

# Dvanáctá přednáška

NAIL062 Výroková a predikátová logika

---

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2025

## Program

- axiomatizovatelnost
- rekurzivní axiomatizace a rozhodnutelnost
- aritmetické teorie
- nerozhodnutelnost predikátové logiky
- Gödelovy věty o neúplnosti

## Materiály

**Zápisky z přednášky**, Sekce 9.4 z Kapitoly 9, Kapitola 10

## 9.4 Axiomatizovatelnost

---

Třída struktur  $K \subseteq M_L$  je:

- **axiomatizovatelná**, existuje-li teorie  $T$  taková, že  $M_L(T) = K$
- **konečně/otevřeně** axiomatiz., je-li ax. konečnou/otevřenou  $T$
- teorie  $T'$  je **konečně/otevřeně** axiomatizovatelná, platí-li to o třídě jejích modelů  $K = M_L(T')$

**Pozorování:** Je-li  $K$  axiomatizovatelná, musí být uzavřená na  $\equiv$ .

Například, jak ukážeme:

- grafy a částečná uspořádání jsou konečně i otevřeně ax.
- tělesa jsou konečně, ale ne otevřeně axiomatizovatelná
- nekonečné grupy jsou axiomatizovatelné, ale ne konečně
- konečné grafy nejsou axiomatizovatelné

# Neaxiomatizovatelnost konečných modelů

**Věta:** Má-li  $T$  libovolně velké konečné modely, má i nekonečný model. Potom není třída jejích konečných modelů axiomatizovatelná.

**Důkaz:** Je-li jazyk bez rovnosti, vezmeme kanonický model pro bezespornou větev v tablu z  $T$  pro  $F \perp$  ( $T$  je bezesporná).

Je-li jazyk s rovností, přidáme spočetně mnoho nových konst.

symbolů  $c_i$  a vezmeme extenzi:  $T' = T \cup \{\neg c_i = c_j \mid i \neq j \in \mathbb{N}\}$

Každá konečná část  $T'$  má model: buď  $k$  největší, že  $c_k$  je v této konečné části: lib.  $\geq (k+1)$ -prvkový model,21 interpretuj  $c_0, \dots, c_k$  jako různé prvky.

**Věta o kompaktnosti** dává model  $T'$ , ten je nekonečný, redukt na původní jazyk (zapomenutí  $c_i^A$ ) je nekonečný model  $T$ .  $\square$

- např. konečné grafy nejsou axiomatizovatelné
- nekonečné modely teorie jsou vždy axiomatizovatelné, máme-li rovnost: stačí přidat 'existuje alespoň  $n$  prvků' pro vš.  $n \in \mathbb{N}$

# Konečná axiomatizovatelnost

**Věta (O konečné axiomatizovatelnosti):**  $K \subseteq M_L$  je konečně axiomatizovatelná, právě když  $K$  i  $\overline{K} = M_L \setminus K$  jsou axiomatizovatelné.

**Důkaz:**  $\Rightarrow$  Je-li  $K$  axiomatizovatelná **sentencemi**  $\varphi_1, \dots, \varphi_n$  (vezmi gen. uzávěry), potom  $\neg(\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n)$  axiomatizuje  $\overline{K}$ .

$\Leftarrow$  Bud'  $K = M(T)$  a  $\overline{K} = M(S)$ . Potom  **$T \cup S$  je sporná**, neboť:

$$M(T \cup S) = M(T) \cap M(S) = K \cap \overline{K} = \emptyset$$

**Věta o kompaktnosti** dává konečné  $T' \subseteq T$  a  $S' \subseteq S$  takové, že:

$$\emptyset = M(T' \cup S') = M(T') \cap M(S')$$

Nyní si všimněme, že platí:

$$M(T) \subseteq M(T') \subseteq \overline{M(S')} \subseteq \overline{M(S)} = M(T)$$

Tím jsme dokázali, že  **$M(T) = M(T')$** , neboli  $T'$  je konečná axiomatizace  $K$ . □

# Tělesa charakteristiky 0 nejsou konečně axiomatizovatelná

Bud'  $T$  teorie těles. Těleso  $\mathcal{A} = \langle A, +, -, 0, \cdot, 1 \rangle$  je

