}$ resp. $\mathcal{F}$ jsou *relace* resp. *funkce (z)* $\mathcal{A}$. Nulární funkce struktury $\mathcal{A}$ se nazývá *konstanta*; je tvaru $\{\langle\emptyset, c\rangle\}$ s jistým $c \in A$; ztotožňujeme ji s c. Dále říkáme, že A je *univerzum* $\mathcal{A}$. Struktura $\mathcal{A}$ je *čistě relační* resp. *funkční* (též *algebraická*), je-li $\mathcal{F} = \emptyset$ resp. $\mathcal{R} = \emptyset$. Někdy píšeme $\underline{A}$ místo $\mathcal{A}$. Je-li $\mathcal{R}$ tvaru $\langle R_0, \ldots, R_{k-1}\rangle$ a $\mathcal{F}$ tvaru $\langle F_0, \ldots, F_{l-1}\rangle$, zapisujeme $\mathcal{A}$ též jako

$$\langle A, R_0, \ldots, R_{k-1}, F_0, \ldots, F_{l-1}\rangle.$$

Velikost čili *kardinalita* $\mathcal{A}$ je velikost (kardinalita) jejího univerza; značíme ji

$$\|\mathcal{A}\|.$$

2. *Podstruktura* struktury $\mathcal{A}$ je struktura $\mathcal{B} = \langle B, \mathcal{R}', \mathcal{F}'\rangle$, kde:

a) $B \subseteq A$.

b) Relace z $\mathcal{R}'$ jsou právě tvaru $R \cap B^m$ s $R \in \mathcal{R}$ a m rovným četnosti R.

c) Funkce z $\mathcal{F}'$ je právě tvaru $F \cap (B^n \times B)$ s $F \in \mathcal{F}$ a n rovným četnosti F.

Speciálně je B uzavřeno na všechny funkce struktury $\mathcal{A}$ a tedy také každá konstanta struktury $\mathcal{A}$ patří do B.

3. Buď navíc $X \subseteq A$. *Množina generovaná v* $\mathcal{A}$ *z* X je nejmenší podmnožina A obsahující X a uzavřená na každou funkci z $\mathcal{F}$; značíme ji $\overline{X}^\mathcal{A}$. Je-li $\overline{X}^\mathcal{A} \neq \emptyset$, je to

univerzum nejmenší podstruktury struktury $\mathcal{A}$; značíme ji $\mathcal{A}\langle X\rangle$ a říkáme, že to je *podstruktura generovaná* X.

Když $\mathcal{F}$ obsahuje konstantu c, je $c \in \overline{X}^{\mathcal{A}}$. Když $\mathcal{F} = \emptyset$, tak $\overline{X}^{\mathcal{A}} = X$.

1.2.3. Realizace signatury.

Realizace signatury $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$ je struktura $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A\rangle$, kde:

$$\begin{array}{ll} \mathcal{R}^A = \langle R'_R;\ R \in \mathcal{R}\rangle; & R'_R \subseteq A^{Ar(R)} \text{ je } \textit{realizace } R \text{ v } \mathcal{A} \text{ a značíme ji } R^A. \\ & \text{Přitom } =^A \text{ je } \{\langle a, a\rangle;\ a \in A\}, \text{ tj. identita na } A. \\ \mathcal{F}^A = \langle F'_F;\ F \in \mathcal{F}\rangle; & F'_F : A^{Ar(F)} \to A \text{ je } \textit{realizace } F \text{ v } \mathcal{A} \text{ a značíme ji } F^A. \end{array}$$

Říkáme také, že $\mathcal{A}$ je $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$*-struktura*, též *struktura pro* $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$ a také, že to je (*sémantická*) *interpretace* uvažované signatury. $'$ je formálně zobrazení $\mathcal{R}$ na $\mathcal{R}^A$ a $\mathcal{F}$ na $\mathcal{F}^A$.

1.2.4. Izomorfizmus struktur.

Buďte $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A\rangle$, $\mathcal{B} = \langle B, \mathcal{R}^B, \mathcal{F}^B\rangle$ dvě $\langle \underline{\mathcal{R}}, \underline{\mathcal{F}}\rangle$-struktury. Zobrazení $h : A \to B$ je *izomorfizmus* struktur $\mathcal{A}$, $\mathcal{B}$, když

- h je prosté a na B,
- pro $R \in \mathcal{R}$, n rovno četnosti R a $\langle a_1, \ldots, a_n\rangle \in A^n$ je
$$R^A(a_1, \ldots, a_n) \Leftrightarrow R^B(h(a_1), \ldots, h(a_n)) \ ,$$
- pro $F \in \mathcal{F}$, n rovno četnosti F a $\langle a_1, \ldots, a_n\rangle \in A^n$ je
$$h(F^A(a_1, \ldots, a_n)) = F^B(h(a_1), \ldots, h(a_n)).$$

Píšeme pak $\mathcal{A} \cong \mathcal{B}$ (*via* h). Speciálně pro konstantní symbol c z $\mathcal{F}$ je $h(c^A) = c^B$.

1.3 Designátory

1.3.1. Aplikace notace.

Buď $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$ obecná notace, X množina konečných sekvencí.

1. *Aplikační doména* $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$ *na* X je množina $Ad(\mathcal{S}, X) = \bigcup_{S\in\mathcal{S}}(\{S\}\times X^{Ar_{\mathcal{S}}(S)})$. Její prvky jsou tedy právě tvaru $\langle S, s\rangle$, kde $S \in \mathcal{S}$, $s \in X^{Ar_{\mathcal{S}}(S)}$.

2. *Aplikace* $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$ *na* X je funkce $Ap_{\mathcal{S},X}$ definovaná na $Ad(\mathcal{S}, X)$ taková, že pro každé $S \in \mathcal{S}$ a $s \in X^{Ar_{\mathcal{S}}(S)}$ je

$$Ap_{\mathcal{S},X}(S, s) = \langle S\rangle \smile \sqcup (s). \tag{1.4}$$

Její obor hodnot se nazývá *množina výrazů aplikace* $Ap_{\mathcal{S},X}$ *na* X. Pro $s \in X^{Ar_{\mathcal{S}}(S)}$ tvaru $\langle s_0, \ldots, s_{n-1}\rangle$ značíme $Ap_{\mathcal{S},X}(S, s)$ jako

$$S(s_0, \ldots, s_{n-1}) \ \text{ nebo také } \ (s_0 S s_1), \text{ když } n = 2. \tag{1.5}$$

Prvý výraz v (1.5) je *prefixní* a druhý *infixní* zápis výrazu $Ap_{\mathcal{S},X}$.

Pro nulární S platí $Ap_{\mathcal{S},X}(S, \emptyset) = \langle S\rangle = S()$; místo $S()$ píšeme často jen S, nevede-li to k nedorozumění. Když $\mathcal{S}$ je prázdné, je $Ap_{\mathcal{S},X}$ prázdná funkce a obor takové aplikace je prázdný.

3. Je-li $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$ notace, říkáme, že $Ap_{\mathcal{S},\mathcal{S}^*}$ je *aplikace* $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$; značíme ji
$$Ap_{\mathcal{S}}.$$
Platí pak $\operatorname{rng}(Ap_{\mathcal{S}}) \subseteq \mathcal{S}^*$, tj. množina výrazů aplikace $Ap_{\mathcal{S}}$ je podmnožina $\mathcal{S}^*$.

POZNÁMKA. Buď $\mathcal{S} = \{F, F(c), c\}$, F unární, $F(c), c$ konstantní. Pak zkrácení designátoru $F(c)()$ na $F(c)$ vede k nedorozumění, neboť $F(c)$ je $Ap_{\mathcal{S}}(F, \langle c\rangle)$.

1.3.2. Designátory.

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

1. *Obor 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 $\langle S^\circ;\ S \in \mathcal{S}\rangle$ funkcí takových, že

$$S^\circ : (\mathcal{S}^*)^{Ar_{\mathcal{S}}(S)} \to \mathcal{S}^* \text{ splňuje } S^\circ(s) = Ap_{\mathcal{S}}(S, s) \text{ pro } s \in (\mathcal{S}^*)^{Ar_{\mathcal{S}}(S)}. \tag{1.6}$$

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. *Obor designátorů* notace $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$ je podstruktura $\underline{\mathrm{D}}(\mathcal{S})$ struktury $\underline{\mathrm{D}}^*(\mathcal{S})$, generovaná prázdnou množinou; její univerzum $\mathrm{D}(\mathcal{S})$ je *množina designátorů* uvažované signatury. $\mathrm{D}(\mathcal{S})$ je tedy nejmenší podmnožina $\mathcal{S}^*$ obsahující každé $\langle S \rangle$ pro $S \in \mathcal{S}$ nulární, která je uzavřená na všechny S° s $S \in \mathcal{S}$ nenulárním. Speciálně je $\mathrm{D}(\mathcal{S})$ definováno zřejmou induktivní definicí:

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

Připomeme, 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.

Mluvíme-li o designátorech a není výslovně uvedená příslušná notace, chápeme ji jako $\langle \mathcal{S}, Ar_{\mathcal{S}} \rangle$. Designátory často značíme $\eta, \eta', \eta_0, \eta_1, \ldots$.

TVRZENÍ 1.3.3. (O jednoznačnosti designátorů.) *Každý designátor je jednoznačně tvaru $Ap_{\mathcal{S}}(S, s)$ pro jisté $S \in \mathcal{S}$ a jisté $s \in \mathrm{D}(\mathcal{S})^{Ar(S)}$.*

Čili $Ap_{\mathcal{S}}$ je prosté zobrazení množiny $Ad(\mathcal{S}, \mathrm{D}(\mathcal{S}))$ na $\mathrm{D}(\mathcal{S})$.

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 $(s)_i \lessdot (s')_i$ nebo $(s')_i \lessdot (s)_i$. To je ve sporu s 1.3.4. □

LEMMA 1.3.4. *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 $\hat\eta'_1, \ldots, \hat\eta'_k$. Jelikož $\eta_1 \lessdot \eta'_1$, 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 $i = 2, \ldots, n$. Speciální tvrzení plyne bezprostředně. □

TVRZENÍ 1.3.5. (O výskytech designátorů.) *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 1.3.4 je $\eta = \eta'$.

