Třináctá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Třináctá přednáška

Program

- aritmetické teorie
- nerozhodnutelnost predikátové logiky
- Gödelovy věty o neúplnosti

Materiály

Zápisky z přednášky, Sekce 10.2-10.4 z Kapitoly 10

10.2 Aritmetika

Aritmetika

- přirozená čísla hrají důležitou roli v matematice i v aplikacích
- jazyk aritmetiky je $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností
- standardní model aritmetiky $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ nemá rekurzivně axiomatizovatelnou teorii (První věta o neúplnosti)
- proto používáme rekurzivně axiomatizované teorie, které vlastnosti $\underline{\mathbb{N}}$ popisují částečně; říkáme jim aritmetiky
- představíme dvě: Robinsonovu Q a Peanovu PA

Robinsonova aritmetika Q

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

- velmi slabá, nelze v ní dokázat např. komutativitu ani asociativitu $+$ či $\cdot$, nebo tranzitivitu $\leq$
- ale lze dokázat všechna existenční tvrzení o numerálech pravdivá v $\underline{\mathbb{N}}$, tj. formule v PNF, jen $\exists$, za volné proměnné substituujeme numerály $\underline{n} = S(\dots S(0) \dots)$
- např. pro $\varphi(x, y) = (\exists z)(x + z = y)$ je $Q \vdash \varphi(\underline{1}, \underline{2})$

Tvrzení: Je-li $\varphi(x_1, \dots, x_n)$ existenční formule, $a_1, \dots, a_n \in \mathbb{N}$, pak $Q \vdash \varphi(x_1/\underline{a_1}, \dots, x_n/\underline{a_n})$ právě když $\underline{\mathbb{N}} \models \varphi[e(x_1/a_1, \dots, x_n/a_n)]$

(Důkaz vynecháme.)

Peanova aritmetika *PA*

Extenze Q o schéma indukce, tj. pro každou L-formuli $\varphi(x,\overline{y})$:

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

- mnohem lepší aproximace $\mathrm{Th}(\underline{\mathbb{N}})$
- dokáže ‘základní’ vlastnosti (např. komut. a asociativitu $+$)
- stále ale existují sentence platné v $\underline{\mathbb{N}}$ ale nezávislé v PA (opět dokážeme v První větě o neúplnosti)

Poznámka: strukturu $\underline{\mathbb{N}}$ lze axiomatizovat (až na $\simeq$) v predikátové logice 2. řádu, extenzí PA o tzv. axiom indukce:

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

- X reprezentuje (libovolnou) podmnožinu modelu
- použijeme na množinu všech následníků 0
- každý prvek je následník 0 $\Rightarrow$ izomorfismus s $\underline{\mathbb{N}}$

10.3 Nerozhodnutelnost predikátové logiky

Nerozhodnutelnost predikátové logiky

Věta (O nerozhodnutelnosti predikátové logiky): Neexistuje algoritmus, který pro vstupní formuli φ rozhodne, zda je logicky platná.

- tj. zda je formule φ [v lib. jazyce 1. řádu] tautologie ($\models \varphi$)
- neboli $T = \emptyset$ není rozhodnutelná

Nemáme formalismus pro algoritmy (Turingovy stroje), dokážeme redukcí na jiný nerozhodnutelný problém: Hilbertův 10. problém

> *"Najděte algoritmus, který po konečně mnoha krocích určí, zda daná diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má celočíselné řešení."*

diofantická rovnice: $p(x_1, \ldots, x_n) = 0$, kde p je celočíselný polynom

ukážeme, že existuje redukce 'těžkého' Hilbertova 10. problému na náš problém, tedy i náš problém je 'těžký'

Nerozhodnutelnost Hilbertova desátého problému

Věta (Matiyasevich 1970): Problém existence celočíselného řešení dané diofantické rovnice s celočís. koeficienty je nerozhodnutelný.

(Důkaz neuvedeme.)

Důsledek: Neexistuje algoritmus rozhodující, mají-li dané polynomy $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ s přiroz. koeficienty přirozené řešení, tj.