- **charakteristiky  $p$** , je-li  $p$  nejmenší prvočíslo takové, že  $\mathcal{A} \models p1 = 0$ , kde  $p1$  je term  $1 + 1 + \dots + 1$  (s  $p$  jedničkami),
- **charakteristiky 0**, pokud není charakteristiky  $p$  pro žádné  $p$ .
- Tělesa charakteristiky  $p$  jsou konečně axiomatizovatelná:

$$T_p = T \cup \{p1 = 0\}$$

- Tělesa char. 0 jsou axiomatizovatelná, ale ne konečně:

$$T_0 = T \cup \{\neg p1 = 0 \mid p \text{ prvočíslo}\}$$

**Tvrzení:** Třída  $K$  těles char. 0 není konečně axiomatizovatelná.

**Důkaz:** Stačí ukázat, že  $\overline{K}$  (tělesa nenulové char. a netělesa) není axiomatizovatelná. **Sporem:**  $\overline{K} = M(S)$ . Potom  $S' = S \cup T_0$  má model, neboť každá konečná část má model: těleso charakteristiky větší než jakékoliv  $p$  z axiomu  $T_0$  tvaru  $\neg p1 = 0$ . Je-li  $\mathcal{A}$  je model  $S'$ , potom  $\mathcal{A} \in M(S) = \overline{K}$ . Zároveň ale  $\mathcal{A} \in M(T_0) = K$ , spor.  $\square$

# Otevřená axiomatizovatelnost

**Tvrzení:** Je-li  $T$  otevřeně axiomatizovatelná, potom je každá podstruktura modelu  $T$  také modelem  $T$ .

**Důkaz:** Buď  $T'$  otevřená axiomatizace  $T$ ,  $\mathcal{A}$  model  $T'$ ,  $\mathcal{B} \subseteq \mathcal{A}$ .

Pro každou  $\varphi \in T'$  platí  $\mathcal{B} \models \varphi$  ( $\varphi$  je otevřená), tedy i  $\mathcal{B} \models T'$ .  $\square$

**Poznámka:** Platí i obráceně, je-li každá podstruktura modelu také model, potom je otevřeně axiomatizovatelná. (Důkaz neuvedeme.)

- DeLO není otevřeně axiomatizovatelná, např. žádná konečná podstruktura modelu DeLO není hustá
- teorie těles není otevřeně axiomatizovatelná, podstruktura  $\mathbb{Z} \subseteq \mathbb{Q}$  není těleso, nemá inverzní prvek k 2 vůči násobení
- pro dané  $n \in \mathbb{N}$  jsou nejvýše  $n$ -prvkové grupy otevřeně axiomatizovatelné (i jejich podgrupy jsou nejvýše  $n$ -prvkové); k (otevřené) teorii grup stačí přidat:  $\bigvee_{1 \leq i < j \leq n+1} x_i = x_j$



# KAPITOLA 10:

## NEROZHODNUTELNOST A NEÚPLNOST

---

Jak lze s teoriemi pracovat algoritmicky?

+ zlatý hřeb přednášky: Gödelovy věty o neúplnosti (1931)

- ukazují limity formálního přístupu
- zastavily program formalizace matematiky
- pojem **algoritmu** budeme chápat jen intuitivně
- technické podrobnosti důkazů vynecháme

Typicky potřebujeme spočetný jazyk.

## 10.1 Rekurzivní axiomatizace a rozhodnutelnost

---

# Rekurzivní axiomatizace

- v dokazování povolujeme nekonečné teorie, jak jsou zadané?
- pro ověření že daný důkaz (např. tablo, rezoluční zamítnutí) je korektní potřebujeme algoritmický přístup ke všem axiomům
- mohli bychom požadovat **enumerátor** pro  $T$ , tj. algoritmus, který vypisuje axiomy z  $T$ , a každý axiom někdy vypíše
- ale kdyby byl v důkazu chybný axiom, nikdy bychom se to nedozvěděli: stále bychom čekali, zda ho enumerátor vypíše
- proto požadujeme silnější vlastnost:

$T$  je **rekurzivně axiomatizovaná**, pokud existuje algoritmus, který pro každou vstupní formuli  $\varphi$  doběhne a odpoví, zda  $\varphi \in T$ .

