Matematická logika

přednáška šestá

Miroslav Kolařík

Zpracováno dle textu R. Bělohlávka:
Matematická logika – poznámky k přednáškám, 2004.

a dle učebního textu R. Bělohlávka a V. Vychodila:
Diskrétní matematika pro informatiky II, Olomouc 2006.

Obsah

Jazyk PL je určen svými relačními a funkčními symboly spolu s definicí jejich arity. Z těchto symbolů spolu se symboly proměnných, logických spojek, kvantifikátorů a pomocných symbolů se skládají termy a formule daného jazyka. Samotné termy a formule jsou syntaktické pojmy a nemají žádný význam (tj. term sám o sobě nemá žádnou hodnotu, formule sama o sobě nemá žádnou pravdivostní hodnotu). To je například dobře patrné u termu $x + 0$: abychom mohli uvažovat hodnotu tohoto termu, musí mít přiřazenu nějakou hodnotu proměnná x a dále musíme interpretovat symboly $+$ a 0.

Interpretací funkčních a relačních symbolů se zabývá sémantika PL (ta přiřazuje význam funkčním a relačním symbolům). Poznamenejme ještě, že interpretaci proměnných definuje tzv. ohodnocení proměnných (viz dále).

Intuitivní pojem interpretace jazyka nyní přesně zavedeme:

Definice

Struktura pro jazyk typu $\langle R, F, \sigma \rangle$ je trojice $\mathbf{M} = \langle M, R^{\mathbf{M}}, F^{\mathbf{M}} \rangle$, která sestává z neprázdné množiny M a dále z množin

$$R^{\mathbf{M}} = \{ r^{\mathbf{M}} \subseteq M^n \mid r \in R, \sigma(r) = n \},$$

$$F^{\mathbf{M}} = \{ f^{\mathbf{M}} : M^n \to M \mid f \in F, \sigma(f) = n \}.$$

Pokud $\approx \in R$, pak $\approx$ interpretujeme vždy relací identity, tj. $\approx^{\mathbf{M}} = \omega_M = \{ \langle u, u \rangle \mid u \in M \}$.

Jinými slovy, struktura $\mathbf{M}$ pro jazyk typu $\langle R, F, \sigma \rangle$ je systém relací a funkcí na jisté množině M, přitom ke každému n-árnímu relačnímu symbolu $r \in R$ je ve struktuře $\mathbf{M}$ odpovídající n-ární relace $r^{\mathbf{M}} \in R^{\mathbf{M}}$ na M a ke každému n-árnímu funkčnímu symbolu $f \in F$ je ve struktuře $\mathbf{M}$ odpovídající n-ární funkce $f^{\mathbf{M}} \in F^{\mathbf{M}}$ v M. Nehrozí-li nebezpečí nedorozumění, budeme někdy vynechávat horní indexy a místo $r^{\mathbf{M}}$ a $f^{\mathbf{M}}$ budeme psát jen r a f.

Příklad

Uvažujme jazyk typu $\langle R, F, \sigma \rangle$, kde $R = \{p, \leq\}$, $F = \{c, \circ\}$, c je nulární, p je unární, $\leq$ a $\circ$ jsou binární. Nechť $M = \mathbb{Z}$.
Definujme relace $p^{\mathbf{M}}$ (unární, tj. podmnožina M), $\leq^{\mathbf{M}}$ a funkce $c^{\mathbf{M}}$ (nulární, tj. vybraný prvek z M) a $\circ^{\mathbf{M}}$ následovně:

$$p^{\mathbf{M}} = \{m \in M \mid m \text{ je větší nebo rovno nule}\},$$

$$\leq^{\mathbf{M}} = \{\langle m_1, m_2 \rangle \in M \times M \mid m_1 \text{ je menší nebo rovno } m_2\},$$

$$c^{\mathbf{M}} = 0, \quad m_1 \circ^{\mathbf{M}} m_2 = m_1 + m_2,$$

tj. $c^{\mathbf{M}}$ je číslo nula a $\circ^{\mathbf{M}}$ je operace sčítání celých čísel.

Jinou strukturu pro stejný jazyk dostaneme, pokud změníme výše uvedenou strukturu tak, že $c^{\mathbf{M}} = 1$, případně ještě definujeme $m_1 \circ^{\mathbf{M}} m_2 = m_1 \cdot m_2$ (násobení celých čísel).

