Výroková a predikátová logika - XII

Petr Gregor

KTIML MFF UK

ZS 2013/2014

Důsledek věty o spočetném modelu

Pomocí kanonického modelu (s rovností) jsme dříve dokázali následující větu.

Věta *Nechť T je bezesporná teorie nejvýše spočetného jazyka L. Je-li L bez rovnosti, má T model, který je spočetný. Je-li L s rovností, má T model, který je nejvýše spočetný.*

Důsledek *Ke každé struktuře $\mathcal{A}$ nejvýše spočetného jazyka bez rovnosti existuje spočetná elementárně ekvivalentní struktura $\mathcal{B}$.*

Důkaz Teorie $\mathrm{Th}(\mathcal{A})$ je bezesporná, neboť má model $\mathcal{A}$. Dle předchozí věty má spočetný model $\mathcal{B}$. Jelikož je teorie $\mathrm{Th}(\mathcal{A})$ kompletní, je $\mathcal{A} \equiv \mathcal{B}$. □

Důsledek *Ke každé nekonečné struktuře $\mathcal{A}$ nejvýše spočetného jazyka s rovností existuje spočetná elementárně ekvivalentní struktura $\mathcal{B}$.*

Důkaz Obdobně jako výše. Jelikož v $\mathcal{A}$ neplatí sentence *"existuje právě n prvků"* pro žádné $n \in \mathbb{N}$ a $\mathcal{A} \equiv \mathcal{B}$, není B konečná, tedy je spočetná. □

Spočetné algebraicky uzavřené těleso

Řekneme, že těleso $\mathcal{A}$ je *algebraicky uzavřené*, pokud v něm každý polynom (nenulového stupně) má kořen, tj. pro každé $n \geq 1$ platí

$$\mathcal{A} \models (\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0)$$

kde y^k je zkratka za term $y \cdot y \cdot \ \cdots \ \cdot y$ ($\cdot$ aplikováno $(k-1)$-krát).

Např. těleso $\underline{\mathbb{C}} = \langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$ je algebraicky uzavřené, zatímco tělesa $\underline{\mathbb{R}}$ a $\underline{\mathbb{Q}}$ nejsou (neboť polynom $x^2 + 1$ v nich nemá kořen).

Důsledek *Existuje spočetné algebraicky uzavřené těleso.*

Důkaz Dle předchozího důsledku existuje spočetná struktura elementárně ekvivalentní s tělesem $\underline{\mathbb{C}}$, tedy je to rovněž algebraicky uzavřené těleso. $\square$

Izomorfismus struktur

Nechť $\mathcal{A}$, $\mathcal{B}$ jsou struktury jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$.

- Bijekce $h\colon A \to B$ je *izomorfismus* struktur $\mathcal{A}$ a $\mathcal{B}$, pokud platí zároveň
  - (i) $h(f^A(a_1, \ldots, a_n)) = f^B(h(a_1), \ldots, h(a_n))$
    pro každý n-ární funkční symbol $f \in \mathcal{F}$ a každé $a_1, \ldots, a_n \in A$,
  - (ii) $R^A(a_1, \ldots, a_n) \quad \Leftrightarrow \quad R^B(h(a_1), \ldots, h(a_n))$
    pro každý n-ární relační symbol $R \in \mathcal{R}$ a každé $a_1, \ldots, a_n \in A$.
- $\mathcal{A}$ a $\mathcal{B}$ jsou *izomorfní* (via h), psáno $\mathcal{A} \simeq \mathcal{B}$ ($\mathcal{A} \simeq_h \mathcal{B}$), pokud existuje izomorfismus h struktur $\mathcal{A}$ a $\mathcal{B}$. Říkáme rovněž, že $\mathcal{A}$ je *izomorfní s* $\mathcal{B}$.
- *Automorfismus* struktury $\mathcal{A}$ je izomorfismus $\mathcal{A}$ s $\mathcal{A}$.

Např. potenční algebra $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$ *s* $X = n$ *je izomorfní s Booleovou algebrou* $\underline{{}^n 2} = \langle {}^n 2, -_n, \wedge_n, \vee_n, 0_n, 1_n \rangle$ *via* $h : A \mapsto \chi_A$, *kde* χ_A *je charakteristická funkce množiny* $A \subseteq X$.

Izomorfismus a sémantika

Uvidíme, že izomorfismus zachovává sémantiku.

