Výroková a predikátová logika - VII

Petr Gregor

KTIML MFF UK

ZS 2020/21

Nesplnitelnost a pravdivost

Problém pravdivosti v teorii lze převést na problém existence modelu.

Tvrzení *Pro každou teorii T a sentenci φ (stejného jazyka)*

$$T, \neg\varphi \text{ nemá model} \quad \Leftrightarrow \quad T \models \varphi.$$

Důkaz Z definic plynou ekvivalence následujících tvrzení.

(1) $T, \neg\varphi$ nemá model,

(2) $\neg\varphi$ neplatí v žádném modelu teorie T,

(3) φ platí v každém modelu teorie T,

(4) $T \models \varphi$. $\square$

Poznámka *Předpoklad, že φ je sentence, je nutný pro $(2) \Rightarrow (3)$.*

Např. teorie $\{P(c), \neg P(x)\}$ nemá model, ale $P(c) \not\models P(x)$, kde P je unární relační symbol a c je konstantní symbol.

Základní algebraické teorie - příklady

- *Teorie grup* nad jazykem $L = \langle +, -, 0\rangle$ s rovností má axiomy

  $x + (y + z) = (x + y) + z$ (asociativita $+$)

  $0 + x = x = x + 0$ (neutralita 0 k $+$)

  $x + (-x) = 0 = (-x) + x$ ($-x$ je inverzní prvek k x)

- *Teorie komutativních grup* má navíc ax. $x + y = y + x$ (komutativita $+$)
- *Teorie okruhů* je jazyka $L = \langle +, -, \cdot, 0, 1\rangle$ s rovností, má navíc axiomy

  $1 \cdot x = x = x \cdot 1$ (neutralita 1 k $\cdot$)

  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (asociativita $\cdot$)

  $x \cdot (y + z) = x \cdot y + x \cdot z,\ (x + y) \cdot z = x \cdot z + y \cdot z$ (distributivita $\cdot$ k $+$)

- *Teorie komutativních okruhů* má navíc ax. $x \cdot y = y \cdot x$ (komutativita $\cdot$)
- *Teorie těles* stejného jazyka má navíc axiomy

  $x \neq 0 \rightarrow (\exists y)(x \cdot y = 1)$ (existence inverzního prvku k $\cdot$)

  $0 \neq 1$ (netrivialita)

Vlastnosti teorií

Teorie T jazyka L je *(sémanticky)*

- *sporná*, jestliže v ní platí $\perp$ (spor), jinak je *bezesporná* (*splnitelná*),
- *kompletní*, jestliže není sporná a každá sentence je v ní pravdivá či lživá,
- *extenze* teorie T' jazyka L', jestliže $L' \subseteq L$ a $\theta^{L'}(T') \subseteq \theta^{L}(T)$,
  o extenzi T teorie T' řekneme, že je *jednoduchá*, pokud $L = L'$, a *konzervativní*, pokud $\theta^{L'}(T') = \theta^{L}(T) \cap \mathrm{Fm}_{L'}$,
- *ekvivalentní* s teorií T', jestliže T je extenzí T' a T' je extenzí T,

Struktury $\mathcal{A}$, $\mathcal{B}$ pro jazyk L jsou *elementárně ekvivalentní*, značeno $\mathcal{A} \equiv \mathcal{B}$, platí-li v nich stejné formule.

Pozorování *Nechť T a T' jsou teorie jazyka L. Teorie T je (sémanticky)*

(1) *bezesporná, právě když má model,*

(2) *kompletní, právě když má až na elementární ekvivalenci jediný model,*

(3) *extenze T', právě když $M(T) \subseteq M(T')$,*

(4) *ekvivalentní s T', právě když $M(T) = M(T')$.*

Podstruktura

Nechť $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ a $\mathcal{B} = \langle B, \mathcal{R}^B, \mathcal{F}^B \rangle$ jsou struktury pro jazyk $L = \langle \mathcal{R}, \mathcal{F} \rangle$.