Nechť výskyt symbolu, jenž je první člen uvažovaného výskytu designátoru η', je v některém $(s)_i$. Pak dle 1.3.6 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 1.3.6. *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 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 1.3.7. (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. □

TVRZENÍ 1.3.8. (Konstrukce rekurzí na $\mathrm{D}(\mathcal{S})$.) *Nechť $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$ je notace a U, W množiny. Pro každé $S \in \mathcal{S}$ a $n = Ar_{\mathcal{S}}(S)$ buďte dány funkce $G_S(z_1, \ldots, z_n, u)$ s hodnotami ve W a definovaná pro každé $z_1, \ldots, z_n$ z $\mathcal{P}(W)$, u z U a $G_{S,1}(u), \ldots, G_{S,n}(u)$ s hodnotami v $\mathcal{P}(U)$ a definované pro každé u z U. Pak existuje právě jedna funkce $H : \mathrm{D}(\mathcal{S}) \times U \to W$ vyhovující podmínkám:*

pro $S \in \mathcal{S}$ četnosti n a $\eta_1, \ldots, \eta_n$ z $\mathrm{D}(\mathcal{S})$ je

$$H(\langle S\rangle \smile \eta_1 \smile \ldots \smile \eta_n, u) = G_S(H[\{\eta_1\} \times G_{S,1}(u)], \ldots, H[\{\eta_n\} \times G_{S,n}(u)], u). \tag{1.7}$$

Říkáme, že H z 1.3.8 je *zkonstruována* či *sestrojena rekurzí předpisy (pravidly)* (1.7) *z funkcí* $G_S, G_{S,i}$, $0 < i \leq n$.

POZNÁMKA 1.3.9.

1. Jelikož $\eta \in \mathrm{D}(\mathcal{S})$ je jednoznačně tvaru $\langle S\rangle \smile \eta_1 \smile \ldots \smile \eta_n$, předpisy (1.7) jsou korektní. Rekurentnost definice je dána tím, že $H(\langle S\rangle \smile \eta_1 \smile \ldots \smile \eta_n, u)$ se počítá z množin $H[\{\eta_i\} \times G_{S,i}(u)]$ (a parametru u), tj. pomocí „již známých hodnot“ $H(\eta_i, u')$ (s libovolným $u' \in U$). Pro nulární S máme jen G_S a rovnost z (1.7) má tvar
$$H(\langle S\rangle, u) = G_S(u).$$

2. Důležitým a praktickým speciálním případem rekurzivního předpisu je

$$\begin{aligned} &H(\langle S\rangle \smile \eta_1 \smile \ldots \smile \eta_n, u) = G_S(H(\eta_1, G_{S,1}(u)), \ldots, H(\eta_n, G_{S,n}(u)), u) \\ &\text{s } G_S(w_1, \ldots, w_n, u) \in W \text{ definovaným pro kadždé } w_1, \ldots, w_n \in W,\ u \in U, \\ &G_{s,i}(u) \in U \text{ pro každé } u \in U,\ i = 1, \ldots, n; \end{aligned} \tag{1.8}$$

zde se odvoláváme jen na prvky w z W, nikoli na všechny podmnožiny W jako v (1.7).

Důkaz 1.3.8. Buď
$$D_0 = \{\langle S\rangle;\ S \in \mathcal{S} \text{ je nulární}\},\ D_{m+1} = \{\langle S\rangle \smile \sqcup(s);\ S \in \mathcal{S} \text{ a } s \in D_m^{Ar_{\mathcal{S}}(S)}\}$$
pro $m \in \mathbb{N}$. Snadno se ukáže indukcí, že $D_m \subseteq D_{m+1}$ pro $m \in \mathbb{N}$ a $\mathrm{D}(\mathcal{S}) = \bigcup_{m\in\mathbb{N}} D_m$.

Indukcí podle m plyne, že jsou-li h_m, h'_m definované na $D_m \times U$ a splňují (1.7) s h_m, h'_m místo H pro všechna $S \in \mathcal{S}$, $\eta_i \in D_{m-1}$ a $u \in U$, tak $h_m = h'_m$. Tudíž H je nejvýše jedna. Protože každé h_m lze (jednoznačně) rozšířit na $D_{m+1} \times U$ do h_{m+1}, hledané H je rovno $\bigcup_{m\in\mathbb{N}} h_m$. □

1.3.10. Hodnota designátoru ve struktuře.

Nechť $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$ je notace a $\mathcal{A}$ je $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$-struktura. *Hodnota $H^A(\eta)$* designátoru η z $\mathrm{D}(\mathcal{S})$ v $\mathcal{A}$ je definována rekurzí:

$$\begin{aligned} &\text{Pro } S \in \mathcal{S} \text{ s } n = Ar_{\mathcal{S}}(S) \text{ a } \eta_1, \ldots, \eta_n \text{ z } \mathrm{D}(\mathcal{S}) \text{ je} \\ &H^A(S(\eta_1, \ldots, \eta_n)) = S^A(H^A(\eta_1), \ldots, H^A(\eta_n)). \end{aligned} \tag{1.9}$$

Speciálně když η je $\langle c\rangle$ s konstantním c, je $H^A(\eta) = c^A$.

TVRZENÍ. *Nechť $\langle \mathcal{S}, Ar_{\mathcal{S}}\rangle$ je notace a $\mathcal{A} = \underline{\mathrm{D}}(\mathcal{S})$. Pak pro η z $\mathrm{D}(\mathcal{S})$ je $H^A(\eta) = \eta$.*

Důkaz. Indukcí na designátorech. Nechť $\eta = \langle S\rangle \smile \sqcup(s)$ s n-árním S a s rovným $\langle \eta_1, \ldots, \eta_n\rangle$, přičemž pro $\eta_1, \ldots, \eta_n$ to platí. Pak
$$H^A(\eta) = S^A(\eta_1, \ldots, \eta_n) = S^\circ(\eta_1, \ldots, \eta_n) = \eta.$$
□

Kapitola 2

Výroková logika

Stručný obsah kapitoly.

- Jazyk a formule výrokové logiky.
- Modely, pravdivost v teorii, sémantická ekvivalence. Normální tvary.
- Booleovská pravidla. Nezávislé formule. Vlastnosti $\models$.
- Extenze teorie, ekvivalentní teorie, kompletní teorie.
- Sémantická kompaktnost. Axiomatizovatelnost.
- Dedukce: důkaz, teorém, vyvratitelná formule, (beze)sporná teorie.
- Existence modelu bezesporné teorie. Věta o úplnosti výrokové logiky.
- Syntaktické metody dokazování.
-
-

2.1 Sémantika

Elementární syntax výroků.

2.1.1. Výrokový jazyk, výroky a teorie.

1. *Výrokový jazyk nad* $\mathbb{P}$ tvoří: a) neprázdná množina $\mathbb{P}$ *prvovýroků* (též *výrokových proměnných* či *atomů*), b) logické spojky $\neg, \rightarrow$ (negace, implikace).

Dále používáme pomocně delimitery $($, $)$ k usnadnění čitelnosti designátorů. Prvovýroky značíme p, q, r, p_0, p' apod.

Je-li potřeba, chápeme $\mathbb{P}$ jako prostý indexovaný soubor $\mathbb{P} = \langle p_i;\ i \in I\rangle$.

2. *Výroky* čili *(výrokové) formule* nad $\mathbb{P}$ jsou právě designátory z $\mathrm{D}(\mathcal{F}_{\mathbb{P}})$, kde $\mathcal{F}_{\mathbb{P}} = \mathbb{P} \cup \{\neg, \rightarrow\}$; přitom prvky z $\mathbb{P}$ jsou nulární, $\neg$ je unární, $\rightarrow$ je binární.

$$\mathrm{VF}_{\mathbb{P}}$$

značí množinu všech výroků nad $\mathbb{P}$: $\mathrm{VF}_{\mathbb{P}} = \mathrm{D}(\mathcal{F}_{\mathbb{P}})$. Výroky značíme $\varphi, \psi, \chi, \varphi', \varphi_1, \psi'$ apod. Symbol $\mathrm{var}(\varphi)$ značí množinu všech prvovýroků vyskytujících se ve φ.

Množina $\mathrm{VF}_{\mathbb{P}}$ je zřejmě definována induktivně pravidly: Pro $p \in \mathbb{P}$ je $\langle p\rangle$ je výrok a jsou-li φ, ψ výroky, jsou jimi i $\neg(\varphi)$ a $\rightarrow(\varphi, \psi)$.

Zpravidla zapisujeme $\langle p\rangle$ pro $p \in \mathbb{P}$ jako p; prvovýrok je tak výrok.

3. *Výroková teorie nad* $\mathbb{P}$, též $\mathbb{P}$-*teorie*, je množina $T \subseteq \mathrm{VF}_{\mathbb{P}}$; její prvky jsou její *axiomy*. Symbol $\mathbb{P}(T)$ značí množinu prvovýroků jazyka teorie T. Výrok teorie T je výrok jejího jazyka.

2.1.2. Zavedení $\&, \vee, \leftrightarrow$ a $\perp, \top$. Konvence o zápisu formulí. Normální tvary.

1. 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 píše také $\wedge$.

Pravdivý výrok $\top$ specifikujeme jako $p \to p$, *lživý* výrok $\bot$ jako $\neg(p \to p)$; na konrétní volbě p nezáleží. Mluvíme o nich též jako o nulárních logických spojkách či výrokových konstantách.

2. Konvence o zápisu formulí. 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 nanzývá *konjunkce s konjunkty* $\varphi_1, \dots, \varphi_n$ resp. *disjunkce s disjunkty* $\varphi_1, \dots, \varphi_n$. Závorky můžeme pro zlepšení čitelnosti i přidat.

3. Výrok je *literál*, je-li to prvovýrok nebo negace prvovýroku. Disjunkce literálů se nazývá *klauzule*, konjunkce literálů též *elementární konjunkce*. Výrok je v *disjunktivně* resp. *konjunktivně normálním tvaru*, je-li to disjunkce konjunkcí literálů resp. konjunkce disjunkcí literálů.

