Výroková a predikátová logika - XII

Petr Gregor

KTIML MFF UK

ZS 2015/2016

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 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)

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 $T' = T \cup \{c_i \neq c_j \mid \text{pro } i \neq j\}$ extenzi teorie T v rozšířeném jazyce o spočetně nekonečně mnoho 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
$$M(T) \subseteq M(T') \subseteq \overline{M(S')} \subseteq \overline{M(S)} = M(T),$$
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. □

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'. □

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

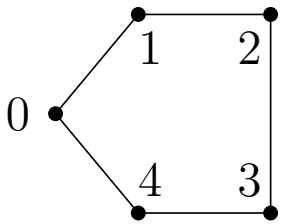
Ukážeme, že definovatelné množiny jsou invariantní vůči automorfismům.

Tvrzení *Nechť $D \subseteq A^n$ je množina definovatelná ve 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

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

Rekurzivní a rekurzivně spočetné množiny

Které problémy jsou algoritmicky řešitelné?

- Intuitivní pojem *"algoritmus"* lze přesně formalizovat (např. pomocí TS).
- Při vhodném kódování přirozenými čísly problém reprezentujeme jako množinu kódů vstupů, na které je odpověď `ano` (kladné instance). Např.

$$SAT = \{\lceil\varphi\rceil \mid \varphi \text{ je splnitelný výrok v CNF}\}.$$

- Množina $A \subseteq \mathbb{N}$ je *rekurzivní*, pokud existuje algoritmus, který pro každý vstup $x \in \mathbb{N}$ skončí a zjistí zda $x \in A$ (výstup `ano/ne`). Říkáme, že takový algoritmus rozhoduje, zda $x \in A$.
- Množina $A \subseteq \mathbb{N}$ je *rekurzivně spočetná* (*r. s.*), pokud existuje algoritmus, který pro každý vstup $x \in \mathbb{N}$ skončí, právě když $x \in A$. Říkáme, že takový algoritmus rozpoznává, že $x \in A$. Ekvivalentně, A je r. s. pokud existuje algoritmus, který na výstup postupně generuje všechny prvky A.

Pozorování *Pro každé $A \subseteq \mathbb{N}$ platí, že A je rekurzivní $\Leftrightarrow$ A, $\overline{A}$ jsou r. s.*

Rozhodnutelné teorie

Dá se pravdivost sentence v dané teorii algoritmicky rozhodovat?.

Předpokládáme (vždy), že jazyk L je rekurzivní. Teorie T nad L je *rozhodnutelná*, je-li $Thm(T)$ rekurzivní, jinak je *nerozhodnutelná*.

Tvrzení *Pro každou teorii T jazyka L s rekurzivně spočetnou axiomatikou,*

(i) $Thm(T)$ *je rekurzivně spočetná,*

(ii) *je-li navíc T kompletní, je $Thm(T)$ rekurzivní, t.j. T je rozhodnutelná.*

Důkaz Konstrukce systematického tabla z T s $F\varphi$ v kořeni předpokládá danou enumeraci axiomů T. Má-li T r. s. axiomatiku, je možné ji poskytnout algoritmicky. Pak konstrukce dává algoritmus, který rozpoznává $T \vdash \varphi$.

Je-li navíc T kompletní, pak pro každou sentenci φ platí $T \nvdash \varphi \Leftrightarrow T \vdash \neg\varphi$. Tedy paralelní konstrukce systematických tabel z T s $F\varphi$ resp. $T\varphi$ v kořeni poskytuje algoritmus pro rozhodování, zda $T \vdash \varphi$. □

Rekurzivně spočetná kompletace

Co když efektivně popíšeme všechny jednoduché kompletní extenze?

Řekneme, že množina všech (až na ekvivalenci) jednoduchých kompletních extenzí teorie T je *rekurzivně spočetná*, existuje-li algoritmus $\alpha(i, j)$, který generuje i-tý axiom j-té extenze (při nějakém očíslování), případně oznámí, že (takový axiom či extenze) neexistuje.