Řekneme, že $\mathcal{B}$ je (indukovaná) *podstruktura* $\mathcal{A}$, značeno $\mathcal{B} \subseteq \mathcal{A}$, pokud

(i) $B \subseteq A$,

(ii) $R^B = R^A \cap B^{\mathrm{ar}(R)}$ pro každé $R \in \mathcal{R}$,

(iii) $f^B = f^A \cap (B^{\mathrm{ar}(f)} \times B)$, tj. $f^B = f^A \restriction B^{\mathrm{ar}(f)}$, pro každé $f \in \mathcal{F}$.

Pozorování *Množina $C \subseteq A$ je doménou nějaké podstruktury struktury $\mathcal{A}$, právě když C je uzavřená na všechny funkce struktury $\mathcal{A}$ (včetně konstant).*

- Pak příslušnou podstrukturu značíme $\mathcal{A} \restriction C$ a říkáme, že je to *restrikce* (*parcializace*) struktury $\mathcal{A}$ na C.
- Množina $C \subseteq A$ je *uzavřená* na funkci $f\colon A^n \to A$, pokud $f(x_0, \ldots, x_{n-1}) \in C$ pro každé $x_0, \ldots, x_{n-1} \in C$.

Např. $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, \cdot, 0 \rangle$ *je podstrukturou* $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, \cdot, 0 \rangle$ *a lze psát* $\underline{\mathbb{Z}} = \underline{\mathbb{Q}} \restriction \mathbb{Z}$.
Dále $\underline{\mathbb{N}} = \langle \mathbb{N}, +, \cdot, 0 \rangle$ *je jejich podstrukturou a* $\underline{\mathbb{N}} = \underline{\mathbb{Q}} \restriction \mathbb{N} = \underline{\mathbb{Z}} \restriction \mathbb{N}$.

Platnost v podstruktuře

Nechť $\mathcal{B}$ je podstruktura struktury $\mathcal{A}$ pro (pevný) jazyk L.

Tvrzení *Pro každou otevřenou formuli φ a ohodnocení $e\colon \mathrm{Var} \to B$ platí*

$$\mathcal{B} \models \varphi[e] \quad \textit{právě když} \quad \mathcal{A} \models \varphi[e].$$

Důkaz Je-li φ atomická, plyne tvrzení z definice platnosti při ohodnocení. Dále snadno indukcí dle struktury formule. $\square$

Důsledek *Otevřená formule platí ve struktuře $\mathcal{A}$, právě když platí v každé podstruktuře $\mathcal{B} \subseteq \mathcal{A}$.*

- Teorie T je *otevřená*, jsou-li všechny její axiomy otevřené formule.

Důsledek *Každá podstruktura modelu otevřené teorie T je modelem T.*

Např. každá podstruktura grafu, tj. modelu teorie grafů, je rovněž grafem, zveme ho podgraf. Obdobně např. podgrupa nebo Booleova podalgebra.

Generovaná podstruktura, expanze, redukt

Nechť $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ je struktura a $X \subseteq A$. Označme B nejmenší podmnožinu množiny A obsahující X, která je uzavřená na všechny funkce struktury $\mathcal{A}$ (včetně konstant). Pak strukturu $\mathcal{A} \restriction B$ značíme rovněž $\mathcal{A}\langle X \rangle$ a podstruktura říkáme, že je to $\mathcal{A}$ *generovaná* množinou X.

Např. pro $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, \cdot, 0 \rangle$, $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, \cdot, 0 \rangle$ *a* $\underline{\mathbb{N}} = \langle \mathbb{N}, +, \cdot, 0 \rangle$ *je* $\underline{\mathbb{Q}}\langle \{1\} \rangle = \underline{\mathbb{N}}$, $\underline{\mathbb{Q}}\langle \{-1\} \rangle = \underline{\mathbb{Z}}$ *a* $\underline{\mathbb{Q}}\langle \{2\} \rangle$ *je podstruktura na všech sudých přirozených číslech.*

Nechť $\mathcal{A}'$ je struktura pro jazyk L' a $L \subseteq L'$ je jazyk. Odebráním realizací symbolů, jež nejsou v L, získáme z $\mathcal{A}'$ strukturu $\mathcal{A}$, kterou nazýváme *redukt* struktury $\mathcal{A}'$ na jazyk L. Obráceně, $\mathcal{A}'$ je *expanze* struktury $\mathcal{A}$ do jazyka L'.