ZNAČENÍ. Pro výrok φ, n-tici výroků $s = \langle \varphi_0, \dots, \varphi_{n-1} \rangle$ a $\sigma : n \to 2$ užíváme následující značení:

$$\varphi^1 \text{ je } \varphi, \qquad \varphi^0 \text{ je } \neg\varphi, \qquad s^\sigma \text{ je } \langle \varphi_0^{\sigma(0)}, \dots, \varphi_{n-1}^{\sigma(n-1)} \rangle,$$

$$\bigwedge s \ \text{ je } \ \varphi_0 \,\&\, \cdots \,\&\, \varphi_n, \qquad \bigwedge \emptyset \text{ je } \top, \qquad \bigvee s \ \text{ je } \ \varphi_0 \vee \cdots \vee \varphi_n, \qquad \bigvee \emptyset \text{ je } \bot.$$

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.

Sémantika výroků.

2.1.3. Modely výrokového jazyka a teorie. Sémantická ekvivalence výroků.

1. *Pravdivostní ohodnocení* $\mathbb{P}$ čili *model výrokového jazyka nad* $\mathbb{P}$ je funkce $v \in {}^{\mathbb{P}}2$. *Hodnota* $\overline{v}(\varphi)$ *výroku* φ *z* $\mathrm{VF}_{\mathbb{P}}$ *v ohodnocení* v je hodnota φ v $\mathcal{F}_{\mathbb{P}}$-struktuře

$$\langle 2, v(p), -_1, \to_1 \rangle_{p \in \mathbb{P}}.$$

Tedy $\overline{v}$ je funkce $\overline{v} : \mathrm{VF}_{\mathbb{P}} \to 2$ sestrojená rekurzí pravidly:

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

Když $\overline{v}(\varphi) = 1$, říkáme, že φ *platí* či *je splněno ve* v a také, že v je *model* φ. Dále je v *model teorie* $T \subseteq \mathrm{VF}_{\mathbb{P}}$, když je modelem každého axiomu T; píšeme

$$v \models T$$

a místo $v \models \{\varphi\}$ píšeme $v \models \varphi$. Místo $\overline{v}(\varphi)$ píšeme stručněji $v(\varphi)$.

2. Pro $T \subseteq \mathrm{VF}_{\mathbb{P}}$ je $\mathsf{M}^{\mathbb{P}}(T)$ *třída všech modelů teorie* T:

$$\mathsf{M}^{\mathbb{P}}(T) = \{v \in {}^{\mathbb{P}}2;\ v \models T\}.$$

Místo $\mathsf{M}^{\mathbb{P}}(T \cup \{\varphi_1, \dots, \varphi_k\})$ píšeme $\mathsf{M}^{\mathbb{P}}(T, \varphi_1, \dots, \varphi_k)$ a T vynecháme, je-li $\emptyset$. Dále $-\mathsf{M}^{\mathbb{P}}(T)$ značí ${}^{\mathbb{P}}2 - \mathsf{M}^{\mathbb{P}}(T)$; je to *komplement* třídy $\mathsf{M}^{\mathbb{P}}(T)$.

3. Buď $T \subseteq \mathrm{VF}_{\mathbb{P}}$. Formule φ, ψ z $\mathrm{VF}_{\mathbb{P}}$ jsou T-*sémanticky ekvivalentní*, když platí $\mathsf{M}^{\mathbb{P}}(T, \varphi) = \mathsf{M}^{\mathbb{P}}(T, \psi)$; píšeme

$$\varphi \sim_T \psi.$$

Vynecháme T, je-li $\emptyset$; místo $\emptyset$-sémanticky ekvivalentní tedy říkáme *sémanticky ekvivalentní* a máme $\varphi \sim \psi \Leftrightarrow \mathsf{M}^{\mathbb{P}}(\varphi) = \mathsf{M}^{\mathbb{P}}(\psi)$.

ÚMLUVA. Symbol $\mathbb{P}$ můžeme vynechat, nevede-li to k nedorozumění. Mluvíme tak např. jen o výrocích, místo $\mathrm{VF}_{\mathbb{P}}$ píšeme VF, místo $\mathsf{M}^{\mathbb{P}}$ jen M atd.

Snadno se zjistí, že pro $T \subseteq \mathrm{VF}$ a $\emptyset \neq \mathcal{T} \subseteq \mathcal{P}(\mathrm{VF})$ platí:

$$T' \subseteq T \Rightarrow \mathsf{M}(T) \subseteq \mathsf{M}(T'), \qquad \mathsf{M}(\bigcup \mathcal{T}) = \bigcap \{\mathsf{M}(T);\, T \in \mathcal{T}\}.$$

TVRZENÍ 2.1.4. (Vlastnosti ohodnocení výroků.) *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* $\mathrm{var}(\varphi)$.

b) $v(\varphi \diamond \psi) = v(\varphi) \diamond_1 v(\psi)$ *pro* $\diamond$ *rovno* $\vee, \wedge, \leftrightarrow$.

2) *Buď* $\mathbb{P}$ *konečné,* $K \subseteq {}^{\mathbb{P}}2$*; označme* $-K = {}^{\mathbb{P}}2 - K$. *Pak*

$$\mathsf{M}^{\mathbb{P}}(\bigvee_{w \in K} \bigwedge_{p \in \mathbb{P}} p^{w(p)}) = K = \mathsf{M}^{\mathbb{P}}(\bigwedge_{w \in -K} \bigvee_{p \in \mathbb{P}} p^{-{}^1 w(p)}).$$

3) *Formule* φ *je sémanticky ekvivalentní 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 $\mathbb{P}$. $\square$

TVRZENÍ 2.1.5. (O třídách modelů formulí v teorii. Definice AM_T.) *Buď* $T \subseteq \mathrm{VF}$ *s* $\mathsf{M}(T) \neq \emptyset$. *Pak*

$$\mathsf{M}(T, \neg\varphi) = \mathsf{M}(T) - \mathsf{M}(T, \varphi),\ \mathsf{M}(T, \bot) = \emptyset,\ \mathsf{M}(T, \top) = \mathsf{M}(T),$$
$$\mathsf{M}(T, \varphi \diamond \psi) = \mathsf{M}(T, \varphi) \diamond' \mathsf{M}(T, \psi),\ \textit{kde } \diamond \textit{ je } \vee, \&\ \textit{a } \diamond' \textit{ je } \cup, \cap.$$

Důsledky.

a) $\mathrm{AM}_T = \{\mathsf{M}(T, \varphi);\, \varphi \in \mathrm{VF}\}$ *je univerzum podalgebry algebry* $\mathcal{P}(\mathsf{M}(T))$. *Uvedená podalgebra se nazývá* algebra tříd modelů formulí v T *a značíme ji* AM_T.

b) *Chápeme-li* $\neg, \vee, \&, \bot, \top$ *jako operace na* $\mathrm{VF}_{\mathbb{P}}$*, platí o nich booleovské zákony, tj. asociativita, komutativita, distributivita, absorbce a kompletace, nahradíme-li v nich* $=$ *vztahem* $\sim_T$. *Z nich plynou dále: idempotence, extremalita, neutralita a de Morganovy zákony.*

Důkaz. Prvá část tvrzení plyne ihned z definic. Důsledek a) je bezprostřední, neboť uvedené rovnosti zaručují uzavřenost AM_T na komplement do $\mathsf{M}(T)$, $\cup$, $\cap$ a $\emptyset$. Důsledek b). Máme $\mathsf{M}(T, \varphi \vee \psi) = \mathsf{M}(T, \varphi) \cup \mathsf{M}(T, \psi) = \mathsf{M}(T, \psi) \cup \mathsf{M}(T, \varphi) = \mathsf{M}(T, \psi \vee \varphi)$. Tedy $\varphi \vee \psi \sim_T \psi \vee \varphi$. Podobně je tomu s komutativitou &, asociativitou $\vee$ atd. $\square$

TVRZENÍ 2.1.6. (O sémantické ekvivalenci.) *Vznikne-li formule* φ' *z* φ *nahrazením některého výskytu podformule* ψ *formulí* ψ'*, tak* $\psi \sim_T \psi' \Rightarrow \varphi \sim_T \varphi'$.

Důkaz. Indukcí na výrocích. Pro prvovýrok φ to jasně platí. Je-li φ tvaru $\neg\varphi_0$, je buď uvažovaný výskyt formule ψ právě φ a je to jasné, nebo to je výskyt ve φ_0. Pak z indukčního předpokladu máme $\mathsf{M}(\varphi_0) = \mathsf{M}(\varphi_0')$ a tedy i $\varphi \sim_T \varphi'$. Podobně, je-li φ tvaru $\varphi_0 \rightarrow \varphi_1$. $\square$

APLIKACE. Důsledek b) z 2.1.5 a 2.1.6 lze užít k nalézání sémantických ekvivalentů. Např.: $(p \rightarrow q)\ \&\ q \sim (\neg p \vee q)\ \&\ q \sim (\neg p\ \&\ q) \vee (q\ \&\ q) \sim (\neg p\ \&\ q) \vee q \sim q$.

1. $\sim$ plyne užitím tvrzení o sémantické ekvivalenci a díky $p \rightarrow q \sim \neg p \vee q$, 2. $\sim$ dává distributivní zákon, 3. $\sim$ idempotence, 4. absorbce. Získali jsme zároveň k formuli $(p \rightarrow q)\ \&\ q$ sémantické ekvivalenty v konjunktivně normálním tvaru i v disjunktivně normálním tvaru.

2.1.7. Pravdivost a lživost výroku v teorii. Nezávislá a splnitelná formule.

Buď $T \subseteq \mathrm{VF}_{\mathbb{P}}$, $\varphi \in \mathrm{VF}_{\mathbb{P}}$.

- Formule φ je *pravdivá v* T, když φ platí v každém modelu v teorie T; píšeme

$$T \models \varphi.$$

- Formule φ je *lživá v* T, neplatí-li v žádném modelu teorie T, čili když $T \models \neg\varphi$. Množinu všech $\mathbb{P}$-formulí pravdivých resp. lživých v T značíme

$$\Theta_{\mathbb{P}}(T) \quad \text{resp.} \quad \Theta'_{\mathbb{P}}(T).$$

- Není-li φ ani pravdivá ani lživá v T, je φ *nezávislá v* T.
- Není-li φ lživá v T, je *splnitelná v* T a též *konzistentní s* T.
- Když $T \models \varphi \to \psi$, je φ *silnější než* ψ a ψ *slabší než* φ *v* T.

Je-li T prázdná teorie, frázi "v (s) T" vynecháváme. Místo φ je pravdivá resp. lživá také říkáme, že φ je *tautologie* resp. *lež*. Množina všech tautologií resp. splnitelných výroků se značí též $\mathrm{TAUT}_{\mathbb{P}}$ resp. $\mathrm{SAT}_{\mathbb{P}}$.

