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

$\neg S(x) = 0$	$x \cdot 0 = 0$
$S(x) = S(y) \rightarrow x = y$	$x \cdot S(y) = x \cdot y + x$
$x + 0 = x$	$\neg x = 0 \rightarrow (\exists y)(x = S(y))$
$x + S(y) = S(x + y)$	$x \leq y \leftrightarrow (\exists z)(z + x = y)$

- 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 $\underline{n} = S(\ldots S(0)\ldots)$
- např. pro $\varphi(x, y) = (\exists z)(x + z = y)$ je $Q \vdash \varphi(\underline{1}, \underline{2})$

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

(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 ($\underline{\mathbb{N}} \models \varphi$, $T \not\vdash \varphi$). 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 syntaxe a 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 $\ulcorner\varphi\urcorner$ příslušný kód, $\underline{\varphi}$ odpovídající $\ulcorner\varphi\urcorner$-tý numerál
- pro danou T máme binární relaci $\mathrm{Proof}_T \subseteq \mathbb{N}^2$ definovanou
  $(n, m) \in \mathrm{Proof}_T \Leftrightarrow n = \ulcorner\varphi\urcorner$, $m = \ulcorner\tau\urcorner$, τ 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. $(n, m) \in \mathrm{Proof}_T$)
- klíčovou technickou částí důkazu První věty je fakt, že relaci Proof_T lze reprezentovat predikátem v Robinsonově aritmetice

Predikát dokazatelnosti

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 $Q \vdash \neg Prf_T(\underline{n}, \underline{m})$

(Důkaz vynecháme!)

- formule $Prf_T(x, y)$ vyjadřuje "y je důkaz x v T"
- formule $(\exists y) Prf_T(x, y)$ znamená "x je dokazatelná v T"
- svědek poskytuje kód tablo důkazu, a $\underline{\mathbb{N}}$ splňuje Q, proto:

Pozorování: $T \vdash \varphi$ právě když $\underline{\mathbb{N}} \models (\exists y) Prf_T(\underline{\varphi}, y)$.

Budeme potřebovat následující důsledek (také bez důkazu):

Důsledek: Je-li $T \vdash \varphi$, potom $T \vdash (\exists y) Prf_T(\underline{\varphi}, y)$.

Self-reference

vyjádřili jsme φ je dokazatelná ale chceme já nejsem dokazatelná

přirozené jazyky mají self-referenci: `Tato věta má 22 znaků.`; formální systémy obvykle ne, umožňují ale přímou referenci (mluvit o posloupnostech symbolů):

`Následující věta má 29 znaků. "Následující věta má 29 znaků."`

zde není žádná self-reference, pomůžeme si proto trikem zdvojení:

`Následující věta zapsaná jednou a ještě jednou v uvozovkách má 149 znaků. "Následující věta zapsaná jednou a ještě jednou v uvozovkách má 149 znaků."`

přímou referencí a zdvojením tedy získáme self-referenci; podobně program v C, který vypíše svůj kód (34 je ASCII kód uvozovek):

```
main(){char *c="main(){char *c=%c%s%c; printf(c,34,c,34);}";
printf(c,34,c,34);}
```

Věta o pevném bodě

Věta: Je-li T extenzí Robinsonovy aritmetiky, potom pro každou formuli $\varphi(x)$ (v jazyce teorie T) existuje sentence ψ taková, že:

$$T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$$

- také "diagonalizační lemma" nebo "self-referenční" lemma
- ψ je self-referenční, říká o sobě: "já splňuji vlastnost φ"
- v důkazu První věty bude $\varphi(x)$ formule $\neg(\exists y)Prf_T(x, y)$
- všimněte si, jak se v důkazu použije přímá reference a zdvojení

Důkaz (myšlenka): Zdvojující funkce $d : \mathbb{N} \to \mathbb{N}$ dekóduje vstup n jako $\varphi(x)$, dosadí numerál $\underline{n}$, znovu zakóduje: pro vš. $\chi(x)$ platí:

$$d(\ulcorner \chi(x) \urcorner) = \ulcorner \chi(\underline{\chi(x)}) \urcorner$$

S využitím T extenze Q se dokáže, že d je v T reprezentovatelná. Pro jednoduchost ať ji reprezentuje term, označíme ho také d (ale ve skutečnosti je to složitá formule).