Např. $\langle \mathbb{N}, + \rangle$ *je redukt* $\langle \mathbb{N}, +, \cdot, 0 \rangle$. *Naopak, struktura* $\langle \mathbb{N}, +, c_i \rangle_{i \in \mathbb{N}}$ *taková, že* $c_i = i$ *pro všechna* $i \in \mathbb{N}$, *je expanze* $\langle \mathbb{N}, + \rangle$ *o jména prvků z* $\mathbb{N}$.

Věta o konstantách

Věta *Nechť φ je formule jazyka L s volnými proměnnými $x_1, \ldots, x_n$ a T je teorie jazyka L. Označme L' rozšíření L o nové konstantní symboly $c_1, \ldots, c_n$ a T' teorii T nad jazykem L'. Pak*

$$T \models \varphi \quad \text{právě když} \quad T' \models \varphi(x_1/c_1, \ldots, x_n/c_n).$$

Důkaz ($\Rightarrow$) Je-li $\mathcal{A}'$ model teorie T', nechť $\mathcal{A}$ je redukt $\mathcal{A}'$ na L. Jelikož $\mathcal{A} \models \varphi[e]$ pro každé ohodnocení e, platí i

$$\mathcal{A} \models \varphi[e(x_1/c_1^{A'}, \ldots, x_n/c_n^{A'})], \quad \text{tj. } \mathcal{A}' \models \varphi(x_1/c_1, \ldots, x_n/c_n).$$

($\Leftarrow$) Je-li $\mathcal{A}$ model teorie T a e ohodnocení, nechť $\mathcal{A}'$ je expanze $\mathcal{A}$ na L' o konstanty $c_i^{A'} = e(x_i)$ pro všechna i. Jelikož $\mathcal{A}' \models \varphi(x_1/c_1, \ldots, x_n/c_n)[e']$ pro libovolné ohodnocení e', platí i

$$\mathcal{A}' \models \varphi[e(x_1/c_1^{A'}, \ldots, x_n/c_n^{A'})], \quad \text{tj. } \mathcal{A} \models \varphi[e]. \quad \square$$

Definovatelné množiny

Zajímá nás, které množiny lze v dané struktuře zadefinovat.

- *Množina definovaná formulí* $\varphi(x_1, \dots, x_n)$ *ve struktuře* $\mathcal{A}$ je množina
$$\varphi^{\mathcal{A}}(x_1, \dots, x_n) = \{(a_1, \dots, a_n) \in A^n \mid \mathcal{A} \models \varphi[e(x_1/a_1, \dots, x_n/a_n)]\}.$$
Zkráceným zápisem, $\varphi^{\mathcal{A}}(\overline{x}) = \{\overline{a} \in A^{|\overline{x}|} \mid \mathcal{A} \models \varphi[e(\overline{x}/\overline{a})]\}$, kde $|\overline{x}| = n$.
- *Množina definovaná formulí* $\varphi(\overline{x}, \overline{y})$ *s parametry* $\overline{b} \in A^{|\overline{y}|}$ *ve struktuře* $\mathcal{A}$ je
$$\varphi^{\mathcal{A}, \overline{b}}(\overline{x}, \overline{y}) = \{\overline{a} \in A^{|\overline{x}|} \mid \mathcal{A} \models \varphi[e(\overline{x}/\overline{a}, \overline{y}/\overline{b})]\}.$$
Např. pro $\varphi = E(x, y)$ *je* $\varphi^{\mathcal{G}, b}(x, y)$ *množina sousedů vrcholu* b *v grafu* $\mathcal{G}$.
- Pro strukturu $\mathcal{A}$, množinu $B \subseteq A$ a $n \in \mathbb{N}$ označme $\mathrm{Df}^n(\mathcal{A}, B)$ třídu všech množin $D \subseteq A^n$ definovatelných ve struktuře $\mathcal{A}$ s parametry z B.

