

# Výroková a predikátová logika - XIII

Petr Gregor

KTIML MFF UK

ZS 2020/21

# Konečná axiomatizovatelnost

**Věta** *Nechť  $K \subseteq M(L)$  a  $\overline{K} = M(L) \setminus K$ , kde  $L$  je jazyk. Pak  $K$  je **konečně axiomatizovatelná**, právě když  $K$  i  $\overline{K}$  jsou axiomatizovatelné.*

**Důkaz** ( $\Rightarrow$ ) Je-li  $T$  konečná axiomatizace  $K$  v **uzavřeném** tvaru, pak teorie s jediným axiomem  $\bigvee_{\varphi \in T} \neg \varphi$  axiomatizuje  $\overline{K}$ . Nyní dokažme ( $\Leftarrow$ ).

- Nechť  $T, S$  jsou teorie jazyka  $L$  takové, že  $M(T) = K$ ,  $M(S) = \overline{K}$ .
- Pak  $M(T \cup S) = M(T) \cap M(S) = \emptyset$  a dle věty o **kompaktnosti** existují konečné  $T' \subseteq T$  a  $S' \subseteq S$  takové, že  $\emptyset = M(T' \cup S') = M(T') \cap M(S')$ .
- Jelikož

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

je  $M(T) = M(T')$ , tj. konečná  $T'$  axiomatizuje  $K$ .  $\square$

# Konečná axiomatizovatelnost - příklad

Nechť  $T$  je teorie těles. Řekneme, že těleso  $\mathcal{A} = \langle A, +, -, \cdot, 0, 1 \rangle$  je

- **charakteristiky 0**, neexistuje-li žádné  $p \in \mathbb{N}^+$  takové, že  $\mathcal{A} \models p1 = 0$ , kde  $p1$  značí term  $1 + 1 + \dots + 1$  ( $+$  aplikováno  $(p - 1)$ -krát).
- **charakteristiky  $p$** , kde  $p$  je prvočíslo, je-li  $p$  je nejmenší t.ž.  $\mathcal{A} \models p1 = 0$ .
- Třída těles charakteristiky  $p$  pro  $p$  prvočíslo je **konečně** axiomatizována teorií  $T \cup \{p1 = 0\}$ .
- Třída těles charakteristiky 0 je axiomatizována (**nekonečnou**) teorií  $T' = T \cup \{p1 \neq 0 \mid p \in \mathbb{N}^+\}$ .

**Tvrzení** Třída  $K$  těles charakteristiky 0 není **konečně** axiomatizovatelná.

**Důkaz** Stačí dokázat, že  $\overline{K}$  není axiomatizovatelná. Kdyby  $M(S) = \overline{K}$ , tak  $S' = S \cup T'$  má model  $\mathcal{B}$ , neboť každá konečná  $S^* \subseteq S'$  má model (těleso prvočíselné charakteristiky větší než jakékoliv  $p$  vyskytující se v axiomech  $S^*$ ). Pak ale  $\mathcal{B} \in M(S) = \overline{K}$  a zároveň  $\mathcal{B} \in M(T') = K$ , což není možné.  $\square$

# Otevřená axiomatizovatelnost

**Věta** *Je-li teorie  $T$  otevřeně axiomatizovatelná, pak každá podstruktura modelu  $T$  je rovněž modelem  $T$ .*

**Důkaz** Nechť  $T'$  je otevřená axiomatika  $M(T)$ ,  $\mathcal{A} \models T'$  a  $\mathcal{B} \subseteq \mathcal{A}$ . Víme, že pro každé  $\varphi \in T'$  je  $\mathcal{B} \models \varphi$ , neboť  $\varphi$  je otevřená. Tedy  $\mathcal{B}$  je modelem  $T'$ .  $\square$

**Poznámka** *Platí i obrácená implikace, tj. je-li každá podstruktura modelu teorie  $T$  rovněž modelem  $T$ , pak  $T$  je otevřeně axiomatizovatelná.*

*Např. teorie DeLO není otevřeně axiomatizovatelná, neboť např. konečná podstruktura modelu DeLO není modelem DeLO.*

*Např. nejvýše  $n$ -prvkové grupy pro pevné  $n > 1$  jsou otevřeně axiomatizovány*

$$T \cup \left\{ \bigvee_{\substack{i,j \leq n \\ i \neq j}} x_i = x_j \right\},$$

*kde  $T$  je (otevřená) teorie grup.*

# Rekurzivní axiomatizace a rozhodnutelnost

- Intuitivní pojem “*algoritmus*” lze přesně formalizovat (např. pomocí TS).
- Teorie  $T$  je *rekurzivně axiomatizovaná*, pokud existuje algoritmus, který pro každou vstupní formuli  $\varphi$  *skončí* a oznámí, zda  $\varphi \in T$ .
- Teorie  $T$  je *rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli  $\varphi$  *skončí* a oznámí, zda  $\varphi \in Thm(T)$ .
- Teorie  $T$  je *částečně rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli  $\varphi$  *skončí*, právě když  $\varphi \in Thm(T)$ .