(ekvivalentní enumerátoru vypisujícím axiomy v lexikograf. pořadí)

Můžeme v dané teorii 'algoritmicky rozhodovat pravdu'?

- $T$  je **rozhodnutelná**, pokud existuje algoritmus, který pro každou vstupní formuli  $\varphi$  doběhne a odpoví, zda  $T \models \varphi$ ,
- $T$  je **částečně rozhodnutelná**, existuje-li algoritmus, který:
  - pokud  $T \models \varphi$ , doběhne a odpoví "ano"
  - pokud  $T \not\models \varphi$ , buď nedoběhne, nebo doběhne a odpoví "ne"

**Tvrzení:** Je-li  $T$  je rekurzivně axiomatizovaná, potom:

(i)  $T$  je část. rozhod.      (ii) je-li navíc kompletní, je rozhodnutelná

**Důkaz:** (i) Algoritmus konstruuje systematické tablo z  $T$  pro  $\mathbb{F}\varphi$ ; stačí enumerátor pro  $T$ , nebo postupně generovat vš. sentence a testovat, jsou-li v  $T$ . Je-li  $T \models \varphi$ , konstrukce skončí, ověříme, že je tablo sporné. (Jinak skončit nemusí.)

(ii) Víme, že buď  $T \vdash \varphi$  nebo  $T \vdash \neg\varphi$ . Paralelně konstruueme tablo pro  $\mathbb{F}\varphi$  a pro  $\mathbb{T}\varphi$  (důkaz a zamítnutí  $\varphi$  z  $T$ ). Jedna z konstrukcí po konečně mnoha krocích skončí.

# Rekurzivně spočetná kompletace

$T$  má **rekurzivně spočetnou kompletaci**, je-li (nějaká) množina až na  $\sim$  všech kompletních jednoduchých extenzí  $T$  spočetná, a **rekurzivně spočetná**, tj. existuje algoritmus, který pro vstup  $(i, j)$  vypíše  $i$ -tý axiom  $j$ -té extenze (v nějakém uspořádání), nebo odpoví, že už neexistuje.

**Tvrzení:** Je-li  $T$  rekurzivně axiomatizovaná a má rekurzivně spočetnou kompletaci, potom je rozhodnutelná.

**Důkaz:** Buď  $T \vdash \varphi$ , nebo existuje protipříklad  $\mathcal{A} \not\models \varphi$ , tj. kompl. jedn. extenze  $T_i$ , že  $T_i \not\models \varphi$ . Kompletnost  $T_i$  dává  $T_i \vdash \neg\varphi$ .

Algoritmus paralelně konstruuje tablo důkaz  $\varphi$  z  $T$  a (postupně) tablo důkazy  $\neg\varphi$  ze všech kompletních jedn. extenzí  $T_1, T_2, \dots$ . (Je-li jich nekonečně mnoho, uděláme **dovetailing**: 1. krok 1. tabla, potom 2. krok 1., 1. krok 2., 3. krok 1., 2. krok 2., 1. krok 3., atd.)

Alespoň jedno z tabel je sporné, můžeme předpokládat konečné, algoritmus ho po konečně mnoha krocích zkonstruuje.  $\square$

Následující teorie jsou rekurzivně axiomatizované a mají rekurzivně spočetnou kompletaci, tedy jsou rozhodnutelné:

- (a) Teorie čisté rovnosti
- (b) Teorie unárního predikátu ( $T = \emptyset$ ,  $L = \langle U \rangle$  s rovností)
- (c) Teorie hustých lineárních uspořádání DeLO\*
- (d) Teorie Booleových algeber (Alfred Tarski 1940),
- (e) Teorie algebraicky uzavřených těles (Tarski 1949),
- (f) Teorie komutativních grup (Wanda Szmielew 1955).

# Rekurzivní axiomatizovatelnost

Kdy lze třídu struktur ‘efektivně (algoritmicky) popsat’?

$K \subseteq M_L$  je **rek. axiomatizovatelná**, pokud existuje rek. axiomatizovaná  $T$ , že  $K = M_L(T)$ .  $T'$  je **rek. axiomatizovatelná**, platí-li to pro třídu jejích modelů (tj. je-li ekvivalentní rek. axiomatizované teorii).