Pozorování $\mathrm{Df}^n(\mathcal{A}, B)$ *je uzavřená na doplněk, sjednocení, průnik a obsahuje* $\emptyset$, A^n. *Tedy tvoří podalgebru potenční algebry* $\underline{\mathcal{P}}(A^n)$.

Příklad - databázové dotazy

Filmy	*název*	*režisér*	*herec*
	Lidé z Maringotek	M. Frič	J. Tříska
	Po strništi bos	J. Svěrák	Z. Svěrák
	Po strništi bos	J. Svěrák	J. Tříska
	...	...	...

Program	*kino*	*název*	*čas*
	Světozor	Po strništi bos	13:15
	Mat	Po strništi bos	16:15
	Mat	Lidé z Maringotek	18:30
	...	...	...

Kde a kdy mohu dnes vidět film s Janem Třískou?

select *Program.kino, Program.čas* **from** *Filmy, Program*
where *Filmy.název = Program.název* **and** *herec* = 'J. Tříska';

Totéž dostaneme jako množinu $\varphi^{\mathcal{D}}(x,y)$ definovanou formulí $\varphi(x,y)$

$$(\exists n)(\exists r)(P(x,n,y) \wedge F(n,r,\text{'J. Tříska'}))$$

ve struktuře $\mathcal{D} = \langle D, \mathit{Filmy}, \mathit{Program}, c^D\rangle_{c\in D}$ jazyka $L = \langle F, P, c\rangle_{c\in D}$, kde $D = \{\text{'Po strništi bos', 'J. Tříska', 'Mat', '13:15'}, \dots\}$ a $c^D = c$ pro každé $c \in D$.

Booleovy algebry

Teorie *Booleových algeber* jazyka $L = \langle -, \wedge, \vee, 0, 1\rangle$ s rovností má axiomy

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \qquad \text{(asociativita } \wedge\text{)}$$
$$x \vee (y \vee z) = (x \vee y) \vee z \qquad \text{(asociativita } \vee\text{)}$$
$$x \wedge y = y \wedge x \qquad \text{(komutativita } \wedge\text{)}$$
$$x \vee y = y \vee x \qquad \text{(komutativita } \vee\text{)}$$
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \qquad \text{(distributivita } \wedge \text{ k } \vee\text{)}$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \qquad \text{(distributivita } \vee \text{ k } \wedge\text{)}$$
$$x \wedge (x \vee y) = x, \quad x \vee (x \wedge y) = x \qquad \text{(absorbce)}$$
$$x \vee (-x) = 1, \quad x \wedge (-x) = 0 \qquad \text{(komplementace)}$$
$$0 \neq 1 \qquad \text{(netrivialita)}$$

Nejmenší model je $\underline{2} = \langle 2, -_1, \wedge_1, \vee_1, 0, 1\rangle$. Konečné Booleovy algebry jsou (až na izomorfismus) právě $\underline{^n2} = \langle {}^n2, -_n, \wedge_n, \vee_n, 0_n, 1_n\rangle$ pro $n \in \mathbb{N}^+$, kde jednotlivé operace *(na binárních n-ticích)* jsou operace z $\underline{2}$ *“po složkách”*.

