Výroková a predikátová logika - XIII

Petr Gregor

KTIML MFF UK

ZS 2013/2014

Algoritmická (ne)rozhodnutelnost

Které problémy jsou algoritmicky řešitelné?

- Intuitivní pojem *"algoritmus"* lze přesně formalizovat (např. pomocí TS).
- Rozhodovací problém je popsán vstupem (instance) a otázkou (`ano/ne`).
  Např. instancí SAT je výrok φ v CNF a otázkou je, zda φ je splnitelný.
- Problém je (algoritmicky) *rozhodnutelný*, pokud existuje algoritmus, který pro každý vstup skončí a vydá správnou odpověď (výstup `ano/ne`).
- Problém je (algoritmicky) *rozpoznatelný*, pokud existuje algoritmus, který pozná, že pro daný vstup odpověď na otázku je `ano`. V tom případě skončí a odpoví `ano`. V opačném případě se neskončí nebo odpoví `ne`.
- Ekvivalentně, problém je rozpoznatelný, pokud existuje algoritmus, který pro daný vstup skončí, právě když odpověď na otázku je `ano`.

Rekurzivní a rekurzivně spočetné množiny

Problémy lze reprezentovat jako množiny přirozených čísel.

- Při vhodném kódování vstupů přirozenými čísly problém reprezentujeme jako množinu kódů jeho kladných instancí (odpověď `ano`). 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`).
- *rozhodnutelný problém* $\approx$ *rekurzivní množina*
- Množina $A \subseteq \mathbb{N}$ je *rekurzivně spočetná* (*r. s.*), pokud existuje algoritmus, který pro vstup $x \in \mathbb{N}$ skončí, právě když $x \in A$. Ekvivalentně, pokud existuje algoritmus, který na výstup postupně generuje všechny prvky A.
- *rozpoznatelný problém* $\approx$ *rekurzivně spočetná množina*

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*,
- *rozpoznatelná*, je-li $Thm(T)$ rekurzivně spočetná.

Tvrzení *Pro každou teorii T jazyka L,*

(i) *má-li T rekurzivně spočetnou axiomatiku, je rozpoznatelná,*

(ii) *má-li T r. s. axiomatiku a je-li kompletní, 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 pro rozpoznání $T \vdash \varphi$.

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 $T \vdash \varphi$. $\square$

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 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. $\square$

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 $n \geq 1$,
  $$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \cdots + x_1 \cdot y + x_0 = 0),$$
  kde y^k je zkratka za term $y \cdot y \cdot \ \cdots \ \cdot y$ ($\cdot$ aplikováno $(k-1)$-krát).
- 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.

Poznámka *Obdobně lze zadefinovat r. s. axiomatizovatelnost.*

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 $\mathcal{A}$."* $\square$

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)

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

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

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

Poznámka PA *je poměrně dobrou aproximací* $\mathrm{Th}(\underline{\mathbb{N}})$*, dokazuje všechny základní vlastnosti 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)*

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

Hilbertův 10. problém

- Nechť $p(x_1, \ldots, x_n)$ je polynom s celočíselnými koeficienty. Má *Diofantická rovnice* $p(x_1, \ldots, x_n) = 0$ celočíselné řešení?
- Hilbert (1900) *"Nalezněte algoritmus, který po konečně mnoha krocích určí, zda daná Diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má celočíselné řešení."*

Poznámka *Ekvivalentně lze požadovat algoritmus rozhodující, zda existuje řešení v přirozených číslech.*

Věta (DPRM, 1970) *Problém existence celočíselného řešení dané Diofantické rovnice s celočíselnými koeficienty je alg. nerozhodnutelný.*

Důsledek *Neexistuje algoritmus rozhodující pro dané polynomy* $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_n)$ *s přirozenými koeficienty, zda*

$$\mathbb{N} \models (\exists x_1) \ldots (\exists x_n)(p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)).$$

Nerozhodutelnost predikátové logiky

Existuje algoritmus, rozhodující o dané sentenci, zda je logicky pravdivá?

- Víme, že Robinsonova aritmetika Q má konečně axiomů, má za model $\underline{\mathbb{N}}$ a stačí k důkazu existenčních tvrzení o numerálech, která platí v $\underline{\mathbb{N}}$.
- Přesněji, pro každou existenční formuli $\varphi(x_1, \ldots, x_n)$ jazyka aritmetiky
$$Q \vdash \varphi(x_1/\underline{a_1}, \ldots, x_n/\underline{a_n}) \quad \Leftrightarrow \quad \underline{\mathbb{N}} \models \varphi[e(x_1/a_1, \ldots, x_n/a_n)]$$
pro každé $a_1, \ldots, a_n \in \mathbb{N}$, kde $\underline{a_i}$ značí a_i-tý numerál.
- Speciálně, pro φ tvaru $(\exists x_1) \ldots (\exists x_n)(p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n))$, kde p, q jsou polynomy s přirozenými koeficienty (numerály), platí
$$\underline{\mathbb{N}} \models \varphi \quad \Leftrightarrow \quad Q \vdash \varphi \quad \Leftrightarrow \quad \vdash \psi \rightarrow \varphi \quad \Leftrightarrow \quad \models \psi \rightarrow \varphi,$$
kde ψ je konjunkce (uzávěrů) všech axiomů Q.
- Tedy, pokud by existoval algoritmus rozhodující logickou pravdivost, existoval by i algoritmus rozhodující, zda $\underline{\mathbb{N}} \models \varphi$, což není možné.

Gödelova 1. věta o neúplnosti

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence pravdivá v $\underline{\mathbb{N}}$ a nedokazatelná v T.*

Poznámky

- *"Rekurzivně axiomatizovaná" znamená, že je "efektivně zadaná".*
- *"Extenze R. aritmetiky" znamená, že je "základní aritmetické síly".*
- *Je-li navíc $\underline{\mathbb{N}} \models T$, je teorie T nekompletní.*
- *V důkazu sestrojená sentence vyjadřuje "nejsem dokazatelná v T".*
- *Důkaz je založen na dvou principech:*

  (a) *aritmetizaci syntaxe,*

  (b) *self-referenci.*