Další strukturou (opět) pro stejný jazyk je struktura s nosičem $M = \{a, b\}$, $p^{\mathbf{M}} = \{a, b\}$, $\leq^{\mathbf{M}} = \{\langle a, a \rangle, \langle b, b \rangle, \langle b, a \rangle\}$, $c^{\mathbf{M}} = b$ a s operací $\circ^{\mathbf{M}}$ definovanou tabulkou:

$\circ^{\mathbf{M}}$	a	b
a	a	b
b	a	a

.

Jak tedy vidíme, k danému jazyku PL existuje nekonečně mnoho struktur. Variabilita je dána jednak nosičem M, který může mít libovolný (nenulový) počet prvků, dále každý relační symbol r může být interpretován libovolnou relací $r^{\mathbf{M}}$ příslušné arity a konečně každý funkční symbol f může být interpretován libovolnou funkcí $f^{\mathbf{M}}$ příslušné arity.

Nechť **M** je struktura pro jazyk typu $\langle R, F, \sigma \rangle$. **M-ohodnocení proměnných** (krátce jen **M-ohodnocení**, popř. jen **ohodnocení**) je zobrazení v přiřazující každé proměnné x prvek $v(x) \in M$. Jsou-li v a v' ohodnocení a x je proměnná, píšeme $v =_x v'$ pokud pro každou proměnnou $y \neq x$ je $v(y) = v'(y)$, tj. v a v' se liší nejvýše v tom, jakou hodnotu přiřazují proměnné x.

Definice

Nechť v je **M**-ohodnocení. **Hodnota $\| \mathbf{t} \|_{\mathbf{M},\mathbf{v}}$ termu t v M při v** je definována

$$\| t \|_{\mathbf{M},v} = \begin{cases} v(x), & \text{je-li } t \text{ proměnná } x \\ f^{\mathbf{M}}(\| t_1 \|_{\mathbf{M},v}, \ldots, \| t_k \|_{\mathbf{M},v}), & \text{je-li } t \text{ tvaru } f(t_1, \ldots, t_k). \end{cases}$$

Uvědomme si, že při dané struktuře **M** a při daném **M**-ohodnocení v je každému termu t přiřazena právě jedna hodnota $\| t \|_{\mathbf{M},v}$ z univerza M. Dále je patrné, že hodnota $\| t \|_{\mathbf{M},v}$ nezávisí na hodnotách přiřazených ohodnocením v těm proměnným, které se v t nevyskytují (lze dokázat jednoduše strukturální indukcí).

Příklad

Uvažujme jazyk typu $\langle\{p,\leq\},\{c,\circ\},\sigma\rangle$, kde $\sigma(c)=0$, $\sigma(p)=1$, $\sigma(\leq)=\sigma(\circ)=2$. Nechť $M=\mathbb{Z}$. Definujme relace $p^{\mathbf{M}}$, $\leq^{\mathbf{M}}$ a funkce $c^{\mathbf{M}}$ a $\circ^{\mathbf{M}}$ následovně:

$$p^{\mathbf{M}}=\{m\in M \mid m \text{ je větší nebo rovno nule}\},$$

$$\leq^{\mathbf{M}}=\{\langle m_1,m_2\rangle\in M\times M \mid m_1 \text{ je menší nebo rovno } m_2\},$$

$$c^{\mathbf{M}}=0,\quad m_1\circ^{\mathbf{M}} m_2=m_1+m_2.$$

Vezmeme-li v této struktuře term $(x\circ(c\circ y))\circ x$, pak při ohodnocení v, kde $v(x)=10$, $v(y)=50$ máme

$\| (x\circ(c\circ y))\circ x \|_{\mathbf{M},v}=\| x\circ(c\circ y) \|_{\mathbf{M},v}+\| x \|_{\mathbf{M},v}=$
$=(\| x \|_{\mathbf{M},v}+\| c\circ y \|_{\mathbf{M},v})+\| x \|_{\mathbf{M},v}=$
$=(\| x \|_{\mathbf{M},v}+(\| c \|_{\mathbf{M},v}+\| y \|_{\mathbf{M},v}))+\| x \|_{\mathbf{M},v}=$
$=(v(x)+(c^{\mathbf{M}}+v(y)))+v(x)=(10+(0+50))+10=70.$

Dále definujeme pravdivostní hodnotu formule ve struktuře při daném ohodnocení.