Vztah výrokové a predikátové logiky

- Výrokové formule s (*univerzálními*) spojkami $\neg$, $\wedge$, $\vee$ (případně s $\top$, $\bot$) lze považovat za Booleovské termy. Hodnota výroku φ při daném ohodnocení je pak hodnotou termu v Booleově algebře $\underline{2}$.
- Algebra výroků nad $\mathbb{P}$ je Booleova algebra (i pro $\mathbb{P}$ nekonečné).
- Reprezentujeme-li atomické formule v otevřené formuli φ (bez rovnosti) pomocí prvovýroků, získame výrokovou formuli, která je pravdivá, právě když φ je pravdivá.
- Výrokovou logiku lze zavést jako fragment predikátové logiky pomocí nulárních relačních symbolů (*syntax*) a nulárních relací (*sémantika*), přičemž $A^0 = \{\emptyset\} = 1$ a tedy $R^A \subseteq A^0$ je $R^A = \emptyset = 0$ anebo $R^A = \{\emptyset\} = 1$.

Tablo metoda ve VL - opakování

- Tablo je binární strom reprezentující vyhledávání *protipříkladu*.
- Vrcholy jsou označeny položkami, tj. formulemi s příznakem T / F, který reprezentuje předpoklad, že formule v nějakém modelu platí / neplatí.
- Je-li tento předpoklad správný, je správný i v nějaké větvi pod ní.
- Větev je sporná (selže), pokud obsahuje $T\psi$, $F\psi$ pro nějaké ψ.
- Důkaz formule φ je sporné tablo s kořenem $F\varphi$, tj. tablo v němž každá větev je sporná (nebyl nalezen protipříklad), pak φ je pravdivá.
- Pokud protipříklad existuje, v dokončeném tablu bude větev, která ho poskytuje, tato větev může být nekonečná.
- Lze zkonstruovat systematické tablo, jež je vždy dokončené.
- Pokud je φ pravdivá, systematické tablo pro φ je sporné, tj. důkazem φ, v tom případě je i konečné.

Tablo metoda v PL - rozdíly

- Formule v položkách budou sentence (uzavřené formule), tj. formule bez volných proměnných.
- Přidáme nová atomická tabla pro kvantifikátory.
- Za kvantifikované proměnné se budou substituovat konstantní termy dle jistých pravidel.
- Jazyk rozšíříme o nové (pomocné) konstantní symboly (spočetně mnoho) pro reprezentaci *"svědků"* položek $T(\exists x)\varphi(x)$ a $F(\forall x)\varphi(x)$.
- V dokončené bezesporné větvi s položkou $T(\forall x)\varphi(x)$ či $F(\exists x)\varphi(x)$ budou instance $T\varphi(x/t)$ resp. $F\varphi(x/t)$ pro každý konstantní term t (rozšířeného jazyka).

Tablo v PL - příklady

$$
\begin{array}{c}
F((\exists x)\neg P(x) \to \neg(\forall x)P(x)) \\
| \\
T(\exists x)\neg P(x) \\
| \\
F(\neg(\forall x)P(x)) \\
| \\
T(\forall x)P(x) \\
| \\
T(\neg P(c)) \quad c \ \text{nové} \\
| \\
FP(c) \\
| \\
T(\forall x)P(x) \\
| \\
TP(c) \\
| \\
\otimes
\end{array}
$$

$$
\begin{array}{c}
F(\neg(\forall x)P(x) \to (\exists x)\neg P(x)) \\
| \\
T(\neg(\forall x)P(x)) \\
| \\
F(\exists x)\neg P(x) \\
| \\
F(\forall x)P(x) \\
| \\
FP(d) \quad d \ \text{nové} \\
| \\
F(\exists x)\neg P(x) \\
| \\
F(\neg P(d)) \\
| \\
TP(d) \\
| \\
\otimes
\end{array}
$$

Předpoklady

1) *Dokazovaná formule* φ *je sentence.* Není-li φ sentence, můžeme ji nahradit za její generální uzávěr φ', neboť pro každou teorii T,

$$T \models \varphi \quad \text{právě když} \quad T \models \varphi'.$$

2) *Dokazujeme z teorie v uzavřeném tvaru, tj. každý axiom je sentence.* Nahrazením každého axiomu ψ za jeho generální uzávěr ψ' získáme ekvivalentní teorii, neboť pro každou strukturu $\mathcal{A}$ (daného jazyka L),

$$\mathcal{A} \models \psi \quad \text{právě když} \quad \mathcal{A} \models \psi'.$$

3) *Jazyk* L *je spočetný.* Pak každá teorie nad L je spočetná. Označme L_C rozšíření jazyka L o nové konstantní symboly $c_0, c_1, \ldots$ (spočetně nekonečně mnoho). Platí, že konstantních termů jazyka L_C je spočetně. Nechť t_i označuje i-tý konstantní term (v pevně zvoleném očíslování).