**Tvrzení** Pro každou rekurzivně axiomatizovanou teorii  $T$ ,

- (i)  $T$  je *částečně rozhodnutelná*,
- (ii) je-li navíc  $T$  *kompletní*, je  $T$  *rozhodnutelná*.

**Důkaz** Konstrukce systematického tabla z  $T$  s  $F\varphi$  v kořeni poskytuje algoritmus, který rozpoznává  $T \vdash \varphi$ . Je-li navíc  $T$  kompletní, *paralelní* konstrukce pro  $F\varphi$  resp.  $T\varphi$  v kořeni rozhoduje, zda  $T \vdash \varphi$  či  $T \vdash \neg\varphi$ . □

# 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 (takový axiom či extenze) neexistuje.

**Tvrzení** *Je-li teorie  $T$  rekurzivně axiomatizovaná a množina všech (až na ekvivalenci) jejích jednoduchých kompletních extenzí je rekurzivně spočetná, je  $T$  rozhodnutelná.*

**Důkaz** Díky rek. axiomatizaci poskytuje konstrukce systematického tabla z  $T$  s  $F\varphi$  v kořeni algoritmus pro rozpoznání  $T \vdash \varphi$ . Pokud ale  $T \not\vdash \varphi$ , 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 sestojí 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  $n \geq 1$ ,
$$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0),$$
kde  $y^k$  je zkratka za term  $y \cdot y \cdot \dots \cdot y$  ( $\cdot$  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 rekurzivně axiomatizovaná teorie  $T$  jazyka  $L$  s  $M(T) = K$ .
- **Teorie**  $T$  je **rekurzivně axiomatizovatelná**, pokud  $M(T)$  je rekurzivně axiomatizovatelná.

**Tvrzení** Pro každou **konečnou** strukturu  $\mathcal{A}$  v konečném jazyce s rovností je  $\text{Th}(\mathcal{A})$  rekurzivně axiomatizovatelná. Tedy,  $\text{Th}(\mathcal{A})$  je **rozhodnutelná**.

**Důkaz** Necht'  $A = \{a_1, \dots, a_n\}$ . Teorii  $\text{Th}(\mathcal{A})$  axiomatizujeme jednou sentencí (tedy rekurzivně) kompletně popisující  $\mathcal{A}$ . Bude tvaru “existuje právě  $n$  prvků  $a_1, \dots, a_n$  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  $\text{Th}(\mathcal{A})$ .

- $\langle \mathbb{Z}, \leq \rangle$ , 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  $\text{Th}(\mathcal{A})$  **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)

$$S(x) \neq 0$$

$$S(x) = S(y) \rightarrow x = y$$

$$x + 0 = x$$

$$x + S(y) = S(x + y)$$

$$x \cdot 0 = 0$$

$$x \cdot S(y) = x \cdot y + x$$

$$x \neq 0 \rightarrow (\exists y)(x = S(y))$$

$$x \leq y \leftrightarrow (\exists z)(z + x = y)$$

*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  $\varphi(x, \bar{y})$  jazyka  $L$  axiom

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

*Poznámka*  $PA$  je poměrně dobrou aproximací  $\text{Th}(\underline{\mathbb{N}})$ , 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)

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

# Hilbertův 10. problém

- Necht'  $p(x_1, \dots, x_n)$  je polynom s celočíselnými koeficienty.  
Má **Diofantická rovnice**  $p(x_1, \dots, x_n) = 0$  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  $p(x_1, \dots, x_n)$ ,  $q(x_1, \dots, x_n)$  s **přirozenými** koeficienty, zda

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

# Nerozhodnutelnost 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  $\varphi(x_1, \dots, x_n)$  jazyka aritmetiky

$$Q \vdash \varphi(x_1/\underline{a_1}, \dots, x_n/\underline{a_n}) \Leftrightarrow \underline{\mathbb{N}} \models \varphi[e(x_1/a_1, \dots, x_n/a_n)]$$

pro každé  $a_1, \dots, a_n \in \mathbb{N}$ , kde  $\underline{a_i}$  značí  $a_i$ -tý numerál.

- Speciálně, pro  $\varphi$  tvaru  $(\exists x_1) \dots (\exists x_n)(p(x_1, \dots, x_n) = q(x_1, \dots, x_n))$ , kde  $p, q$  jsou polynomy s přirozenými koeficienty (numerály), platí

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

kde  $\psi$  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  $\mathbb{N}$  a **nedokazatelná** v  $T$ .*

## Poznámky

- “Rekurzivně axiomatizovaná” znamená, že je “efektivně zadaná”.
- “Extenze  $R$ . aritmetiky” znamená, že je “**základní aritmetické síly**”.
- Je-li navíc  $\mathbb{N} \models T$ , je teorie  $T$  **nekompletní**.
- V důkazu sestavená sentence vyjadřuje “**nejsem dokazatelná v  $T$** ”.
- Důkaz je založen na dvou principech:
  - (a) **aritmetizaci syntaxe**,
  - (b) **self-referenci**.