Místo $\emptyset \models \varphi$ píšeme $\models \varphi$, místo $\{\varphi_0, \ldots, \varphi_{n-1}\} \models \varphi$ též jen $\varphi_0, \ldots, \varphi_{n-1} \models \varphi$.

TVRZENÍ 2.1.8. (Vlastnosti $\Theta(T)$.) *Buďte T, S teorie. Pak platí:*
1) $\mathsf{M}(\Theta(T)) = \mathsf{M}(T)$.
2) $T \subseteq \Theta(T)$, $\qquad T \subseteq S \Rightarrow \Theta(T) \subseteq \Theta(S)$, $\qquad \Theta(T) = \Theta(\Theta(T))$.

Důkaz. 1) Jelikož $v \models T \Rightarrow v \models \Theta(T)$, máme $\mathsf{M}(T) \subseteq \mathsf{M}(\Theta(T))$. Inkluze $\supseteq$ plyne z $T \subseteq \Theta(T)$. Druhé tvrzení z 2) plyne snadno. Jelikož $T \models \varphi \Leftrightarrow \mathsf{M}(T) \subseteq \mathsf{M}(\varphi)$, dostaneme i třetí tvrzení z 2) užitím 1): $\varphi \in \Theta(\Theta(T)) \Leftrightarrow \Theta(T) \models \varphi \Leftrightarrow \mathsf{M}(\Theta(T)) \subseteq \mathsf{M}(\varphi) \Leftrightarrow \mathsf{M}(T) \subseteq \mathsf{M}(\varphi) \Leftrightarrow T \models \varphi \Leftrightarrow \varphi \in \Theta(T)$. □

TVRZENÍ 2.1.9. (Vztahy $\models$ a M.) *Pro teorii T a formule φ, ψ jejího jazyka platí:*
1) $T \models \varphi \Leftrightarrow \mathsf{M}(T) \subseteq \mathsf{M}(\varphi)$
2) $T \models \varphi \to \psi \Leftrightarrow \mathsf{M}(T,\varphi) \subseteq \mathsf{M}(T,\psi) \Leftrightarrow \mathsf{M}(T,\varphi) \subseteq \mathsf{M}(\psi) \Leftrightarrow T,\varphi \models \psi$
3) $T \models \varphi \leftrightarrow \psi \Leftrightarrow \mathsf{M}(T,\varphi) = \mathsf{M}(T,\psi)$

Důkaz plyne snadno z definic. □

VĚTA 2.1.10. (Vlastnosti $\models$.) *Pro teorii T a formule φ, ψ, χ jejího jazyka platí:*

1)
$$\begin{array}{lcl}
T \models \varphi \to \psi & \Leftrightarrow & T \models \neg\psi \to \neg\varphi \\
T \models \varphi \leftrightarrow \psi & \Leftrightarrow & T \models \varphi \to \psi \ \text{ a } \ T \models \psi \to \varphi \\
T \models \varphi \,\&\, \psi & \Leftrightarrow & T \models \varphi \text{ a } T \models \psi \\
T \models \varphi \vee \psi & \Leftarrow & T \models \varphi \text{ nebo } T \models \psi \\
T \models \varphi \to \psi \ \text{ a } \ T \models \varphi & \Rightarrow & T \models \psi \\
T \models \varphi \to \psi \ \text{ a } \ T \models \psi \to \chi & \Rightarrow & T \models \varphi \to \chi \\
T \models \varphi \leftrightarrow \psi \ \text{ a } \ T \models \psi \leftrightarrow \chi & \Rightarrow & T \models \varphi \leftrightarrow \chi \\
T \models \varphi \leftrightarrow \psi & \Rightarrow & (T \models \varphi \Leftrightarrow T \models \psi)
\end{array}$$

2) *(Rozbor případů.)* $T \models (\varphi \vee \psi) \to \chi \Leftrightarrow (T \models \varphi \to \chi$ *a* $T \models \psi \to \chi)$
Speciálně: $T \models \varphi \to \psi$ *a* $T \models \neg\varphi \to \psi \Rightarrow T \models \psi$

Důkaz. 1) $T \models \varphi \to \psi \Leftrightarrow \mathsf{M}(T,\varphi) \subseteq \mathsf{M}(T,\psi) \Leftrightarrow -\mathsf{M}(T,\psi) \subseteq -\mathsf{M}(T,\varphi) \Leftrightarrow \mathsf{M}(T,\neg\psi) \subseteq \mathsf{M}(T,\neg\varphi) \Leftrightarrow T \models \neg\psi \to \neg\varphi$. Užili jsme 2.1.9. Podobně nebo užitím již dokázaného plynou další položky.

2) $T \models (\varphi \vee \psi) \to \chi \Leftrightarrow \mathsf{M}(\varphi \vee \psi) \subseteq \mathsf{M}(\chi) \Leftrightarrow \mathsf{M}(\varphi) \subseteq \mathsf{M}(\chi)$ a $\mathsf{M}(\psi) \subseteq \mathsf{M}(\chi) \Leftrightarrow T \models \varphi \to \chi$ a $T \models \psi \to \chi$. □

2.1.11. Extenze teorie, ekvivalentní, konečně axiomatizovatelné a kompletní teorie.
Buďte T, S výrokové teorie.

1. Teorie S je *extenze* T, když $\mathbb{P}(T) \subseteq \mathbb{P}(S)$ a $\Theta(T) \subseteq \Theta(S)$. Je-li $\mathbb{P}(T) = \mathbb{P}(S)$, je to *jednoduchá* extenze. Teorie T je *ekvivalentní s* S, je-li každá z nich extenzí druhé. Teorie je *konečně axiomatizovatelná*, je-li ekvivalentní teorii s konečně axiomy.

2. Teorie T je *kompletní*, jestliže má model a pro každou formuli φ jejího jazyka je $T \models \varphi$ nebo $T \models \neg\varphi$, tj. T nemá nezávislý výrok.

TVRZENÍ 2.1.12. *Buďte T, S výrokové teorie v témže jazyce.*

1) *Teorie S je extenze T, právě když $\mathsf{M}(S) \subseteq \mathsf{M}(T)$. Teorie S je ekvivalentní s T, právě když $\mathsf{M}(S) = \mathsf{M}(T)$.*

2) *Teorie T je kompletní, právě když má právě jeden model.*

Důkaz. 1) Platí $T' \subseteq T \Rightarrow \mathsf{M}(T) \subseteq \mathsf{M}(T')$. Užijeme-li ještě 2.1.8, 1), dostaneme požadované. 2) Má-li T právě jeden model, je jasně kompletní. Nechť naopak T má alespoň dva různé modely v, w; existuje pvovýrok p s $v(p) \neq w(p)$. Pak p je nezávislý výrok T. $\square$

APLIKACE. Základní analýza teorií nad konečně prvovýroky.

Buď $\mathbb{P}$ velikosti $l \in \mathbb{N}$, T nějaká $\mathbb{P}$-teorie. Pomocí 2.1.9 a 2.1.12 lze zjistit počet pravdivých, lživých a nezávislých výroků T až na sémantickou ekvivalenci $\sim$, dále počet neekvivalentních jednoduchých (kompletních) extenzí T, počet nezávislých výroků T až na $\sim_T$ apod. Např. počet pravdivých výroků φ teorie T až na $\sim$ je $2^{2^l - |\mathsf{M}(T)|}$, neboť různých $\mathsf{M}(\varphi)$ takových, že $\mathsf{M}(T) \subseteq \mathsf{M}(\varphi)$ je tolik, kolik je podmnožin množiny ${}^{\mathbb{P}}2 - \mathsf{M}(T)$.

Sémantická kompaktnost. Axiomatizovatelnost.

VĚTA 2.1.13. (O sémantické kompaktnosti.) *Teorie má model, právě když každá její konečná část má model.*

Důkaz. Implikace zleva doprava je jasná. Dokážeme opačnou. Buď T teorie, jejíž každá konečná část má model; říkejme, že T je konečně splnitelná. Existuje maximální konečně splnitelná teorie $S \supseteq T$, tj. taková konečně splnitelná teorie $S \supseteq T$, jejíž každé vlastní rozšíření má konečnou část, která nemá model. Existence S plyne z principu maximality, aplikovaného na uspořádání

$$\langle \{T';\ \ T' \text{ je konečně splnitelná a } T' \supseteq T\}, \subseteq \rangle;$$

to splňuje předpoklad principu maximality, že totiž každá lineárně uspořádané podmnožina $\mathbb{L}$ má majorantu – tou je jasně $\bigcup \mathbb{L}$. Tudíž uvažované uspořádání má maximální prvek S. Ukážeme, že S má model; ten je díky $T \subseteq S$ i modelem T. Předně platí:

(a) $(\varphi \in S, \varphi \to \psi \in S) \Rightarrow \psi \in S$, (b) $\varphi \in S \Leftrightarrow \neg\varphi \notin S$,
(c) $\varphi \to \psi \in S \;\Leftrightarrow \neg\varphi \in S$ nebo $\psi \in S$.

(a) je jasné, neboť $S \cup \{\psi\}$ je konečně splnitelná. (b): $\Rightarrow$ platí, neboť $\{\varphi, \neg\varphi\}$ nemá model. Dokážeme $\Leftarrow$. Buď $\neg\varphi \notin S$; dokážeme, že $S \cup \{\varphi\}$ je konečně splnitelná – díky maximalitě pak $\varphi \in S$. Existuje $S_0 \subseteq S$ konečná tak, že $S_0 \cup \{\neg\varphi\}$ nemá model. Pro $S' \subseteq S$ konečnou existuje model $v \models S' \cup S_0$; ovšem $v(\varphi) = 1$ a jsme hotovi. (c) Implikace $\Rightarrow$. Když $\neg\varphi \notin S$, tak $\varphi \in S$ dle (b) a pak $\psi \in S$ dle (a). Implikace $\Leftarrow$. Když $\neg\varphi \in S$, pro $S' \subseteq S$ konečnou existuje model $v \models S' \cup \{\neg\varphi\}$; pak $v(\varphi \to \psi) = 1$ a vidíme, že $S \cup \{\varphi \to \psi\}$ je konečně splnitelná. Stejně je tomu, když $\psi \in S$.