Pokračování důkazu

Tedy Q, proto i T, dokazuje o numerálech, že d opravdu ‘zdvojuje’:

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})}$$

Hledaná self-referenční sentence ψ je sentence:

$$\varphi(d(\underline{\varphi(d(x))}))$$

Chceme dokázat, že $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$, neboli:

$$T \vdash \varphi(d(\underline{\varphi(d(x))})) \leftrightarrow \varphi(\underline{\varphi(d(\underline{\varphi(d(x))}))})$$

K tomu stačí $T \vdash d(\underline{\varphi(d(x))}) = \underline{\varphi(d(\underline{\varphi(d(x))}))}$ což máme z reprezentovatelnosti d, kde $\chi(x)$ je $\varphi(d(x))$. $\square$

ψ tedy říká: »Následující věta zapsaná jednou a ještě jednou v uvozovkách má vlastnost φ. “Následující věta zapsaná jednou a ještě jednou v uvozovkách má vlastnost φ.”« kde v uvozovkách znamená numerál kódu (přímá reference)

Nedefinovatelnost pravdy

Věta: V žádném bezesporném rozšíření Robinsonovy aritmetiky nemůže existovat definice pravdy.

- definice pravdy v aritmetické teorii T je formule $\tau(x)$ taková, že pro každou sentenci ψ platí: $T \vdash \psi \leftrightarrow \tau(\underline{\psi})$
- kdyby existovala, místo dokazování by stačilo spočíst kód $\ulcorner\psi\urcorner$, dosadit numerál $\underline{\psi}$ do τ, a vyhodnotit
- rozcvička pro důkaz Gödelovy První věty o neúplnosti
- důkaz užívá Paradox lháře, vyjádříme "Nejsem pravdivá v T"
- důkaz První věty užívá stejný trik s "Nejsem dokazatelná v T"

Důkaz: Sporem, ať existuje definice pravdy $\tau(x)$. Z Věty o pevném bodě kde $\varphi(x)$ je $\neg\tau(x)$ dostáváme sentenci ψ takovou, že:

$$T \vdash \psi \leftrightarrow \neg\tau(\underline{\psi})$$

Protože $\tau(x)$ je definice pravdy, platí ale i $T \vdash \psi \leftrightarrow \tau(\underline{\psi})$, tedy i $T \vdash \tau(\underline{\psi}) \leftrightarrow \neg\tau(\underline{\psi})$. To by ale znamenalo, že T je sporná. $\square$

Důkaz První věty o neúplnosti

T bezesp. rek. ax. ext. Q. Gödelovu sentenci ($\underline{\mathbb{N}} \models \psi_T$, $T \not\models \psi_T$) získáme z Věty o pevném bodě kde $\varphi(x)$ je $\neg(\exists y)Prf_T(x, y)$:

$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y)$$

Tedy ψ_T je v T ekvivalentní "ψ_T není dokazatelná v T".
Ekvivalence platí i v $\underline{\mathbb{N}}$ (z konstrukce, protože $\underline{\mathbb{N}}$ splňuje Q), a spolu s ekvivalencí z Pozorování o predikátu dokazatelnosti:

$$\underline{\mathbb{N}} \models \psi_T \;\Leftrightarrow\; \underline{\mathbb{N}} \models \neg(\exists y)Prf_T(\underline{\psi_T}, y) \;\Leftrightarrow\; T \not\vdash \psi_T$$

Stačí tedy ukázat nedokazatelnost ψ_T v T. Sporem: ať $T \vdash \psi_T$.

- Self-reference: $T \vdash \neg(\exists y)Prf_T(\underline{\psi_T}, y)$
- Důsledek o predikátu dokazatelnosti: $T \vdash (\exists y)Prf_T(\underline{\psi_T}, y)$

To by ale znamenalo, že T je sporná. $\square$

Důsledky a zesílení

Důsledek (už byl): Je-li T rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky a je-li $\underline{\mathbb{N}}$ model T, potom T není kompletní.

Důkaz: T není sporná, tedy splňuje předpoklady První věty. Víme, že G. sentence splňuje $\underline{\mathbb{N}} \models \psi_T$ a $T \not\vdash \psi_T$. Je-li T kompletní, máme $T \vdash \neg\psi_T$, z korektnosti $T \models \neg\psi_T$, tj. $\underline{\mathbb{N}} \models \neg\psi_T$, spor. $\square$

Důsledek: Teorie $\mathrm{Th}(\underline{\mathbb{N}})$ není rekurzivně axiomatizovatelná.