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

Důkaz: Lagrangeova věta o čtyřech čtvercích říká, že každé celé číslo lze vyjádřit jako rozdíl dvou přirozených, a naopak, každé přirozené číslo lze vyjádřit jako součet čtyř čtverců. Diofantickou rovnici lze tedy transformovat na rovnici z důsledku, a naopak. $\square$

Důkaz nerozhodnutelnosti predikátové logiky

Uvažme φ tvaru $(\exists x_1)\ldots(\exists x_n)\ p(x_1,\ldots,x_n) = q(x_1,\ldots,x_n)$ kde p a q jsou přirozené polynomy. Dle Tvrzení o Robinsonově aritmetice:

$$\underline{\mathbb{N}} \models \varphi \ \Leftrightarrow\ Q \vdash \varphi$$

Buď ψ_Q konjunkce (gen. uzávěrů) axiomů Q (je konečná). Zřejmě:

$$Q \vdash \varphi \ \Leftrightarrow\ \psi_Q \vdash \varphi \ \Leftrightarrow \vdash \psi_Q \rightarrow \varphi$$

Dle Věty o úplnosti je to ale ekvivalentní $\models \psi_Q \rightarrow \varphi$. Dostáváme:

$$\underline{\mathbb{N}} \models \varphi \ \Leftrightarrow \models \psi_Q \rightarrow \varphi$$

Sporem: Pokud bychom měli algoritmus rozhodující logickou platnost, mohli bychom rozhodovat i existenci přirozeného řešení rovnice $p(x_1,\ldots,x_n) = q(x_1,\ldots,x_n)$, tj. Hilbertův 10. problém. $\square$

10.4 Gödelovy věty

První věta o neúplnosti + důsledek o nekompletnosti

Věta (Gödel 1931): Je-li T bezesporná rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky, potom existuje sentence, která je pravdivá v $\underline{\mathbb{N}}$, ale není dokazatelná v T.

- vlastnosti aritmetiky přir. čísel nelze 'rozumně', efektivně popsat (v logice 1. řádu), takový popis je nutně 'neúplný'
- pravdivost je ve standardním modelu $\underline{\mathbb{N}}$ zatímco dokazatelnost v T (samozřejmě pravdivá v T je v T i dokazatelná)
- bezespornost nutná (sporná teorie dokáže vše)
- bez rekurzivní axiomatizovatelnosti by teorie nebyla 'užitečná'
- extenze Q znamená 'základní aritmetická síla' (různé varianty předpokladu; nelze-li zakódovat přir. čísla s $+, \cdot$ je moc 'slabá'

Důsledek: Splňuje-li teorie T předpoklady První věty o neúplnosti a je-li navíc $\underline{\mathbb{N}}$ modelem T, potom T není kompletní.

Důkaz: Vezměme Gödelovu sentenci φ ($\underline{\mathbb{N}} \models \varphi$, $T \nvdash \varphi$). Je-li T kompletní, víme $T \vdash \neg\varphi$, z korektnosti $T \models \neg\varphi$, tedy $\underline{\mathbb{N}} \models \neg\varphi$. $\square$

O důkazu

- Gödelova sentence formalizuje "Nejsem dokazatelná v T"
- převratná důkazová technika, dva hlavní principy:
- aritmetizace syntaxe, zakódování sentencí a jejich dokazatelnosti do přirozených čísel
- self-reference, sentence 'mluví sama o sobě' (o svém kódu)
- všechny technické detaily vynecháme, viz např. V. Švejdar: *Logika – neúplnost, složitost a nutnost*, Academia 2002

Aritmetizace dokazatelnosti

- Gödelovo číslování 'rozumně' kóduje konečné syntaktické objekty (termy, formule, tablo důkazy) do $\mathbb{N}$: lze algoritmicky [de-]kódovat, simulovat 'manipulaci' s objekty na jejich kódech
- pro φ bude $\lceil\varphi\rceil$ příslušný kód, $\underline{\varphi}$ odpovídající $\lceil\varphi\rceil$-tý numerál
- pro danou T máme binární relaci $\mathrm{Proof}_T \subseteq \mathbb{N}^2$ definovanou
  $(n, m) \in \mathrm{Proof}_T \Leftrightarrow n = \lceil\varphi\rceil,\ m = \lceil\tau\rceil,\ \tau$ je tablo důkaz φ z T
- je-li T rek. axiomatizovaná, je relace $\mathrm{Proof}_T \subseteq \mathbb{N}^2$ rekurzivní (lze algoritmicky ověřit korektnost tabla, tj. $(n, m) \in \mathrm{Proof}_T$)
- klíčová část důkazu První věty (důkaz vynecháme):

Tvrzení: Je-li T rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky, potom existuje formule $Prf_T(x, y)$ v jazyce aritmetiky, která reprezentuje relaci Proof_T, tj. pro každá $n, m \in \mathbb{N}$:

- je-li $(n, m) \in \mathrm{Proof}_T$, potom $Q \vdash Prf_T(\underline{n}, \underline{m})$
- jinak $Q \vdash \neg Prf_T(\underline{n}, \underline{m})$

Predikát dokazatelnosti

Self-reference

Věta o pevném bodě

Nedefinovatelnost pravdy

Důkaz První věty o neúplnosti

Důsledky První věty o neúplnosti

Gödelova Druhá věta o neúplnosti

Důsledky Druhé věty o neúplnosti