Definice

Pravdivostní hodnota $\| \varphi \|_{\mathbf{M},\mathbf{v}}$ **formule** φ **při M-ohodnocení v** je definována následovně:

(i) pro atomické formule

$$\| r(t_1,\ldots,t_n) \|_{\mathbf{M},v} = \begin{cases} 1, & \text{je-li } \langle \| t_1 \|_{\mathbf{M},v},\ldots,\| t_n \|_{\mathbf{M},v} \rangle \in r^{\mathbf{M}} \\ 0, & \text{jinak} \end{cases}$$

(ii) pro formule φ ve tvaru $\neg\alpha$ a $\alpha \Rightarrow \beta$

$$\| \neg\alpha \|_{\mathbf{M},v} = \begin{cases} 1, & \text{pokud } \| \alpha \|_{\mathbf{M},v} = 0 \\ 0, & \text{pokud } \| \alpha \|_{\mathbf{M},v} = 1 \end{cases}$$

$$\| \alpha \Rightarrow \beta \|_{\mathbf{M},v} = \begin{cases} 1, & \text{pokud } \| \alpha \|_{\mathbf{M},v} = 0 \text{ nebo} \\ & \| \beta \|_{\mathbf{M},v} = 1 \\ 0, & \text{jinak} \end{cases}$$

(iii) pro kvantifikovanou formuli φ

$$\| (\forall x)\varphi \|_{\mathbf{M},v} = \begin{cases} 1, & \text{pokud pro každé } v' \text{ takové, že} \\ & v' =_x v \text{ je } \| \varphi \|_{\mathbf{M},v'} = 1 \\ 0, & \text{jinak.} \end{cases}$$

Je-li $\| \varphi \|_{\mathbf{M},v} = 1$ ($\| \varphi \|_{\mathbf{M},v} = 0$), říkáme, že formule φ je **pravdivá** (**nepravdivá**) **ve struktuře M při ohodnocení v.**

Stejně jako u ohodnocení termů je (při daných **M** a v) každé formuli φ přiřazena právě jedna hodnota $\| \varphi \|_{\mathbf{M},v}$.

Strukturální indukcí lze jednoduše dokázat, že hodnota $\| \varphi \|_{\mathbf{M},v}$ nezávisí na hodnotách přiřazených ohodnocením v proměnným, které se ve φ nevyskytují.

Uvědomme si, že říct: "formule φ je pravdivá" nemá smysl, protože pravdivost φ vztahujeme vždy k nějaké struktuře při některém ohodnocení proměnných.
Běžně sice říkáme např. "formule $(\forall x)(\forall y)x \leq x + \mathrm{abs}(y)$ je pravdivá", ale to je způsobeno tím, že implicitně nějakou strukturu předpokládáme dle kontextu, ve kterém formuli uvažujeme. Např. v matematické analýze jde většinou o číselné struktury, např. reálná čísla s běžnými relacemi ("menší nebo rovno") a operacemi ("sčítání reálných čísel", "absolutní hodnota").

Nyní budeme zkoumat platnost formulí ve struktuře "přes všechna ohodnocení" a platnost formulí "přes všechny struktury".

Definice

Formule φ se nazývá **tautologie ve struktuře** (**pravdivá ve struktuře**) **M**, jestliže $\| \varphi \|_{\mathbf{M},v} = 1$ pro každé **M**-ohodnocení v.
Formule φ se nazývá **tautologie**, jestliže je φ tautologie v každé struktuře **M**.

Formule φ je tedy tautologie, jestliže pro libovolnou strukturu **M** a libovolné ohodnocení v je $\| \varphi \|_{\mathbf{M},v} = 1$.

Definice

Teorie v jazyku PL typu $\langle R, F, \sigma \rangle$ je libovolná množina T formulí jazyka tohoto typu. Struktura **M** jazyka typu $\langle R, F, \sigma \rangle$ se nazývá **model teorie** T (píšeme $\mathbf{M} \models T$, popř. $\| T \|_{\mathbf{M}} = 1$), jestliže každá formule z T je pravdivá v **M**.

Poznámka: Teorie formalizuje soubor předpokladů. Pojem teorie je zcela přirozený. Běžně se říká "S tvojí teorií nesouhlasím." apod. Přitom teorií rozumíme soubor tvrzení, které daná osoba zastává. Soubor tvrzení v PL představuje množina formulí. Též pojem model je přirozený a vyskytuje se v běžné komunikaci. Například obratem "Představme si modelovou situaci, kdy ..." chceme vyjádřit, abychom se soustředili na nějaký konkrétní model jisté teorie.