Tvrzení *Nechť $\mathcal{A}$, $\mathcal{B}$ jsou struktury jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$. Bijekce $h\colon A \to B$ je izomorfismus $\mathcal{A}$ a $\mathcal{B}$, právě když platí zároveň*

(i) $h(t^A[e]) = t^B(he)$ *pro každý term t a $e\colon \mathrm{Var} \to A$,*

(ii) $\mathcal{A} \models \varphi[e] \;\Leftrightarrow\; \mathcal{B} \models \varphi[he]$ *pro každou formuli φ a $e\colon \mathrm{Var} \to A$.*

Důkaz $(\Rightarrow)$ Indukcí dle struktury termu t, respektive formule φ.

$(\Leftarrow)$ Dosazením termu $f(x_1, \ldots, x_n)$ do (i) či atomické formule $R(x_1, \ldots, x_n)$ do (ii) pro ohodnocení $e(x_i) = a_i$ dostaneme, že h vyhovuje definici izomorfismu. $\square$

Důsledek *Pro každé struktury $\mathcal{A}$, $\mathcal{B}$ stejného jazyka,*

$$\mathcal{A} \simeq \mathcal{B} \;\Rightarrow\; \mathcal{A} \equiv \mathcal{B}.$$

Poznámka *Obrácená implikace obecně neplatí, např. $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$, ale $\langle \mathbb{Q}, \leq \rangle \not\simeq \langle \mathbb{R}, \leq \rangle$, neboť $|\mathbb{Q}| = \omega$ a $|\mathbb{R}| = 2^\omega$.*

Konečné modely s rovností

Tvrzení *Pro každé konečné struktury $\mathcal{A}$, $\mathcal{B}$ stejného jazyka s rovností,*

$$\mathcal{A} \equiv \mathcal{B} \quad \Rightarrow \quad \mathcal{A} \simeq \mathcal{B}.$$

Důkaz Je $|A| = |B|$, neboť lze vyjádřit *"existuje právě n prvků"*.

- Nechť $\mathcal{A}'$ je expanze $\mathcal{A}$ do jazyka $L' = L \cup \{c_a\}_{a \in A}$ o jména prvků z A.
- Ukážeme, že $\mathcal{B}$ lze expandovat na $\mathcal{B}'$ do jazyka L' tak, že $\mathcal{A}' \equiv \mathcal{B}'$. Pak zřejmě $h\colon a \mapsto c_a^{B'}$ je izomorfismus $\mathcal{A}'$ s $\mathcal{B}'$ a tedy i izomorfismus $\mathcal{A}$ s $\mathcal{B}$.
- Stačí ukázat, že pro každé $c_a^{A'} = a \in A$ existuje $b \in B$ t.ž. $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$.
- Označme Ω množinu formulí $\varphi(x)$ t.ž. $\langle \mathcal{A}, a \rangle \models \varphi(x/c_a)$, tj. $\mathcal{A} \models \varphi[e(x/a)]$.
- Jelikož je A konečné, existuje konečně formulí $\varphi_0(x), \ldots, \varphi_m(x)$ tak, že pro každé $\varphi \in \Omega$ je $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$ pro nějaké i.
- Jelikož $\mathcal{B} \equiv \mathcal{A} \models (\exists x) \bigwedge_{i \le m} \varphi_i$, existuje $b \in B$ t.ž. $\mathcal{B} \models \bigwedge_{i \le m} \varphi_i[e(x/b)]$.
- Tedy pro každou $\varphi \in \Omega$ je $\mathcal{B} \models \varphi[e(x/b)]$, tj. $\langle \mathcal{B}, b \rangle \models \varphi(x/c_a)$. $\square$

Důsledek *Má-li kompletní teorie jazyka s rovností konečný model, jsou všechny její modely izomorfní.*

Kategoričnost

- *Izomorfní spektrum* teorie T je počet $I(\kappa, T)$ navzájem neizomorfních modelů teorie T pro každou kardinalitu κ.
- Teorie T je *κ-kategorická*, pokud má až na izomorfismus právě jeden model kardinality κ, tj. $I(\kappa, T) = 1$.