(podobně lze definovat **rek. spočetnou axiomatizovatelnost**)

**Tvrzení:** Je-li  $\mathcal{A}$  konečná struktura v konečném jazyce s rovností, potom je teorie  $\text{Th}(\mathcal{A})$  rekurzivně axiomatizovatelná.

(z toho plyne i rozhodnutelnost  $\text{Th}(\mathcal{A})$ , ale  $\mathcal{A} \models \varphi$  lze ověřit přímo)

**Důkaz:** Buď  $A = \{a_1, \dots, a_n\}$ .  $\text{Th}(\mathcal{A})$  axiomatizujeme sentencí “existuje právě  $n$  prvků  $a_1, \dots, a_n$  splňujících právě ty **základní vztahy** o funkčních hodnotách a relacích, které platí v  $\mathcal{A}$ ”.

Např. je-li  $f^{\mathcal{A}}(a_4, a_2) = a_{17}$ , přidej atom. formuli  $f(x_{a_4}, x_{a_2}) = x_{a_{17}}$ , je-li  $(a_3, a_3, a_1) \notin R^{\mathcal{A}}$  přidej  $\neg R(x_{a_3}, x_{a_3}, x_{a_1})$ .  $\square$



Pro následující struktury je  $\text{Th}(\mathcal{A})$  rekurzivně axiomatizovatelná:

- $\langle \mathbb{Z}, \leq \rangle$ , jde o tzv. teorii **diskrétních lineárních uspořádání**
- $\langle \mathbb{Q}, \leq \rangle$ , jde o teorii DeLO
- $\langle \mathbb{N}, S, 0 \rangle$ , teorie **následníka s nulou**
- $\langle \mathbb{N}, S, +, 0 \rangle$ , **Presburgerova aritmetika**
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$ , teorie **reálně uzavřených těles**, znamená že lze algoritmicky rozhodovat Euklid. geometrii (Tarski, 1949)
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$ , teorie **algebraicky uzavřených těles char. 0**

**Důsledek:** Pro struktury výše platí, že  $\text{Th}(\mathcal{A})$  je rozhodnutelná.

**Důkaz:**  $\text{Th}(\mathcal{A})$  je vždy kompletní.

Teorie **standardního modelu aritmetiky**  $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$  ale **není** rekurzivně axiomatizovatelná (viz První Gödelova věta o neúplnosti).

## 10.2 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  $\mathbb{N}$ , 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  $\mathbb{N} \models \varphi[e(x_1/a_1, \dots, x_n/a_n)]$

(Důkaz vynecháme.)

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

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

- mnohem lepší aproximace  $\text{Th}(\underline{\mathbb{N}})$
- 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  $\varphi$  rozhodne, zda je logicky platná.

- tj. zda je formule  $\varphi$  [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:**  $p(x_1, \dots, x_n) = 0$ , 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 celočísl. koeficienty je nerozhodnutelný.  
(Důkaz neuvedeme.)

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

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

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



# Důkaz nerozhodnutelnosti predikátové logiky

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

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

Buď  $\psi_Q$  konjunkce (gen. uzávěrů) axiomů  $Q$  (je konečná). Zřejmě:

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

Díky úplnosti a korektnosti je to ale ekvivalentní  $\models \psi_Q \rightarrow \varphi$ .

Dostáváme:

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

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

## 10.4 Gödelovy věty

---

# První věta o neúplnosti + důsledek o nekompletnosti

**Věta (Gödel 1931):** Je-li  $T$  bezsporná rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky, potom existuje sentence, která je pravdivá v  $\mathbb{N}$ , 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  $\mathbb{N}$  zatímco **dokazatelnost** v  $T$  (samozřejmě pravdivá v  $T$  je v  $T$  i dokazatelná)
- **bezspornost** 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  $\mathbb{N}$  modelem  $T$ , potom  $T$  není kompletní.