Definujme nyní $v \in {}^{\mathbb{P}}2$ takto: $v(p) = 1 \Leftrightarrow p \in S$. Pak pro každou formuli φ platí $v(\varphi) = 1 \Leftrightarrow \varphi \in S$, což plyne indukcí na formulích: pro prvovýrok φ to vyplývá z definice, indukční krok pro $\neg$ resp. $\to$ plyne užitím (b) resp. (c). $\square$

2.1.14. Axiomatizovatelné množiny ohodnocení. Elementární konjunkce ε_σ.

1. Množina $K \subseteq {}^{\mathbb{P}}2$ je *axiomatizovatelná* resp. *konečně axiomatizovatelná*, existuje-li teorie resp. konečná teorie T tak, že $K = \mathsf{M}(T)$. Je-li K konečně axiomatizovatelná, je zřejmě $K = \mathsf{M}(\varphi)$ pro nějakou formuli φ.

2. Pro funkci $\sigma \subseteq \mathbb{P} \times 2$ značíme

$$\widetilde{\sigma} = \{v \in {}^{\mathbb{P}}2;\ \sigma \subseteq v\}.$$

Pro konečnou funkci $\sigma \subseteq \mathbb{P} \times 2$ je *elementární konjunkce určená* σ formule $\bigwedge_{p \in \mathrm{dom}(\sigma)} p^{\sigma(p)}$; značíme ji ε_σ. Platí: $\mathsf{M}(\varepsilon_\sigma) = \widetilde{\sigma}$.

Buď $K \subseteq {}^{\mathbb{P}}2$. Řekneme, že $v \in {}^{\mathbb{P}}2$ je *oddělené* od K, když existuje $\sigma \subseteq v$ konečné s $\widetilde{\sigma} \cap K = \emptyset$. Dále K je *uzavřená*, když K obsahuje každé v, které není oddělené od K. K je *otevřená* resp. *obojetná*, je-li komplement ${}^{\mathbb{P}}2 - K$ uzavřená resp. K i její komplement jsou uzavřené. Zřejmě $\emptyset, {}^{\mathbb{P}}2$ jsou uzavřené.

Z definic ihned plyne:

K1) a) Průnik neprázdného systému uzavřených množin je uzavřená množina.
b) Sjednocení konečně mnoha uzavřených množin je uzavřená množina.

K2) Buď $K \subseteq {}^{\mathbb{P}}2$. Pak:
a) $v \in {}^{\mathbb{P}}2 - K$ je oddělená od K $\Leftrightarrow$ existuje ψ s $v \in \mathsf{M}(\psi)$ a $\mathsf{M}(\psi) \cap K = \emptyset$.
b) K je uzavřená $\Leftrightarrow$ pro každou $v \in {}^{\mathbb{P}}2 - K$ existuje ψ s $v \in \mathsf{M}(\psi)$ a $\mathsf{M}(\psi) \cap K = \emptyset$.

VĚTA 2.1.15. (O axiomatizovatelnosti.)

1) *Množina $K \subseteq {}^{\mathbb{P}}2$ je konečně axiomatizovatelná, právě když ona i její komplement jsou axiomatizovatelné.*

2) a) *Množina $K \subseteq {}^{\mathbb{P}}2$ je axiomatizovatelná, právě když je uzavřená.*

b) *Množina $K \subseteq {}^{\mathbb{P}}2$ je konečně axiomatizovatelná, právě když je obojetná.*

Důkaz. 1) Implikace $\Rightarrow$ je jasná. Dokážeme opačnou. Nechť T, S jsou takové teorie, že $K = \mathsf{M}(T) = -\mathsf{M}(S)$. Pak $\mathsf{M}(T \cup S) = \mathsf{M}(T) \cap \mathsf{M}(S) = \emptyset$, tedy díky kompaktnosti existují $T' \subseteq T$, $S' \cup S$ 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) a) Implikace $\Leftarrow$. Dle K2) b) je $-K = \bigcup_{\psi \in S} \mathsf{M}(\psi)$ pro jistou množinu S formulí. Pak $K = \bigcap_{\psi \in S} \mathsf{M}(\neg\psi)$ a tedy $K = \mathsf{M}(T)$ s $T = \{\neg\psi;\ \psi \in S\}$.

Implikace $\Rightarrow$. Předně je $\mathsf{M}(\varphi)$ uzavřená. Pro v z $-\mathsf{M}(\varphi)$ je totiž $v \in \mathsf{M}(\neg\psi_i)$ s jistou ψ_i, přičemž $\bigvee_{i<n} \psi_i$ je disjunktivně normální tvar φ s elementárními konjunkcemi ψ_i; uzavřenost $\mathsf{M}(\varphi)$ plyne z K2) b). Je-li nyní $K = \mathsf{M}(T)$, je $K = \bigcap_{\varphi \in T} \mathsf{M}(\varphi)$ a uzavřenost K plyne z K1) a).

b) je důsledek 1) a 2) a). □

2.2 Dedukce. Úplnost výrokové logiky

Dedukce je vyvozování formulí z jistých předpokladů, a to podle pravidel dedukce. Předpoklady jsou představovány axiomy nějaké teorie $T \subseteq \mathrm{VF}$; vždy k nim přidáváme množinu LAx tzv. *logických axiomů*, což jsou jisté pravdivé formule. Pravidlo dedukce je obecně zobrazení, které nějakým konečně mnoha formulí přiřadí jednu jako jejich důsledek, vyvozený podle tohoto pravidla.

2.2.1. Logické axiomy a pravidlo dedukce.

1. Logické výrokové axiomy LAx jsou dány následujícími schematy formulí:

(PL1) $\varphi \to (\psi \to \varphi)$
(PL2) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$
(PL3) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$

2. V seznamu axiomů teorie T logické axiomy nadále neuvádíme. Říkáme pak, že formule z T jsou *mimologické axiomy* teorie T.

3. Pravidlo dedukce je ve výrokové logice jediné, a to *pravidlo odloučení* neboli *modus ponens* (MP):

$$\text{z } \varphi,\ \varphi \to \psi \text{ odvoď } \psi.$$

Formálně jde o zobrazení $\mathrm{MP}(\varphi, \varphi \to \psi) = \psi$.

2.2.2. Důkaz, dokazatelná formule čili teorém. Sporná a bezesporná teorie.

Buď T teorie.

1. *Důkaz v* T je {MP}-odvození z $T \cup \mathrm{LAx}$; je to *důkaz formule*, která je jeho posledním členem. Formule φ je *dokazatelná* v T čili to je *teorém* v T, existuje-li nějaký její důkaz v T; píšeme pak

$$T \vdash \varphi.$$

Formule φ je *vyvratitelná* a též *spor* v T, když $T \vdash \neg\varphi$. Když $T = \emptyset$, vypouštíme v uvedených pojmech výraz „v T“ či jej nahradíme výrazem „logicky“. Množinu všech teorémů teorie T značíme

$$\mathrm{Thm}(T) \quad \text{nebo} \quad \mathrm{Thm}_T.$$

Tedy $\mathrm{Thm}(T)$ je {MP}-uzávěr $T \cup \mathrm{LAx}$. Speciálně jsou teorémy teorie T definovány induktivně pravidly:

- Každý axiom teorie T a každý logický axiom je teorém teorie T.
- Jsou-li φ, $\varphi \to \psi$ teorémy teorie T, je ψ teorém teorie T.

2. Teorie T je *sporná*, je-li v ní dokazatelná každá formule; jinak je *bezesporná.*

TVRZENÍ 2.2.3.

1) (O korektnosti.) *Každá v T dokazatelná formule je v T pravdivá.*

2) *Má-li teorie model, je bezesporná.*

Důkaz. 1) Indukcí na teorémech. Každý axiom z T nebo logický 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. □

Níže dokážeme i opačnou implikaci k tvrzení o korektnosti a získáme tak zásadní větu o úplnosti výrokové logiky: formule je v T dokazatelná, právě když je v T pravdivá. Její důkaz se opírá o větu o existenci modelu bezesporné teorie – vše je formulováno v 2.2.6.

VĚTA 2.2.4. *Buďte φ, ψ formule výrokové teorie T.*

1) $\vdash \varphi \to \varphi$.

2) (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 $T \vdash \psi \to \varphi$. □

LEMMA 2.2.5. *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. □

VĚTA 2.2.6. *Buďte φ, ψ formule teorie T.*

1) a) *Teorie T je sporná, právě když je v ní dokazatelný spor.*

   b) (Důkaz sporem.) *$T, \neg\varphi$ je sporná $\Leftrightarrow T \vdash \varphi$.*

2) *Buď T maximální bezesporná teorie. 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.*

3) *Bezesporná teorie má maximální bezesporné rozšíření (v témže jazyce).*

4) (O existenci modelu.) *Teorie má model, právě když je bezesporná.*

5) (O kompaktnosti.) *Teorie má model, právě když každá její konečná podteorie má model.*

6) (O úplnosti.) *$T \vdash \varphi \;\Leftrightarrow\; T \models \varphi$ platí pro každou teorii T a její formuli φ.*

Důkaz. 1) a) Je-li φ spor, tj. $\vdash \neg\varphi$, a $T \vdash \varphi$, plyne z 2.2.5, a), že $T \vdash \psi$ pro jakýkoli výrok ψ. b) Implikace $\Rightarrow$: $T, \neg\varphi$ sporná implikuje $T \vdash \neg\varphi \to \varphi$ užitím věty o dedukci. Pak $T \vdash \varphi$ užitím z 2.2.5, e). Implikace $\Leftarrow$ plyne z 2.2.5, a).

2) 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 2.2.5, 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 $w = v$.

3) 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.

4) Má-li T model v a $T \vdash \varphi$, tak $\overline{v}(\varphi) = 1$, tedy $\overline{v}(\neg\varphi) = 0$, tedy $T \nvdash \neg\varphi$ a T je bezesporná. Nechť je T bezesporná. Dle 3) existuje maximální bezesporná teorie $T' \supseteq T$ a dle 2), c) existuje model teorie T', což je i model T.

5) Plyne z 4) a z toho, že teorie je bezesporná, právě když je bezesporná každá její konečná podteorie.

6) $T \vdash \varphi \Rightarrow T \models \varphi$ 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 1), b). □

POZNÁMKA 2.2.7. K existenci maximálního bezesporného rozšíření teorie T jsme potřebovali axiom výběru. Je-li T v jazyce s nejvýše spočetně prvovýroky, uvedené rozšíření se sestrojí snadno 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.

