Výroková a predikátová logika - XIV

Petr Gregor

KTIML MFF UK

ZS 2013/2014

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.*

Aritmetizace syntaxe

- Konečné objekty syntaxe (symboly jazyka, termy, formule, důkazy) lze vhodně zakódovat přirozenými čísly.
- Nechť $\ulcorner\varphi\urcorner$, $\ulcorner t\urcorner$ značí kód formule φ resp. termu t. Dále nechť $\underline{\varphi}$, $\underline{t}$ značí numerál (term jazyka aritmetiky) reprezentující $\ulcorner\varphi\urcorner$ resp. $\ulcorner t\urcorner$.
- Kódování lze zvolit *"efektivní"*. Chceme např., aby funkce sub definovaná

$$sub(\ulcorner\varphi\urcorner, \ulcorner x\urcorner, \ulcorner t\urcorner) = \begin{cases} \ulcorner\varphi(x/t)\urcorner & \textit{pokud } t \textit{ je substituovatelný,} \\ 0 & \textit{jinak} \end{cases}$$

  byla reprezentovatelná v Q nějakou formulí $\psi(x_1, x_2, x_3, y)$ tak, že

$$Q \vdash \psi(\underline{a_1}, \underline{a_2}, \underline{a_3}, y) \leftrightarrow y = \underline{sub(a_1, a_2, a_3)}$$

  pro každé $a_1, a_2, a_3 \in \mathbb{N}$.
- Pak v extenzi T aritmetiky Q o formulí ψ definovaný symbol sub platí

$$T \vdash sub(\underline{a_1}, \underline{a_2}, \underline{a_3}) = \underline{a} \quad \Leftrightarrow \quad sub(a_1, a_2, a_3) = a.$$

- *Poznámka* *Detaily aritmetizace a reprezentovatelnosti vynecháme.*

Princip self-reference

- *Tato věta má 16 písmen.*

  Self-reference ve formálních systémech většinou není přímo k dispozici.

- *Následující věta má 24 písmen "Následující věta má 24 písmen".*

  Přímá reference obvykle je k dispozici, stačí, když umíme "mluvit" o posloupnostech symbolů. Uvedená věta ale není self-referenční.

- *Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen "Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen".*

  Pomocí přímé reference lze dosáhnout self-reference. Namísto *"má x písmen"* může být jiná vlastnost.

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

Věta o pevném bodě

Věta *Nechť T je bezesporné rozšíření Robinsonovy aritmetiky. Pro každou formuli $\varphi(x)$ jazyka teorie T existuje sentence ψ taková, že $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$.*

Poznámka *Sentence ψ je self-referenční, říká "splňuji podmínku φ".*

Důkaz (idea) Uvažme *zdvojující* funkci d takovou, že pro každou formuli $\chi(x)$

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

- Platí, že d je reprezentovatelná v T. Předpokládejme *(pro jednoduchost)*, že nějakým termem, který si označme d, stejně jako funkci d.
- Pak pro každou formuli $\chi(x)$ jazyka teorie T platí

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})} \qquad (1)$$

- Za ψ vezměme sentenci $\varphi(d(\underline{\varphi(d(x))}))$. Stačí ověřit $T \vdash d(\underline{\varphi(d(x))}) = \underline{\psi}$.
- To plyne z (1) pro $\chi(x)$ tvaru $\varphi(d(x))$, neboť v tom případě

$$T \vdash d(\underline{\varphi(d(x))}) = \underline{\varphi(d(\underline{\varphi(d(x))}))} \qquad \square$$

Nedefinovatelnost pravdy

Řekneme, že formule $\tau(x)$ *definuje pravdu* v aritmetické teorii T, pokud pro každou sentenci φ platí $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.