**Důkaz:** Vezměme Gödelovu sentenci  $\varphi$  ( $\mathbb{N} \models \varphi$ ,  $T \not\models \varphi$ ). Je-li  $T$  kompletní, víme  $T \vdash \neg\varphi$ , z korektnosti  $T \models \neg\varphi$ , tedy  $\mathbb{N} \models \neg\varphi$ .  $\square$

- 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

- 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  $\varphi$  bude  $\lceil \varphi \rceil$  příslušný kód,  $\varphi$  odpovídající  $\lceil \varphi \rceil$ -tý numerál
- pro danou  $T$  máme binární relaci  $\text{Proof}_T \subseteq \mathbb{N}^2$  definovanou  $(n, m) \in \text{Proof}_T \Leftrightarrow n = \lceil \varphi \rceil, m = \lceil \tau \rceil, \tau \text{ je tablo důkaz } \varphi \text{ z } T$
- je-li  $T$  rek. axiomatizovaná, je relace  $\text{Proof}_T \subseteq \mathbb{N}^2$  **rekurzivní** (lze algoritmicky ověřit korektnost tabla, tj.  $(n, m) \in \text{Proof}_T$ )
- klíčovou technickou částí důkazu První věty je fakt, že relaci  $\text{Proof}_T$  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  $\text{Proof}_T$ , tj. pro každá  $n, m \in \mathbb{N}$ :

- je-li  $(n, m) \in \text{Proof}_T$ , 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  $\varphi$  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 uvozovky):

```
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  $\psi$  taková, že:

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

- také “diagonalizační lemma” nebo “self-referenční” lemma
- $\psi$  je **self-referenční**, říká o sobě: “já splňuji vlastnost  $\varphi$ ”
- 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**  $d: \mathbb{N} \rightarrow \mathbb{N}$  dekoduje vstup  $n$  jako  $\varphi(x)$ , dosadí numerál  $\underline{n}$ , znovu zakóduje: pro vš.  $\chi(x)$  platí:

$$d(\lceil \chi(x) \rceil) = \lceil \chi(\underline{\chi(x)}) \rceil$$

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':

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

Hledaná self-referenční sentence  $\psi$  je sentence:

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

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

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

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  $\varphi(d(x))$ . □

$\psi$  tedy říká: »Následující věta zapsaná jednou a ještě jednou v uvozovkách má vlastnost  $\varphi$ . «Následující věta zapsaná jednou a ještě jednou v uvozovkách má vlastnost  $\varphi$ .» 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  $\psi$  platí:  $T \vdash \psi \leftrightarrow \tau(\underline{\psi})$
- kdyby existovala, místo dokazování by stačilo spočíst kód  $\lceil \psi \rceil$ , dosadit numerál  $\underline{\psi}$  do  $\tau$ , 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  $\psi$  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 ( $\underline{N} \models \psi_T, T \not\models \psi_T$ ) 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  $\psi_T$  je v  $T$  ekvivalentní “ $\psi_T$  není dokazatelná v  $T$ ”.

Ekvivalence platí i v  $\underline{N}$  (z konstrukce, protože  $\underline{N}$  splňuje  $Q$ ), a spolu s ekvivalencí z Pozorování o predikátu dokazatelnosti:

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

Stačí tedy ukázat nedokazatelnost  $\psi_T$  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. □

## Důsledky a zesílení

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

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

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

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

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

**Věta (Rosserův trik, 1936):** V bezsporné 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:  $\mathbb{N} \models Con_T \Leftrightarrow T \not\models 0 = S(0)$
- 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  $\mathbb{N}$  (neboť  $T$  je bezesporná)
- není třeba plná síla  $PA$ , stačí slabší předpoklad
- ukážeme si hlavní myšlenku důkazu

Gödelova sentence  $\psi_T$  vyjadřuje: “Nejsem dokazatelná v  $T$ .”

V důkazu První věty o neúplnosti jsme ukázali:

“Pokud je  $T$  bezesporná, potom  $\psi_T$  není dokazatelná v  $T$ .”

Z toho jednak plyne, že  $T \not\vdash \psi_T$ , 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.  $\square$

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

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

**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  $PA \not\vdash Con_{PA}$ . Také triviálně  $T \vdash \neg Con_{PA}$ , tj.  $T$  ‘dokazuje spornost’  $PA$ . Protože  $PA \subseteq T$ , platí i  $T \vdash \neg Con_T$ .  $\square$

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

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 je ZFC bezesporná, znamenalo by to, že je ZFC sporná.