Uveďme několik důsledků věty o úplnosti.
Je $\mathrm{Thm}(T) = \Theta(T)$. Speciálně je T extenze T', právě když $\mathrm{Thm}(T) \supseteq \mathrm{Thm}(T')$ a T je ekvivalentní s T', právě když $\mathrm{Thm}(T) = \mathrm{Thm}(T')$. Z 2.1.6 získáme syntaktickou verzi tvrzení o ekvivalenci: *Vznikne-li formule φ' z φ nahrazením některých výskytů podformule ψ formulí ψ', tak $T \vdash \psi \leftrightarrow \psi' \Rightarrow T \vdash \varphi \leftrightarrow \varphi'$.* V 2.1.10 lze zaměnit $\models$ za $\vdash$; získaná tvrzení můžeme nazývat *deduktivní obraty výrokové logiky.*

Syntaktické metody dokazování.

2.2.8. O syntaktických metodách dokazování.
Jde o metody prokazování dokazatelnosti formulí (v nějaké dané teorii T, to jest vztahu $T \vdash \varphi$) jen pomocí syntaktických pojmů, tj. bez užití pojmu modelu, pravdivosti a věty o úplnosti. Typicky se užívají:
– Již syntakticky prokázané dokazatelnosti nějakých formulí, speciálně axiomů.
– Pravidlo MP, věta o dedukci, důkaz sporem a dále indukce.
– Obraty tvaru

$$T \vdash \varphi_1, \ldots, T \vdash \varphi_n \Rightarrow T \vdash \varphi, \text{ pokud } \varphi_1, \ldots, \varphi_n, \varphi \text{ splňují } ---,$$

jsou-li získány syntakticky. Říkejme jim neformálně důkazová pravidla; pojem zavádíme jen k jistému zpřehlednění vyjadřování. Uveďme, že z $T \vdash \varphi \to \psi$ plyne triviálně důkazové pravidlo $T \vdash \varphi \Rightarrow T \vdash \psi$; můžeme tak např. užívat jako důkazové pravidlo $T \vdash \varphi \Rightarrow T \vdash \neg\neg\varphi$ dle b) z 2.2.5, dále důkazové pravidlo $T \vdash \varphi \Rightarrow T \vdash \psi \to \varphi$ plynoucí z (PL1) apod. Další taková pravidla jsou obsažená např. v 2.2.9 3). Jiné důkazové pravidlo je obsaženo v 2.2.12 ve formulaci b).

Syntakticky prokázané jsou zatím

$$\vdash \varphi \to \varphi \text{ (viz 2.2.4)}, \qquad \text{a) – e) z 2.2.5.}$$

Na a) – e) z 2.2.5 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 2.2.9.

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)
$$T \vdash \varphi \,\&\, \psi \quad \Leftrightarrow \quad T \vdash \varphi \text{ a } T \vdash \psi$$
$$T \vdash \varphi \leftrightarrow \psi \quad \Leftrightarrow \quad T \vdash \varphi \to \psi \text{ a } T \vdash \psi \to \varphi$$

Pravidlo tranzitivity $\leftrightarrow$:

$$T \vdash \varphi \leftrightarrow \psi \text{ a } T \vdash \psi \leftrightarrow \chi \quad \Rightarrow \quad T \vdash \varphi \leftrightarrow \chi$$

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 2.2.5.

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 2.2.10. *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 2.2.9 1) a věty o dedukci máme $\vdash \varphi \to (\varphi \,\&\, \varphi)$, $\vdash (\varphi \,\&\, \varphi) \to \varphi$, dle 2.2.9 2) tedy $\vdash \varphi \leftrightarrow (\varphi \,\&\, \varphi)$. 2) Dle 2.2.9 1) je $\varphi \,\&\, \psi \vdash \{\varphi, \psi\} \vdash \{\psi, \varphi\} \vdash \psi \to \varphi$, tj. $\vdash (\varphi \,\&\, \psi) \to (\psi \,\&\, \varphi)$. Tudíž i $\vdash (\psi \,\&\, \varphi) \to (\varphi \,\&\, \psi)$ a dokazovaná ekvivalence plyne z 2.2.9 2). 3) se dokáže zcela obdobně.

4) Je $\vdash \varphi \to \varphi$, dle 2.2.9 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 2.2.9 3) tedy i $\vdash \varphi \leftrightarrow \neg\neg\varphi$. □

TVRZENÍ 2.2.11. *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 2.2.9 2) b). Dokažme $\to$ indukcí dle n. Užitím 2.2.9 1) b), MP a indukčního předpokladu máme

$$\{\varphi_1 \,\&\, (\varphi_2 \,\&\, \cdots \,\&\, \varphi_n), (\varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots)))\} \vdash$$
$$\{\varphi_2 \,\&\, \cdots \,\&\, \varphi_n, \varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots))\} \vdash \psi.$$

Zcela stejně plyne $\leftarrow$.

2) Stačí ukázat dokazatelnost $\to$ a $\leftarrow$; tvrzení pak plyne z 2.2.9 2) b). Implikace $\to$ plyne z 2.2.9 2) a), 1) b) a tranzitivity dedukce, implikace $\leftarrow$ z 2.2.9 1) a), 2) b) a tranzitivity dedukce.

3) Stačí ukázat dokazatelnost $\to$ a $\leftarrow$; tvrzení pak plyne z 2.2.9 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 2.2.9, [c], MP; tedy $\varphi \leftrightarrow \psi \vdash \neg\varphi \to \neg\psi$. Zcela stejně plyne $\neg\varphi \to \neg\psi \vdash \varphi \leftrightarrow \psi$. Dle 2.2.9 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 2.2.12. (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 $\vdash (\psi \to \psi') \to (\psi \to \psi')$, 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 2.2.11 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 2.2.9 3) pak $\psi \leftrightarrow \psi' \vdash \varphi \leftrightarrow \varphi'$. □

TVRZENÍ 2.2.13. *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:

$\neg(\varphi \,\&\, \psi)$	$\leftrightarrow$	$\neg\neg(\varphi \to \neg\psi)$	zavedení &
	$\leftrightarrow$	$\varphi \to \neg\psi$	$\vdash \neg\neg\chi \leftrightarrow \chi$
	$\leftrightarrow$	$\neg\neg\varphi \to \neg\psi$	věta o ekvivalenci, $\vdash \chi \leftrightarrow \neg\neg\chi$
	$\leftrightarrow$	$\neg\varphi \vee \neg\psi$	zavedení $\vee$.

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 $x \wedge y = -(-x \vee -y)$, $x \vee y = -(-x \wedge -y)$.

Vícehodnotová sémantika výroků.

2.2.14. Výroková evaluace a sémantika nad ní.

Ukážeme jisté abstraktní zobecnění výrokové sémantiky. Pomocí ní prokážeme nevyvoditelnost některých axiomů výrokové logiky z jiných.

1. *Výroková evaluace* je struktura $\underline{\mathsf{V}} = \langle \mathsf{V}, \neg^{\mathsf{V}}, \to^{\mathsf{V}} \rangle$, kde

$$\{0, 1\} \subseteq \mathsf{V}, \;\; \neg^{\mathsf{V}} \text{ je unární funkce}, \;\; \to^{\mathsf{V}} \text{ je binární funkce}.$$

2. Pro *ohodnocení* $v : \mathbb{P} \to \mathsf{V}$ výrokových proměnných ve V je *hodnota* $v^{\mathsf{V}}(\varphi)$ výroku φ hodnota $\mathcal{F}_{\mathbb{P}}$-designátoru φ ve struktuře

$$\langle \mathsf{V}, v(p)_{p\in\mathbb{P}}, \neg^{\mathsf{V}}, \to^{\mathsf{V}} \rangle,$$

tj. je sestrojená rekurzí pravidly:

$$v^{\mathsf{V}}(p) = v(p) \text{ je-li } \varphi \text{ z } \mathbb{P},\ v^{\mathsf{V}}(\neg\varphi) = \neg^{\mathsf{V}}(v^{\mathsf{V}}(\varphi)),\ v^{\mathsf{V}}(\varphi \to \psi) = v^{\mathsf{V}}(\varphi) \to^{\mathsf{V}} v^{\mathsf{V}}(\psi).$$

Říkáme, že $\underline{\mathsf{V}}$ je MP-*korektní*, pokud platí:

$$(v^{\mathsf{V}}(\varphi) = 1 \text{ a } v^{\mathsf{V}}(\varphi \to \psi) = 1) \Rightarrow v^{\mathsf{V}}(\psi) = 1.$$

Speciálním případem je výroková evaluace $\langle 2, -_1, \to_1 \rangle$, 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 $\varphi \in \mathrm{VF}_{\mathbb{P}}$, $T \subseteq \mathrm{VF}_{\mathbb{P}}$, $v : \mathbb{P} \to \mathsf{V}$.

- $v \models^{\mathsf{V}} \varphi$ 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 $v : \mathbb{P} \to \mathsf{V}$.
- $T \models^{\mathsf{V}} \varphi$ značí, že $v \models^{\mathsf{V}} T \Rightarrow v \models^{\mathsf{V}} \varphi$. Je-li $T = \emptyset$, nepíšeme je.
- φ je $^{\mathsf{V}}$-*tautologie*, když $\models^{\mathsf{V}} \varphi$.

TVRZENÍ 2.2.15. (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 korektnosti $\underline{\mathsf{V}}$.

2.2.16.
Buď T tvořeno právě schematy (PL1), (PL2).
1. Buď výroková evaluace $\underline{\mathsf{V}} = \langle 3, \neg', \to' \rangle$ dána takto:

$\neg'$	
0	1
1	0
2	0

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

Platí:
a) $\underline{\mathsf{V}}$ je MP-korektní a $\models^{\mathsf{V}} T \cup \{\varphi \to (\neg\varphi \to \psi)\}$. Speciálně

$$T \models^{\mathsf{V}} \varphi \to (\neg\varphi \to \psi).$$

b) Buďte p, q různé prvovýroky. Pak:
Není $\models^{\mathsf{V}} (\neg p \to \neg q) \to (q \to p)$.
Axiom $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$ není $\{\mathrm{MP}\}$-odvozený z T.