Věta *V žádném bezesporném rozšíření Robinsonovy aritmetiky neexistuje definice pravdy.*

Důkaz Dle věty o pevném bodě pro $\neg\tau(x)$ existuje sentence φ taková, že

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

Kdyby formule $\tau(x)$ definovala pravdu v T, bylo by

$$T \vdash \varphi \leftrightarrow \neg\varphi,$$

což v bezesporné teorii není možné. $\square$

Poznámka *Důkaz je založen na paradoxu lháře, sentence φ by vyjadřovala "nejsem pravdivá v T".*

Aritmetizace - predikát dokazatelnosti

- Konečná tabla lze rovněž vhodně zakódovat přirozenými čísly.
- Pro teorii T uvažme relaci $\mathrm{Prf}_T \subseteq \mathbb{N}^2$ definovanou

$$\mathrm{Prf}_T(x,y) \quad \Leftrightarrow \quad \text{(tablo) } y \text{ je důkazem (sentence) } x \text{ v } T.$$

- Je-li T rekurzivně axiomatizovaná, je Prf_T rekurzivní relace.
- Je-li T navíc extenze Robinsonovy aritmetiky Q, dá se dokázat, že Prf_T je reprezentovatelná nějakou formulí $Prf_T(x,y)$ tak, že pro každé $x, y \in \mathbb{N}$

$$\begin{aligned} Q &\vdash Prf_T(\underline{x},\underline{y}), && \text{je-li} \quad \mathrm{Prf}_T(x,y), \\ Q &\vdash \neg Prf_T(\underline{x},\underline{y}), && \text{jinak.} \end{aligned}$$

- $Prf_T(x,y)$ vyjadřuje *„y je důkaz x v T"*.
- $(\exists y)Prf_T(x,y)$ vyjadřuje *„x je dokazatelná v T"*.
- Je-li $T \vdash \varphi$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\varphi},y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\varphi},y)$.

Důkaz 1. věty o neúplnosti

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

Důkaz Nechť $\varphi(x)$ je $\neg(\exists y)Prf_T(x,y)$, vyjadřuje "*$x$ není dokazatelná v T*".

- Dle věty o pevném bodě pro $\varphi(x)$ existuje sentence ψ_T taková, že
$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y). \tag{2}$$
  ψ_T říká "*nejsem dokazatelná v T*". Přesněji, ψ_T je ekvivalentní sentenci vyjadřující, že ψ_T není dokazatelná v T. (Ekvivalence platí v $\underline{\mathbb{N}}$ i v T).
- Nejprve ukážeme, že ψ_T *není dokazatelná v T*. Kdyby $T \vdash \psi_T$, tj. ψ_T je lživá v $\underline{\mathbb{N}}$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy z (2) plyne $T \vdash \neg\psi_T$, což ale není možné, neboť T je bezesporná.
- Zbývá dokázat, že ψ_T je pravdivá v $\underline{\mathbb{N}}$. Kdyby ne, tj. $\underline{\mathbb{N}} \models \neg\psi_T$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy $T \vdash \psi_T$, což jsme již dokázali, že neplatí. $\square$

Důsledky a zesílení 1. věty

Důsledek *Je-li navíc $\underline{\mathbb{N}} \models T$, je teorie T nekompletní.*

Důkaz Kdyby byla T kompletní, pak $T \vdash \neg\psi_T$ a tedy $\underline{\mathbb{N}} \models \neg\psi_T$, což je ve sporu s $\underline{\mathbb{N}} \models \psi_T$. $\square$

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

Důkaz $\mathrm{Th}(\underline{\mathbb{N}})$ je bezesporná extenze Robinsonovy aritmetiky a má model $\underline{\mathbb{N}}$. Kdyby byla rekurzivně axiomatizovatelná, dle předchozího důsledku by byla nekompletní, ale $\mathrm{Th}(\underline{\mathbb{N}})$ je kompletní. $\square$

Gödelovu 1. větu o neúplnosti lze následovně zesílit.

Věta (Rosser) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje nezávislá sentence. Tedy T je nekompletní.*

Poznámka *Tedy předpoklad, že $\underline{\mathbb{N}} \models T$, je v prvním důsledku nadbytečný.*

Gödelova 2. věta o neúplnosti

Označme Con_T sentenci $\neg(\exists y)Prf_T(\underline{0 = 1}, y)$. Platí $\underline{\mathbb{N}} \models Con_T \Leftrightarrow T \nvdash 0 = \underline{1}$.
Tedy Con_T vyjadřuje, že *"T je bezesporná"*.