Tvrzení *Teorie $DeLO$ (tj. "bez konců") je ω-kategorická.*

Důkaz Nechť $\mathcal{A}, \mathcal{B} \models DeLO$ s $A = \{a_i\}_{i\in\mathbb{N}}$, $B = \{b_i\}_{i\in\mathbb{N}}$. Indukcí dle n lze nalézt prosté parciální funkce $h_n \subseteq h_{n+1} \subset A \times B$ zachovávající uspořádání tak, že $\{a_i\}_{i<n} \subseteq \mathrm{dom}(h_n)$ a $\{b_i\}_{i<n} \subseteq \mathrm{rng}(h_n)$. Pak $\mathcal{A} \simeq \mathcal{B}$ via $h = \cup h_n$. $\square$

Obdobně dostaneme, že např. $\mathcal{A} = \langle \mathbb{Q}, \leq \rangle$, $\mathcal{A} \restriction (0,1]$, $\mathcal{A} \restriction [0,1)$, $\mathcal{A} \restriction [0,1]$ jsou až na izomorfismus všechny nejvýše spočetné modely teorie $DeLO^*$. Pak

$$I(\kappa, DeLO^*) = \begin{cases} 0 & \text{pro } \kappa \in \mathbb{N}, \\ 4 & \text{pro } \kappa = \omega. \end{cases}$$

ω-kategorické kritérium kompletnosti

Věta *Nechť jazyk L je nejvýše spočetný.*

(i) *Je-li teorie T jazyka L bez rovnosti ω-kategorická, je kompletní.*

(ii) *Je-li teorie T jazyka L s rovností ω-kategorická a bez konečného modelu, je kompletní.*

Důkaz Každý model teorie T je elementárně ekvivalentní s nějakým spočetným modelem T, ale ten je až na izomorfismus jediný. Tedy všechny modely T jsou elementárně ekvivalentní, tj. T je kompletní. $\square$

Např. teorie DeLO, DeLO^+, DeLO^-, $\mathrm{DeLO}^\pm$ jsou kompletní a jsou to všechny (navzájem neekvivalentní) jednoduché kompletní extenze teorie DeLO^*.

Poznámka *Obdobné kritérium platí i pro vyšší než spočetné kardinality.*

Axiomatizovatelnost

Zajímá nás, zda se daná část světa dá "dobře" popsat.

Nechť $K \subseteq M(L)$ je třída struktur jazyka L. Řekneme, že K je

- *axiomatizovatelná*, pokud existuje teorie T jazyka L s $M(T) = K$,
- *konečně axiomatizovatelná*, pokud je axiomatizovatelná konečnou teorií,
- *otevřeně axiomatizovatelná*, pokud je axiomatizovatelná otevřenou teorií,
- teorie T je konečně (otevřeně) axiomatizovatelná, pokud $M(T)$ je konečně (respektive otevřeně) axiomatizovatelná.

Pozorování *Není-li K uzavřená na el. ekvivalenci, není axiomatizovatelná.*

Například

$a)$ *lineární uspořádání jsou konečně i otevřeně axiomatizovatelná,*

$b)$ *tělesa jsou konečně axiomatizovatelná, ale ne otevřeně,*

$c)$ *nekonečné grupy jsou axiomatizovatelné, ale ne konečně.*

Důsledek kompaktnosti

Věta *Má-li teorie T pro každé $n \in \mathbb{N}$ alespoň n-prvkový model, má i nekonečný model.*

Důkaz V jazyce bez rovnosti je to zřejmé, uvažme jazyk s rovností.

- Označme extenzi $T' = T \cup \{c_i \neq c_j \mid \text{pro } i \neq j\}$ teorie T v jazyce rozšířeném o spočetně nových konstantních symbolů c_i.
- Dle předpokladu má každá konečná část teorie T' model.
- Tedy dle věty o kompaktnosti má T' model, ten je nutně nekonečný.
- Jeho redukt na původní jazyk je hledaný nekonečný model teorie T. □

Důsledek *Má-li teorie T pro každé $n \in \mathbb{N}$ alespoň n-prvkový model, není třída všech jejích konečných modelů axiomatizovatelná.*

Např. nelze axiomatizovat konečné grupy, konečná tělesa, atd. Avšak třída nekonečných modelů teorie T jazyka s rovností je axiomatizovatelná.

Konečná axiomatizovatelnost

Věta *Nechť $K \subseteq M(L)$ a $\overline{K} = M(L) \setminus K$, kde L je jazyk. Pak K je konečně axiomatizovatelná, právě když K i $\overline{K}$ jsou axiomatizovatelné.*

Důkaz ($\Rightarrow$) Je-li T konečná axiomatizace K v uzavřeném tvaru, pak teorie s jediným axiomem $\bigvee_{\varphi \in T} \neg\varphi$ axiomatizuje $\overline{K}$. Nyní dokažme ($\Leftarrow$).