Důkaz. a) MP-korektnost je zřejmá. $v^{\mathsf{V}}(\chi) = 1$ pro χ z $T \cup \{\varphi \to (\neg\varphi \to \psi)\}$ se zjistí propočtem. b) Buď $v(p) = 2$, $v(q) = 1$. Pak

$$v^{\mathsf{V}}((\neg p \to \neg q) \to (q \to p)) = (0 \to' 0) \to' (1 \to' 2) = 1 \to' 2 = 2.$$

Odtud a z 2.2.15 plyne, že axiom $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$ není $\{\mathrm{MP}\}$-odvozený z T.

2. Buď výroková evaluace $\underline{\mathsf{W}} = \langle 3, \neg'', \to'' \rangle$ dána takto ($\to''$ jako $\to'$ z 1.):

$\neg''$	
0	1
1	0
2	2

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

Platí:
a) $\underline{\mathsf{W}}$ je MP-korektní a $\models^{\mathsf{W}} T$.
b) Buďte p, q různé prvovýroky. Pak:
Není $\models^{\mathsf{W}} p \to (\neg p \to q)$.
Formule $p \to (\neg p \to q)$ není $\{\mathrm{MP}\}$-odvozená z T.
Je však $T \models^{\mathsf{V}} p \to (\neg p \to q)$.

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 $v^{\mathsf{W}}(p \to (\neg p \to q)) = 2 \to'' (\neg'' 2 \to'' 0) = 2 \to'' 0 = 0$. Odtud a z 2.2.15 plyne, že formule $p \to (\neg p \to q)$ není $\{\mathrm{MP}\}$-odvozená z T. Konečně $T \models^{\mathsf{V}} p \to (\neg p \to q)$ víme z 1. a).

Kapitola 3

Predikátová logika

Stručný obsah kapitoly.

- Základní syntax. Model jazyka, platnost v modelu, platnost v teorii. Dedukce. Teorémy logiky a pravidla dokazování. Prenexní tvar.
- Existence modelu. Věta o úplnosti a kompaktnosti.
- Extenze teorie definicemi.
-
-
-

Predikátová logika je základní a nejrozvinutější matematická verze logiky; její význam dokresluje i to, že v ní lze formulovat teorii množin, která je obecnou bází pro veškerou matematiku. Predikátová logika se zabývá dokazováním a zjišťováním pravdivosti tvrzení o individuích, přičemž je k dispozici predikování o individuích, operování s nimi a kvantifikování typu „každé individuum" a „existuje individuum" (symbolicky $(\forall x)$, $(\exists x)$), a dále logické spojky; tím spolu se spočetně proměnnými jakožto symbolizacemi individuí je dán jazyk L v predikátové logice a korelativně množina Fm_L jeho formulí. Predikátové logice se také říká *logika 1. řádu*, anglicky *first order logic*, neboť již nevypovídá navíc o systémech individuí, systémech systémů individuí atd., což přísluší logikám 2., 3. a dalších řádů.

Predikátová logika obsahuje výrokovou logiku, hledíme-li na formule jako na výroky nad množinou $\mathbb{P}$ prvovýroků, kterými jsou formule z Fm_L neobsahující logickou spojku nebo začínají kvantifikací (tvaru $(\forall x)$). Teorií rozumíme nějakou množinu $T \subseteq \mathrm{Fm}_L$ (axiomů). Na straně syntaxe je definován vztah „dokazatelnost formule φ v teorii T", formálně $T \vdash \varphi$, na straně sémantiky pak vztah „platnost formule φ v teorii T", formálně $T \models \varphi$. Základním rysem predikátové logiky je její úplnost: $T \vdash \varphi \Leftrightarrow T \models \varphi$; to plyne z tvrzení, že každá bezesporná teorie má model, odkud plyne i kompaktnost pro tuto logiku: teorie má model, má-li její každý konečný fragment model. Jelikož sémantické realizace neboli modely v predikátové logice jsou struktury 1. řádu (široce uplatňované v matematice), přináší logika řadu netriviálních tvrzení o nich. Zkoumání v tomto směru se označuje jako teorie modelů; zabývá se klasifikací modelů a strukturou třídy všech modelů dané teorie. Problém složitosti množiny $\mathrm{Thm}(T)$ všech v T dokazatelných formulí se posuzuje jednak co do efektivnosti $\mathrm{Thm}(T)$, jednak z hlediska deskriptivní složitosti formulí φ patřících do $\mathrm{Thm}(T)$. Deskriptivní složitost se základně měří počtem a typem kvantifikací v φ. V extrémním případě může být každá formule v T ekvivalentní formuli bezkvantifikátorové; pak říkáme, že T má eliminaci kvantifikátorů a lze říci, že T je deskriptivně jednoduchá. Efektivnost $\mathrm{Thm}(T)$ chápeme tak, že $\mathrm{Thm}(T)$ je rekurzivní, tj. je to po vhodném zakódování rekurzivní množina přirozených čísel. Přitom množina X přirozených čísel je rekurzivní, je-li její charakteristická funkce rekurzivní, neboli algoritmicky vyčíslitelná; to, zda $n \in \mathbb{N}$ patří do rekurzivní X, lze tedy zjistit algoritmicky. Je-li dán rekurzivní jazyk L a T je teorie v něm zapsaná, říkáme, že T je rozhodnutelná, je-li rekurzivní $\mathrm{Thm}(T)$.

Problematika klasifikace modelů, deskriptivní složitosti a (ne)rozhodnutelnosti pro různé teorie patří ke stěžejní problematice predikátové logiky.

3.1 Základy syntaxe a sémantiky

Základní syntax: Jazyk, termy, formule, teorie. Substituce.

3.1.1. Jazyk predikátové logiky.

1. *Jazyk* tvoří *logické symboly*, *mimologické symboly* a eventuálně *relační symbol rovnosti* $=$.

- Logické symboly jsou:
  - logické spojky $\neg, \rightarrow$,
  - *proměnné* tvořící spočetnou množinu Var,
  - *obecné kvantifikace* $\forall_x$ (proměnné) x s x z Var; $\forall_x$ čteme „pro každé x“.

Proměnné značíme často x, y, z s indexy, čárkami apod.

- Mimologické symboly jsou symboly nějaké signatury $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$, přičemž $\mathcal{R}, \mathcal{F}$ neobsahují žádný logický symbol ani $=$. Říkáme pak, že jde o *jazyk signatury* L; signatura může být prázdná. Symboly z $\mathcal{R}$ resp. $\mathcal{F}$ jsou *relační* (též *predikátové*) resp. *funkční symboly* jazyka L. Pro mimologický symbol S jazyka L řekneme, že jeho *typ v* L je relační resp. funkční, je-li to relační resp. funkční symbol jazyka L.

2. *Jazyk s rovností* je jazyk, který obsahuje predikátový symbol rovnosti $=$; jinak je to *jazyk bez rovnosti*. Vždy předpokládáme, že jazyk má alespoň jeden relační symbol.

Jazyk je tedy specifický jen svou signaturou L a tím, zda je jeho symbolem $=$. Říkáme proto, že jde o *jazyk* L, eventuálně navíc *s rovností*; jazyk v tomto smyslu ztotožňujeme s jeho signaturou.

3. *Velikost* čili *kardinalita* $\|L\|$ *jazyka* L je velikost signatury, je-li nekonečná a je spočetná jinak; formálně to je $\max(\omega, |L|)$, kde $|L|$ je velikost signatury L.

4. 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 S 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.

Jazyk L zapisujeme uvedením jeho signatury, často ve tvaru

$$\langle R_0, \ldots, F_0, \ldots, c_0, \ldots \rangle,$$

R_0 je m_0-ární relační symbol, ...,
F_0 je n_0-ární fukční symbol, ..., c_0 je konstantní symbol, ...

Nemusíme pak ani nejprve vypisovat relační a pak funkční symboly, ale můžeme je uvádět v libovolném pořadí, avšak tak, aby byly patrné četnosti. Například jazyk aritmetiky přirozených čísel L^A je jazyk s rovností, který zapisujeme jako $\langle \mathrm{S}, +, \cdot, 0, \leq \rangle$, S je unární funkční symbol, $+, \cdot$ jsou binární funkční symboly, 0 je konstantní symbol, $\leq$ je binární relační symbol.

ÚLOHA. Co lze říci o jazycích L_0, L_1, kde:

$L_0 = \langle +, < \rangle$, $+$ je binární funkční symbol, $<$ je binární relační symbol.
$L_1 = \langle +, < \rangle$, $+$ je binární relační symbol, $<$ je binární funkční symbol.

$L_2 = \langle +, <, 0 \rangle$, $\quad + $ je binární relační symbol, $<$ je binární funkční symbol, 0 je konstantní funkční symbol.

3.1.2. Termy a formule.

Pro daný jazyk L symbolicky reprezentují termy složené operace z funkčních symbolů jazyka L a formule pak tvrzení či vlastnosti, jež lze formulovat v L. Termy a formule budeme definovat jako designátory. K usnadnění čitelnosti designátorů používáme pomocně obvyklým způsobem delimitery (,). Dále zde užíváme často konvence, že designátor tvaru $\langle S \rangle$, kde S je symbol, „ztotožňujeme" s S.

Buď $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ jazyk.

1. Množina Term_L *termů jazyka* L čili L*-termů* je množina $\mathrm{D}(\mathrm{Var} \cup \mathcal{F})$ designátorů, kde každá proměnná představuje nulární funkční symbol. Má tedy induktivní definici s pravidly: Každé $\langle x \rangle$ s $x \in \mathrm{Var}$ je L-term. Je-li F z $\mathcal{F}$, n četnost F a $t_0, \ldots, t_{n-1}$ jsou L-termy, je $F(t_0, \ldots, t_{n-1})$ také L-term. Nadále zpravidla $\langle x \rangle$ s $x \in \mathrm{Var}$ zapisujeme jako x; proměnná je tak term.

2. Množina $\mathrm{A^pFm}_L$ *atomických L-preformulí* je tvořena právě designátory tvaru

$$R(t_0, \ldots, t_{n-1}), \tag{3.1}$$

kde R je predikátový symbol jazyka L, n je četnost R a $t_0, \ldots, t_{n-1}$ jsou L-termy.