# Aritmetizace - predikát dokazatelnosti

- **Konečné objekty** syntaxe (symboly jazyka, termy, formule, konečná tabla, tablo důkazy) lze vhodně **zakódovat** přirozenými čísly.
- Nechť  $\lceil \varphi \rceil$  značí kód formule  $\varphi$  a nechť  $\underline{\varphi}$  značí **numerál** (term jazyka aritmetiky) reprezentující  $\lceil \varphi \rceil$ .
- Je-li  $T$  rekurzivně axiomatizovaná, je relace  $\text{Prf}_T \subseteq \mathbb{N}^2$  **rekurzivní**.

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

- Je-li  $T$  navíc extenze Robinsonovy aritmetiky  $Q$ , dá se dokázat, že  $\text{Prf}_T$  je **reprezentovatelná** nějakou formulí  $\text{Prf}_T(x, y)$  tak, že pro každé  $x, y \in \mathbb{N}$

$$Q \vdash \text{Prf}_T(\underline{x}, \underline{y}), \quad \text{je-li } \text{Prf}_T(x, y),$$

$$Q \vdash \neg \text{Prf}_T(\underline{x}, \underline{y}), \quad \text{jinak.}$$

- $\text{Prf}_T(x, y)$  vyjadřuje “ $y$  je důkaz  $x$  v  $T$ ”.
- $(\exists y)\text{Prf}_T(x, y)$  vyjadřuje “ $x$  je dokazatelná v  $T$ ”.
- Je-li  $T \vdash \varphi$ , pak  $\mathbb{N} \models (\exists y)\text{Prf}_T(\underline{\varphi}, y)$  a navíc  $T \vdash (\exists y)\text{Prf}_T(\underline{\varphi}, y)$ .

# 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  $\psi$  taková, že  $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$ .*

**Poznámka** *Sentence  $\psi$  je self-referenční, říká “**splňuji podmínku  $\varphi$** ”.*

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

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

- 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

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

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

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

# Nedefinovatelnost pravdy

Řekneme, že formule  $\tau(x)$  *definuje pravdu* v aritmetické teorii  $T$ , pokud pro každou sentenci  $\varphi$  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  $\varphi$  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  $\varphi$  by vyjadřovala “nejsem pravdivá v  $T$ ”.

# 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** Necht'  $\varphi(x)$  je  $\neg(\exists y)Prf_T(x, y)$ , vyjadřuje “ $x$  není dokazatelná v  $T$ ”.

- Dle věty o pevném bodě pro  $\varphi(x)$  existuje sentence  $\psi_T$  taková, že

$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y). \quad (2)$$

$\psi_T$  říká “**nejsem dokazatelná v  $T$** ”. Přesněji,  $\psi_T$  je ekvivalentní sentenci vyjadřující, že  $\psi_T$  není dokazatelná v  $T$ . (Ekvivalence platí v  $\mathbb{N}$  i v  $T$ ).

- Nejprve ukážeme, že  $\psi_T$  *není dokazatelná v  $T$* . Kdyby  $T \vdash \psi_T$ , tj.  $\psi_T$  je lživá v  $\mathbb{N}$ , pak  $\mathbb{N} \models (\exists y)Prf_T(\underline{\psi_T}, y)$  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  $\psi_T$  je pravdivá v  $\mathbb{N}$ . Kdyby ne, tj.  $\mathbb{N} \models \neg\psi_T$ , pak  $\mathbb{N} \models (\exists y)Prf_T(\underline{\psi_T}, y)$ . 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**  $\text{Th}(\underline{\mathbb{N}})$  *není rekurzivně axiomatizovatelná.*

**Důkaz**  $\text{Th}(\underline{\mathbb{N}})$  je bezesporná extenze Robinsonovy aritmetiky a má model  $\underline{\mathbb{N}}$ . Kdyby byla rekurzivně axiomatizovatelná, dle předchozího důsledku by byla nekompletní, ale  $\text{Th}(\underline{\mathbb{N}})$  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  $\neg(\exists y)Prf_T(\underline{0} = \underline{1}, y)$ . Platí  $\mathbb{N} \models Con_T \Leftrightarrow T \not\vdash 0 = \underline{1}$ .  
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)** Necht'  $\psi_T$  je Gödelova sentence “nejsem dokazatelná v  $T$ ”.

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

$$\text{“Je-li } T \text{ bezesporná, pak } \psi_T \text{ není dokazatelná v } T\text{.”} \quad (3)$$

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  $T \not\vdash \psi_T$ .
- Z předchozích dvou bodů vyplývá, že  $T \not\vdash Con_T$ .  $\square$

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

## Důsledky 2. věty

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

**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  $T \vdash \neg \text{Con}_T$ .

**Důkaz** Nechť  $T = PA \cup \{\neg \text{Con}_{PA}\}$ . Pak  $T$  je bezesporná, neboť  $PA \not\vdash \text{Con}_{PA}$ . Navíc  $T \vdash \neg \text{Con}_{PA}$ , tj.  $T$  dokazuje spornost  $PA \subseteq T$ , tedy i  $T \vdash \neg \text{Con}_T$ .  $\square$

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

**Důsledek** Je-li teorie množin ZFC bezesporná, není  $\text{Con}_{ZFC}$  dokazatelná v ZFC.