- Nechť T, S jsou teorie jazyka L takové, že $M(T) = K$, $M(S) = \overline{K}$.
- Pak $M(T \cup S) = M(T) \cap M(S) = \emptyset$ a dle věty o kompaktnosti existují konečné $T' \subseteq T$ a $S' \subseteq S$ takové, že $\emptyset = M(T' \cup S') = M(T') \cap M(S')$.
- Jelikož

$$M(T) \subseteq M(T') = \overline{M(S')} \subseteq \overline{M(S)} = M(T),$$

je $M(T) = M(T')$, tj. konečná T' axiomatizuje K. $\square$

Konečná axiomatizovatelnost - příklad

Nechť T je teorie těles. Řekneme, že těleso $\mathcal{A} = \langle A, +, -, \cdot, 0, 1 \rangle$ je

- *charakteristiky* 0, neexistuje-li žádné $p \in \mathbb{N}^+$ takové, že $\mathcal{A} \models p1 = 0$, kde $p1$ značí term $1 + 1 + \cdots + 1$ ($+$ aplikováno $(p-1)$-krát).
- *charakteristiky* p, kde p je prvočíslo, je-li p je nejmenší t.ž. $\mathcal{A} \models p1 = 0$.
- Třída těles charakteristiky p pro p prvočíslo je konečně axiomatizována teorií $T \cup \{p1 = 0\}$.
- Třída těles charakteristiky 0 je axiomatizována (nekonečnou) teorií $T' = T \cup \{p1 \neq 0 \mid p \in \mathbb{N}^+\}$.

Tvrzení *Třída K těles charakteristiky 0 není konečně axiomatizovatelná.*

Důkaz Stačí dokázat, že $\overline{K}$ není axiomatizovatelná. Kdyby $M(S) = \overline{K}$, tak $S' = S \cup T'$ má model $\mathcal{B}$, neboť každá konečná $S^* \subseteq S'$ má model (těleso prvočíselné charakteristiky větší než jakékoliv p vyskytující se v axiomech S^*). Pak ale $\mathcal{B} \in M(S) = \overline{K}$ a zároveň $\mathcal{B} \in M(T') = K$, což není možné. $\square$

Otevřená axiomatizovatelnost

Věta *Je-li teorie T otevřeně axiomatizovatelná, pak každá podstruktura modelu T je rovněž modelem T.*

Důkaz Nechť T' je otevřená axiomatika $M(T)$, $\mathcal{A} \models T'$ a $\mathcal{B} \subseteq \mathcal{A}$. Víme, že pro každé $\varphi \in T'$ je $\mathcal{B} \models \varphi$, neboť φ je otevřená. Tedy $\mathcal{B}$ je modelem T'. $\square$

Poznámka *Platí i obrácená implikace, tj. je-li každá podstruktura modelu teorie T rovněž modelem T, pak T je otevřeně axiomatizovatelná.*

Např. teorie $DeLO$ není otevřeně axiomatizovatelná, neboť např. konečná podstruktura modelu $DeLO$ není modelem $DeLO$.

Např. nejvýše n-prvkové grupy pro pevné $n > 1$ jsou otevřeně axiomatizovány

$$T \cup \{ \bigvee_{\substack{i,j \leq n \\ i \neq j}} x_i = x_j \},$$

kde T je (otevřená) teorie grup.

Definovatelné množiny

Zajímá nás, které množiny lze v dané struktuře zadefinovat.

- *Množina definovaná formulí* $\varphi(x_1, \ldots, x_n)$ *ve struktuře* $\mathcal{A}$ je množina
$$\varphi^{\mathcal{A}}(x_1, \ldots, x_n) = \{(a_1, \ldots, a_n) \in A^n \mid \mathcal{A} \models \varphi[e(x_1/a_1, \ldots, x_n/a_n)]\}.$$
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* $\underline{\mathcal{P}}(A^n)$.

Definovatelnost a automorfismy

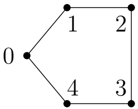
Ukážeme, že definovatelné množiny jsou invariantní vůči automorfismům.