Množina Fm_L *formulí jazyka* L čili L*-formulí* je množina

$$\mathrm{D}(\mathrm{A^pFm}_L \cup \{\neg, \rightarrow\} \cup \{\forall_x;\ x \in \mathrm{Var}\}),$$

kde symboly z $\mathrm{A^pFm}_L$ jsou nulární a každý symbol $\forall_x$ je unární. Má tedy induktivní definici s pravidly: Každé $\langle \eta \rangle$ s $\eta \in \mathrm{A^pFm}_L$ je L-formule. Jsou-li φ, ψ nějaké L-formule, jsou jimi i $\neg\varphi$, $\varphi \rightarrow \psi$ a $\forall_x(\varphi)$ pro každé x z Var.

Formule $\langle \eta \rangle$ s $\eta \in \mathrm{A^pFm}_L$ se nazývá *atomická L-formule.* Nadále ji zapisujeme zpravidla jako η, tj. ztotožňujeme ji s atomickou preformulí η. Množinu všech atomických L-formulí značíme AFm_L.

Buď např. $L = \langle \leq \rangle$, kde $\leq$ je binární relační symbol, x, y proměnné. Pak atomickou L-formuli $\langle x \leq y \rangle$ zapíšeme jako (atomickou preformuli) $x \leq y$. Dále například $\langle \forall_x, \rightarrow, x \leq y, x \leq y \rangle$ je formule, kterou zapíšeme v obvyklém tvaru jako $(\forall x)(x \leq y \rightarrow x \leq y)$ – viz též zkratky a konvence.

3. Je-li jazyk L patrný z kontextu či nevede-li to k nedorozumění, vynecháváme L. Říkáme tak například jen term, formule a píšeme jen Term, Fm apod., a to i v souvislosti s dále definovanými pojmy vztahujícími se k L.

4. *Podterm* resp. *podformule* termu resp. formule η je poddesignátor η. Výskyt proměnné x v (3.1) je výskyt x v nějakém t_i, $i < n$, nebo výskyt t_i v (3.1), je-li x term t_i, výskyt proměnné x ve formuli je výskyt x v nějaké její atomické podformuli. *Proměnná* uvedeného designátoru η je proměnná se v něm vyskytující. Term resp. formule je *bez proměnných*, neobsahuje-li žádnou proměnnou. Term bez proměnných se též nazývá *konstantní.*

Termy značíme nejčastěji, t, s, t', t_0 apod., formule pak φ, ψ, χ, φ', φ_0 apod.

Je patrné, že formule jazyka L 1. řádu jsou výroky nad prvovýroky $\mathbb{P}(L)$, kterými jsou právě všechny atomické a kvantifikátorem začínající L-formule.

TVRZENÍ 3.1.3. *Buď $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$ jazyk. Velikost množiny L-termů je* $\max(\omega, |\mathcal{F}|)$, *velikost množiny L-formulí je* $\|L\| = \max(\omega, |\mathcal{R}|, |\mathcal{F}|)$.

Důkaz. Termů je alespoň tolik, kolik je velikost množiny $\mathrm{Var} \cup \mathcal{F}$, což je $\max(\omega, |\mathcal{F}|)$. Dále jich není více, než je počet sekvencí ve $\mathrm{Var} \cup \mathcal{F}$; těch je také $\max(\omega, |\mathcal{F}|)$. Podobně je tomu s velikostí množiny všech formulí. $\square$

3.1.4. Zavedení &, $\vee$, $\leftrightarrow$, $\exists$ a další konvence o zápisu formulí.

• Logické spojky &, $\vee$, $\leftrightarrow$ *konjunkce, disjunkce, ekvivalence* zavádíme jako zkratky stejně jako ve výrokové logice. Užíváme i ostatní konvence z výrokové logiky.

• Formuli $\forall_x(\varphi)$ zapisujeme jako $(\forall x)\varphi$. Říkáme, že $\forall$ je *obecný* (*univerzální*) *kvantifikátor.*

$(\exists x)\varphi$ je zavedeno jako zkratka za $\neg(\forall x)\neg\varphi$; $(\exists x)$ je *existenční kvantifikace* (proměnné) x. $(\exists x)$ čteme „existuje x“. Říkáme, že $\exists$ je *existenční kvantifikátor*.

Je-li Q kvantifikátor, píšeme též $(Qx_1, \ldots, x_n)\varphi$ za $(Qx_1)(Qx_2)\ldots(Qx_n)\varphi$.

- Je-li $\diamond$ binární relační symbol, píše se též $t \not\diamond s$ za $\neg(t \diamond s)$.

ÚLOHA. Buď L jazyk s rovností, φ buď L-formule a $0 < n \in \mathbb{N}$.

Napište L-formule vyjadřující:

„existuje právě n prvků“, „existuje méně než n prvků“,
„existuje $\diamond n$ prvků“ s $\diamond \in \{<, \leq, >, \geq\}$.
„existuje právě n prvků x s vlastností $\varphi(x, \ldots)$“,
„prvků x s vlastností φ je $\diamond n$“ s $\diamond \in \{<, \leq, >, \geq\}$.

3.1.5. Teorie. Teorie rovnosti.

1. *Teorie* je dána jako jazyk L a množina $T \subseteq \mathrm{Fm}_L$; formule z T jsou *axiómy* a L jazyk takové teorie – formálně je teorie dvojice $\langle L, T\rangle$. Říkáme pak (tradičně), že T je *teorie v* L neboli L-*teorie* a její jazyk značíme $L(T)$; ten je ovšem určen jednoznačně. *Teorie s rovností* je taková teorie, jejíž jazyk je s rovností. Místo $L(T)$-formule se říká též *formule teorie* T. Teorie značíme často T, S, T', T_0 apod.

2. *Teorie rovnosti v* L je teorie $\mathrm{TE}_L = \emptyset$ v jazyce L s rovností, tj. teorie bez mimologických axiomů v jazyce L s rovností; je-li L prázdný jazyk s rovností, značíme $\mathrm{TE}_\emptyset$ jako PE a říkáme, že to je *teorie čisté rovnosti*.

Jakožto množiny axiomů jsou PE a TE_L totožné a prázdné, jako teorie však nikoli, neboť $L(\mathrm{PE}) \neq L(\mathrm{TE}_L)$, je-li signatura L neprázdná.

Buď T teorie TE_L, kde L je jazyk aritmetiky $L^A = \langle \mathrm{S}, +, \cdot, 0, \leq\rangle$(což je spočetný jazyk). Je zajímavé, že T je nerozhodnutelná teorie, avšak teorie PE je rozhodnutelná; to jsou již hlubší poznatky z matematické logiky.

3.1.6. Volné a vázané proměnné. Otevřené formule. Sentence. 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 může být zároveň volná i vázaná v nějaké formuli. Jsou-li proměnné x, y různé, tak volné výskyty x v $\neg\varphi$, $\varphi \to \psi$, $(\forall y)\varphi$ jsou právě volné výskyty ve 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. Formule je *otevřená* a též *bezkvantifikátorová*, není-li v ní žádný kvantifikátor. *(Generální) uzávěr* φ je formule $(\forall x_1, \ldots, x_n)\varphi$, kde mezi $x_1, \ldots, x_n$ jsou všechny volné proměnné formule φ. Množinu všech otevřených L-formulí značíme OFm_L.

Nápis

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

značí, že $\overline{x} = \langle x_0, \ldots, x_{n-1}\rangle$ je prostá sekvence proměnných a mezi $x_0, \ldots, x_{n-1}$ jsou všechny proměnné termu t resp. všechny volné proměnné formule φ.

3.1.7. 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

$$\varphi(x_1/t_1, \ldots, x_n/t_n)$$

a získána z φ nahražením všech volných výskytů $x_1, \ldots, x_n$ za $t_1, \ldots, t_n$, přičemž $x_1, \ldots, x_n$ jsou různé proměnné, term t_i je substituovatelný za x_i do φ pro $i = 1, \ldots, n$ a substituce se provádí simultánně. Formule $\varphi(x_1/t_1)(x_2/t_2)\cdots(x_n/t_n)$ získána postupně prováděnou substitucí tedy není obecně instance φ.

Obdobně $t(x_1/t_1, \ldots, x_n/t_n)$ značí term získaný z termu t simultánním nahražením všech výskytů $x_1, \ldots, x_n$ za $t_1, \ldots, t_n$, přičemž $x_1, \ldots, x_n$ jsou různé proměnné. Výsledkem je term, jak plyne z tvrzení o substituci v designátorech.

Místo $\varphi(x_1/t_1, \ldots, x_n/t_n)$ resp. $t(x_1/t_1, \ldots, x_n/t_n)$ píšeme též, nevede-li to k nedorozumění, jen

$$\varphi(t_1, \ldots, t_n) \text{ resp. } t(t_1, \ldots, t_n).$$

Poznamenejme, že $\varphi(x_1/t_1, \ldots, x_n/t_n)$ můžeme získat postupně prováděnou substitucí t_i za x'_i do $\varphi(x_1/x'_1, \ldots, x_n/x'_n)$, kde $x'_1, \ldots, x'_n$ jsou různé a nevyskytují ani ve φ ani v žádném t_i. 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, tedy např. nemá výskyt ve ψ).

POZNÁMKA 3.1.8.

1. Substituovatelnost vyjadřuje korektnost substituce; ta má např. zaručit platnost formule $(\forall x)\varphi \to \varphi(x/t)$. Pokud nahradíme všechny volné výskyty x termem t i tehdy, kdy term t není substituovatelný za x do φ, nemusí uvedená implikace platit. Buď totiž např. $\varphi(x)$ tvaru $(\exists y)(x \neq y)$ s různými x, y. Pak $(\forall x)\varphi$ platí např. v oboru individuí $A = \{0, 1\}$ s $=$ interpretovaným jako identita, tj. platí ve struktuře $\langle A \rangle$. Avšak po nekorektní substituci termu t rovnému y za x do φ získáme $(\exists y)(y \neq y)$ a tato formule neplatí v $\langle A \rangle$. Tedy ani $(\forall x)\varphi \to (\exists y)(y \neq y)$ neplatí v $\langle A \rangle$.

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 rovnost 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 $(\forall x < y)(x < y)$ & $x + 0 = x$ s různými x, y, je x volná i vázaná. Buď x' proměnná různá od x, y. Pak je formule $(\forall x')(x' < y)$ & $x + 0 = x$ varianta φ, ve které není žádná proměnná zároveň vázaná i volná.