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Peanovy aritmetiky platí, že Con_T není dokazatelná v T.*

Důkaz (náznak) Nechť ψ_T je Gödelova sentence *"nejsem dokazatelná v T"*.

- V první části důkazu 1. věty o neúplnosti jsme ukázali, že

  "Je-li T bezesporná, pak ψ_T není dokazatelná v T." (3)

  Jinak vyjádřeno, platí $Con_T \rightarrow \psi_T$.
- Je-li T extenze Peanovy aritmetiky, důkaz tvrzení (3) lze formalizovat v rámci T. Tedy $T \vdash Con_T \rightarrow \psi_T$.
- Jelikož T je bezesporná dle předpokladu věty, podle (3) je $T \nvdash \psi_T$.
- Z předchozích dvou bodů vyplývá, že $T \nvdash Con_T$. $\square$

Poznámka *Taková teorie T tedy neumí dokázat vlastní bezespornost.*

Důsledky 2. věty

Důsledek *Existuje model* $\mathcal{A}$ *Peanovy aritmetiky t.ž.* $\mathcal{A} \models (\exists y) Prf_{PA}(\underline{0 = 1}, y)$.

Poznámka *$\mathcal{A}$ musí být nestandardní model PA, svědkem musí být nestandardní prvek (jiný než hodnoty numerálů).*

Důsledek *Existuje bezesporná rekurzivně axiomatizovaná extenze T Peanovy aritmetiky taková, že $T \vdash \neg Con_T$.*

Důkaz Nechť $T = PA \cup \{\neg Con_{PA}\}$. Pak T je bezesporná, neboť $PA \nvdash Con_{PA}$. Navíc $T \vdash \neg Con_{PA}$, tj. T dokazuje spornost $PA \subseteq T$, tedy i $T \vdash \neg Con_T$. □

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

Důsledek *Je-li teorie množin ZFC bezesporná, není Con_{ZFC} dokazatelná v ZFC.*

Co bude u zkoušky?

Písemná část: 90 min, pro postup do ústní části aspoň 1/2 bodů. `[vzor]`

Ústní část: cca 20 min, obvykle v pořadí odevzdávání písemné části.

Co nebude v písemné části.

- Hilbertovský kalkul.
- LD a SLD rezoluce, SLD stromy (ani v ústní části).
- Programy v Prologu (ani v ústní části).
- (Ne)rozhodnutelnost a neúplnost.

Co bude v ústní části?

(a) Definice, algoritmy či konstrukce, znění vět.

(b) Důkaz zadané věty či tvrzení.

Poznámka *Část* (a) *bude včetně nerozhodnutelnosti a neúplnosti.*

Které důkazy se zkouší?

- Cantorova věta, Königovo lemma.
- Algoritmy pro 2-SAT a Horn-SAT (důkaz korektnosti).
- Tablo metoda ve VL: syst. tablo (dokončenost, kon. důkazu), korektnost, úplnost.
- Věta o kompaktnosti VL. Hilbertovský kalkul ve VL: korektnost.
- Rezoluce ve VL: korektnost, úplnost. LI-rezoluce (úplnost pro Horn. formule).
- Sémantika PL: věta o konstantách, vlastnosti otevřených teorií, věta o dedukci.
- Tablo metoda v PL: syst. tablo (dokon., kon. důkazu), význam axiomů rovnosti.
- Tablo metoda v PL: korektnost, kanonický model, úplnost. L.-S. věta.
- Věta o kompaktnosti PL a její důsledky. Hilbertovský kalkul v PL: korektnost.
- Extenze o definice, Skolemova věta, Herbrandova věta.
- Rezoluce v PL: korektnost, lift. lemma, úplnost. LI-rezoluce (úplnost pro Horn.).
- Elementární ekvivalence, důsledky L.-S. věty. Izomorfismus a sémantika.
- ω-kategoričnost, podmínky pro konečnou a otevřenou axiomatizovatelnost.
- Invariance definovatelných množin na automorfismy.