Tvrzení *Nechť $D \subseteq A^n$ je množina definovatelná v struktuře $\mathcal{A}$ z parametrů $\overline{b}$ a h je automorfismus $\mathcal{A}$, který je identický na $\overline{b}$. Pak $h[D] = D$.*

Důkaz Nechť $D = \varphi^{\mathcal{A},\overline{b}}(\overline{x},\overline{y})$. Pak pro každé $\overline{a} \in A^{|\overline{x}|}$

$$\overline{a} \in D \;\Leftrightarrow\; \mathcal{A} \models \varphi[e(\overline{x}/\overline{a},\overline{y}/\overline{b})] \;\Leftrightarrow\; \mathcal{A} \models \varphi[he(\overline{x}/\overline{a},\overline{y}/\overline{b})]$$
$$\Leftrightarrow\; \mathcal{A} \models \varphi[e(\overline{x}/h\overline{a},\overline{y}/h\overline{b})] \;\Leftrightarrow\; \mathcal{A} \models \varphi[e(\overline{x}/h\overline{a},\overline{y}/\overline{b})] \;\Leftrightarrow\; h\overline{a} \in D. \quad \square$$

Např. graf $\mathcal{G}$ má právě jeden netriv. automorfismus h zachovávající vrchol 0.



$h(0) = 0,\;\; h(1) = 4,\;\; h(2) = 3,\;\; h(3) = 2,\;\; h(4) = 1$

$\{0\} = (x = y)^{\mathcal{G},0}$, $\{1,4\} = (E(x,y))^{\mathcal{G},0}$, $\{2,3\} = (x \neq y \wedge \neg E(x,y))^{\mathcal{G},0}$

Navíc množiny $\{0\}$, $\{1,4\}$, $\{2,3\}$ jsou definovatelné z parametru 0. Tedy

$\mathrm{Df}^1(\mathcal{G},\{0\}) = \{\emptyset, \{0\}, \{1,4\}, \{2,3\}, \{0,1,4\}, \{0,2,3\}, \{1,4,2,3\}, \{0,1,2,3,4\}\}.$

Základní algebraické teorie

- *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 $x + y = y + x$ (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 $x \cdot y = y \cdot x$ (komutativita $\cdot$)

- *Teorie těles* stejného jazyka má navíc axiomy

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

  $0 \neq 1$ (netrivialita)

Robinsonova aritmetika

Jak efektivně a přitom co nejúplněji axiomatizovat $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ *?*

Jazyk aritmetiky je $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností.

Robinsonova aritmetika Q má axiomy (konečně mnoho)

$$\begin{array}{ll} S(x) \neq 0 & x \cdot 0 = 0 \\ S(x) = S(y) \rightarrow x = y & x \cdot S(y) = x \cdot y + x \\ x + 0 = x & x \neq 0 \rightarrow (\exists y)(x = S(y)) \\ x + S(y) = S(x + y) & x \leq y \leftrightarrow (\exists z)(z + x = y) \end{array}$$

Poznámka Q *je velmi slabá, např. nedokazuje komutativitu či asociativitu operací* $+$, $\cdot$ *ani transitivitu* $\leq$*. Nicméně postačuje například k důkazu existenčních tvrzení o numerálech, která jsou pravdivá v* $\underline{\mathbb{N}}$*.*

Např. pro $\varphi(x, y)$ *tvaru* $(\exists z)(x + z = y)$ *je*

$$Q \vdash \varphi(\underline{1}, \underline{2}), \quad \text{kde } \underline{1} = S(0) \text{ a } \underline{2} = S(S(0)).$$

Peanova aritmetika

Peanova aritmetika PA má axiomy

(a) Robinsonovy aritmetiky Q,

(b) schéma indukce, tj. pro každou formuli $\varphi(x,\overline{y})$ jazyka L axiom

$$(\varphi(0,\overline{y}) \wedge (\forall x)(\varphi(x,\overline{y}) \rightarrow \varphi(S(x),\overline{y}))) \rightarrow (\forall x)\varphi(x,\overline{y}).$$

Poznámka *PA je poměrně dobrou aproximací $\mathrm{Th}(\underline{\mathbb{N}})$, dokazuje všechny základní vlastnosti $\underline{\mathbb{N}}$. Na druhou stranu existují tvrzení pravdivá v $\underline{\mathbb{N}}$ ale nezávislá v PA.*

Poznámka *V jazyce 2. řádu lze axiomatizovat $\underline{\mathbb{N}}$ (až na izomorfismus), vezmeme-li místo schéma indukce přímo axiom indukce (2. řádu)*

$$(\forall X)\ ((X(0) \wedge (\forall x)(X(x) \rightarrow X(S(x)))) \rightarrow (\forall x)\ X(x)).$$