Důkaz: $\mathrm{Th}(\underline{\mathbb{N}})$ je extenze Q, platí v $\underline{\mathbb{N}}$. Kdyby byla rekurzivně axiomatizovatelná, podle Důsledku by [její rekurzivní axiomatizace] nebyla kompletní, ale je. $\square$

Zesílení První věty: předpoklad $\underline{\mathbb{N}} \models T$ v Důsledku je nadbytečný.

Věta (Rosserův trik, 1936): V bezesporné rekurzivně axiomatizované extenzi Robinsonovy aritmetiky existuje nezávislá sentence.

(Bez důkazu.)

Gödelova Druhá věta o neúplnosti

Efektivně daná, dostatečně bohatá T nedokáže svou bezespornost.

- bezespornost vyjádří sentence Con_T: $\neg(\exists y) Prf_T(\underline{0 = S(0)}, y)$
- všimněte si: $\underline{\mathbb{N}} \models Con_T \Leftrightarrow T \not\vdash 0 = S(0)$
- tj. Con_T opravdu vyjadřuje, že "T je bezesporná"

Věta (Gödel, 1931): Je-li T bezesporná rekurzivně axiomatizovaná extenze PA, potom Con_T není dokazatelná v T.

- všimněte si: Con_T je pravdivá v $\underline{\mathbb{N}}$ (neboť T je bezesporná)
- není třeba plná síla PA, stačí slabší předpoklad
- ukážeme si hlavní myšlenku důkazu

Myšlenka důkazu

Gödelova sentence ψ_T vyjadřuje: "Nejsem dokazatelná v T."

V důkazu První věty o neúplnosti jsme ukázali:

"Pokud je T bezesporná, potom ψ_T není dokazatelná v T."

Z toho jednak plyne, že $T \nvdash \psi_T$, neboť T bezesporná je.

Na druhou stranu to lze formulovat jako: "Platí $Con_T \rightarrow \psi_T$."

Je-li T extenze Peanovy aritmetiky, lze důkaz tohoto tvrzení zformalizovat v rámci teorie T, tedy ukázat, že:

$$T \vdash Con_T \rightarrow \psi_T$$

Kdyby platilo $T \vdash Con_T$, dostali bychom i $T \vdash \psi_T$, což je spor. $\square$

Důsledky

Důsledek: PA má model, ve kterém platí $(\exists y)Prf_{PA}(\underline{0 = S(0)}, y)$.

Důkaz: Sentence Con_{PA} není dokazatelná, tedy ani pravdivá v PA. Platí ale v $\underline{\mathbb{N}}$ (neboť PA je bezesporná), což znamená, že je Con_{PA} nezávislá v PA. V nějakém modelu tedy musí platit její negace, která je ekvivalentní $(\exists y)Prf_{PA}(\underline{0 = S(0)}, y)$. □

Poznámka: Musí to být nestandardní model PA, svědek nestandardní prvek (není hodnotou žádného numerálu).

Důsledek: PA má bezespornou rekurzivně axiomatizovanou extenzi, která "dokazuje svou spornost", tj. $T \vdash \neg Con_T$.

Důkaz: $T = PA \cup \{\neg Con_{PA}\}$ je bezesporná, neboť $PA \nvdash Con_{PA}$. Také triviálně $T \vdash \neg Con_{PA}$, tj. T 'dokazuje spornost' PA. Protože $PA \subseteq T$, platí i $T \vdash \neg Con_T$. □

Poznámka: $\underline{\mathbb{N}}$ nemůže být modelem T.

Bezespornost ZFC

Formalizace matematiky je založena na Zermelově–Fraenkelově teorii množin s axiomem výběru (ZFC). Formálně vzato to není extenze *PA*, ale můžeme v ní Peanovu aritmetiku 'interpretovat'.

Důsledek: Je-li ZFC bezesporná, není Con_{ZFC} v ZFC dokazatelná.

Pokud by tedy někdo v rámci ZFC dokázal, že ZFC bezesporná, znamenalo by to, že je ZFC sporná.