Příklad

Uvažujme jazyk $\mathscr{J}$ typu $\langle R, F, \sigma \rangle$, kde $R = \{r\}$, $F = \emptyset$ a $\sigma(r) = 2$. Struktury pro $\mathscr{J}$ jsou $\mathbf{M} = \langle M, \{r^{\mathbf{M}}\}, \emptyset \rangle$, kde $r^{\mathbf{M}}$ je binární relace na M (tedy struktury jsou vlastně binární relace na M). Struktura $\mathbf{M}$ je modelem teorie $T = \{(\forall x) r(x,x), (\forall x,y,z)((r(x,y) \wedge r(y,z)) \Rightarrow r(x,z))\}$, právě když je relace $r^{\mathbf{M}}$ reflexivní a tranzitivní.

Poznámka: Některé teorie nemají model.

Příklad

Mějme jazyk typu $\langle R, F, \sigma \rangle$, kde $R = \{r\}$, $F = \emptyset$ a r je unární. Teorie $T = \{(\forall x)r(x), (\exists x)\neg r(x)\}$ zřejmě nemá žádný model.

Nyní zavedeme sémantické vyplývání v PL.

Definice

Množina S formulí **sémanticky plyne** z množiny T formulí (píšeme $T \models S$; píšeme také $T \models \varphi$, jestliže $S = \{\varphi\}$, podobně když $T = \{\psi\}$), jestliže každý model T je modelem S.

Tedy $T \models S$, právě když v každé struktuře, ve které jsou pravdivé všechny formule z T, jsou také pravdivé všechny formule z S.

Všimněme si, že pojem sémantického vyplývání je zaveden analogicky jako v případě VL, jen místo "pravdivostních ohodnocení" používáme z pochopitelných důvodů pojem model.
Dále platí, že φ je tautologie, právě když $\models \varphi$.

Vidíme i jak prokázat, že daná formule φ sémanticky neplyne z teorie T. Stačí najít jediný model $\mathbf{M} \models T$ a **M**-ohodnocení v takové, že $\| \varphi \|_{\mathbf{M},v} = 0$ (což nemusí být vůbec jednoduché).
Podotkněme ještě, že daleko větším problémem je ověření, zda-li φ z T sémanticky plyne.

Příklad

Formule $\varphi = (\forall x, y, z, w)((r(x, y) \wedge r(y, z) \wedge r(z, w)) \Rightarrow r(x, w))$ sémanticky plyne z formule
$\psi = (\forall x, y, z)((r(x, y) \wedge r(y, z)) \Rightarrow r(x, z))$, tj. $\psi \models \varphi$. Obrácené vyplývání, tj. $\varphi \models \psi$, neplatí.

Příklad

Následující tautologie vyjadřují záměnu pořadí kvantifikátorů:

$$\models (\forall x)(\forall y)\varphi \Leftrightarrow (\forall y)(\forall x)\varphi,$$

$$\models (\exists x)(\exists y)\varphi \Leftrightarrow (\exists y)(\exists x)\varphi,$$

$$\models (\exists x)(\forall y)\varphi \Rightarrow (\forall y)(\exists x)\varphi.$$

Ukažme, že implikaci ve 3. tautologii nelze obrátit. Uvažujme jazyk typu $\langle R, \emptyset, \sigma\rangle$, kde $R = \{r\}$, $\sigma(r) = 2$ a strukturu tohoto jazyka $\mathbf{M} = \langle M, \{r^{\mathbf{M}}\}, \emptyset\rangle$, kde $M = \{a, b\}$ a relace $r^{\mathbf{M}}$ je definována $r^{\mathbf{M}} = \{\langle a, b\rangle, \langle b, a\rangle\}$. Ve struktuře **M** máme $\| (\forall y)(\exists x)r(x, y) \|_{\mathbf{M},v} = 1$ při libovolném ohodnocení v. Na druhou stranu však $\| (\exists x)(\forall y)r(x, y) \|_{\mathbf{M},v} = 0$, tj. máme model, ve kterém není $(\forall y)(\exists x)\varphi \Rightarrow (\exists x)(\forall y)\varphi$ pravdivá.