Tvrzení *Má-li teorie T rekurzivně spočetnou axiomatiku a množina všech (až na ekvivalenci) jejích jednoduchých kompletních extenzí je rekurzivně spočetná, je T rozhodnutelná.*

Důkaz Díky r. s. axiomatice poskytuje konstrukce systematického tabla z T s $F\varphi$ v kořeni algoritmus pro rozpoznání $T \vdash \varphi$. Pokud ale $T \nvdash \varphi$, pak $T' \vdash \neg\varphi$ v nějaké jednoduché kompletní extenzi T' teorie T. To lze rozpoznat paralelní postupnou konstrukcí systematických tabel pro $T\varphi$ z jednotlivých extenzí. V i-tém stupni se sestrojí tabla do i kroků pro prvních i extenzí. □

Příklady rozhodnutelných teorií

Následující teorie jsou rozhodnutelné, ačkoliv jsou nekompletní.

- teorie čisté rovnosti; bez axiomů v jazyce $L = \langle\rangle$ s rovností,
- teorie unárního predikátu; bez axiomů v jazyce $L = \langle U \rangle$ s rovností, kde U je unární relační symbol,
- teorie hustých lineárních uspořádání $DeLO^*$,
- teorie algebraicky uzavřených těles v jazyce $L = \langle +, -, \cdot, 0, 1 \rangle$ s rovností, s axiomy teorie těles a navíc axiomy pro každé $n \geq 1$,

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

  kde y^k je zkratka za term $y \cdot y \cdot \dots \cdot y$ ($\cdot$ aplikováno $(k-1)$-krát).
- teorie komutativních grup,
- teorie Booleových algeber.

Rekurzivní axiomatizovatelnost

Dají se matematické struktury "efektivně" popsat?

- Třída $K \subseteq M(L)$ je *rekurzivně axiomatizovatelná*, pokud existuje teorie T jazyka L s rekurzivní axiomatikou a $M(T) = K$.
- Teorie T je rekurzivně axiomatizovatelná, pokud $M(T)$ je rekurzivně axiomatizovatelná.

Tvrzení *Pro každou konečnou strukturu $\mathcal{A}$ v konečném jazyce s rovností je $\mathrm{Th}(\mathcal{A})$ rekurzivně axiomatizovatelná. Tedy, $\mathrm{Th}(\mathcal{A})$ je rozhodnutelná.*

Důkaz Nechť $A = \{a_1, \ldots, a_n\}$. Teorii $\mathrm{Th}(\mathcal{A})$ axiomatizujeme jednou sentencí (tedy rekurzivně) kompletně popisující $\mathcal{A}$. Bude tvaru *"existuje právě n prvků $a_1, \ldots, a_n$ splňujících právě ty základní vztahy o funkčních hodnotách a relacích, které platí ve struktuře $\mathcal{A}$."* □

Příklady rekurzivní axiomatizovatelnosti

Následující struktury $\mathcal{A}$ mají rekurzivně axiomatizovatelnou teorii $\mathrm{Th}(\mathcal{A})$.

- $\langle \mathbb{Z}, \leq \rangle$, teorií diskrétních lineárních uspořádání,
- $\langle \mathbb{Q}, \leq \rangle$, teorií hustých lineárních uspořádání bez konců ($DeLO$),
- $\langle \mathbb{N}, S, 0 \rangle$, teorií následníka s nulou,
- $\langle \mathbb{N}, S, +, 0 \rangle$, tzv. Presburgerovou aritmetikou,
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, teorií reálně uzavřených těles,
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, teorií algebraicky uzavřených těles charakteristiky 0.

Důsledek *Pro uvedené struktury je* $\mathrm{Th}(\mathcal{A})$ *rozhodnutelná.*

Poznámka *Uvidíme, že ale* $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ *rekurzivně axiomatizovat nelze. (Vyplývá to z první Gödelovy věty o neúplnosti).*

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)

$$S(x) \neq 0 \qquad x \cdot 0 = 0$$
$$S(x) = S(y) \to x = y \qquad x \cdot S(y) = x \cdot y + x$$
$$x + 0 = x \qquad x \neq 0 \to (\exists y)(x = S(y))$$
$$x + S(y) = S(x + y) \qquad x \leq y \leftrightarrow (\exists z)(z + x = y)$$

Poznámka Q *je velmi slabá, např. nedokazuje komutativitu či asociativitu operací* $+, \cdot$ *ani tranzitivitu* $\leq$*. 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

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

Poznámka *PA je poměrně dobrou aproximací $\mathrm{Th}(\underline{\mathbb{N}})$, dokazuje všechny základní vlastnosti platné v $\underline{\mathbb{N}}$ (např. komutativitu $+$). Na druhou stranu existují sentence pravdivé v $\underline{\mathbb{N}}$ ale nezávislé 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)*

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