4) *Zatím budeme předpokládat, že jazyk je bez rovnosti.*

Atomická tabla - původní

Atomická tabla jsou všechny následující (položkami značkované) stromy, kde α je libovolná atomická sentence a φ, ψ jsou libovolné sentence, vše v L_C.

$T\alpha$	$F\alpha$	$T(\varphi \wedge \psi)$ $T\varphi$ $T\psi$	$F(\varphi \wedge \psi)$ $F\varphi$ / $F\psi$	$T(\varphi \vee \psi)$ $T\varphi$ / $T\psi$	$F(\varphi \vee \psi)$ $F\varphi$ $F\psi$
$T(\neg\varphi)$ $F\varphi$	$F(\neg\varphi)$ $T\varphi$	$T(\varphi \rightarrow \psi)$ $F\varphi$ / $T\psi$	$F(\varphi \rightarrow \psi)$ $T\varphi$ $F\psi$	$T(\varphi \leftrightarrow \psi)$ $T\varphi$ / $F\varphi$ $T\psi$ / $F\psi$	$F(\varphi \leftrightarrow \psi)$ $T\varphi$ / $F\varphi$ $F\psi$ / $T\psi$

Atomická tabla - nová

Atomická tabla jsou i následující (položkami značkované) stromy, kde φ je libovolná formule jazyka L_C ve volné proměnné x, t je libovolný konstantní term jazyka L_C a c je nový konstantní symbol z $L_C \setminus L$.

$\sharp$ $T(\forall x)\varphi(x)$ $\vert$ $T\varphi(x/t)$ pro libovolný konst. term t	$*$ $F(\forall x)\varphi(x)$ $\vert$ $F\varphi(x/c)$ pro *novou* konstantu c	$*$ $T(\exists x)\varphi(x)$ $\vert$ $T\varphi(x/c)$ pro *novou* konstantu c	$\sharp$ $F(\exists x)\varphi(x)$ $\vert$ $F\varphi(x/t)$ pro libovolný konst. term t

Poznámka *Konstantní symbol c reprezentuje “svědka” položky $T(\exists x)\varphi(x)$ či $F(\forall x)\varphi(x)$. Jelikož nechceme, aby na c byly kladeny další požadavky, je v definici tabla omezeno, jaký konstantní symbol c lze použít.*

Tablo

Konečné tablo z teorie T je binární, položkami značkovaný strom s předpisem

(*i*) každé atomické tablo je konečné tablo z T, přičemž v případě $(*)$ lze použít libovolný konstantní symbol $c \in L_C \setminus L$,

(*ii*) je-li P položka na větvi V konečného tabla z T, pak připojením atomického tabla pro P na konec větve V vznikne konečné tablo z T, přičemž v případě $(*)$ lze použít pouze konstantní symbol $c \in L_C \setminus L$, který se dosud nevyskytuje na V,

(*iii*) je-li V větev konečného tabla z T a $\varphi \in T$, pak připojením $T\varphi$ na konec větve V vznikne rovněž konečné tablo z T.

(*iv*) každé konečné tablo z T vznikne konečným užitím pravidel (*i*), (*ii*), (*iii*).

Tablo z teorie T je posloupnost $\tau_0, \tau_1, \ldots, \tau_n, \ldots$ konečných tabel z T takových, že τ_{n+1} vznikne z τ_n pomocí (*ii*) či (*iii*), formálně $\tau = \cup \tau_n$.