První Gödelova věta z pražské perspektivy, její strukturální důkaz

Vítězslav Švejdar

Karlova Univerzita v Praze, http://www.cuni.cz/~svejdar/

Gödelovy dny, Brno, duben 2016

Obsah

První Gödelova věta

Předběžné (nepřesné) znění

Každá rozumná a dostatečně silná axiomatická teorie je neúplná (a nerozhodnutelná).

První Gödelova věta

Předběžné (nepřesné) znění

Každá rozumná a dostatečně silná axiomatická teorie je neúplná (a nerozhodnutelná).

Axiomatická teorie je dána jazykem a množinou axiomů (množinou sentencí v onom jazyce).

První Gödelova věta

Předběžné (nepřesné) znění

Každá rozumná a dostatečně silná axiomatická teorie je neúplná (a nerozhodnutelná).

Axiomatická teorie je dána jazykem a množinou axiomů (množinou sentencí v onom jazyce).
Aritmetický jazyk je jazyk $\{+, \cdot, 0, \mathrm{S}, \leq, <\}$ obsahující symboly pro sčítání a násobení, konstantu pro číslo nula, symbol S pro následnickou funkci (přičítání jedničky) a symboly pro neostré a ostré uspořádání.

První Gödelova věta

Předběžné (nepřesné) znění

Každá rozumná a dostatečně silná axiomatická teorie je neúplná (a nerozhodnutelná).

Axiomatická teorie je dána jazykem a množinou axiomů (množinou sentencí v onom jazyce).
Aritmetický jazyk je jazyk $\{+, \cdot, 0, \mathrm{S}, \leq, <\}$ obsahující symboly pro sčítání a násobení, konstantu pro číslo nula, symbol S pro následnickou funkci (přičítání jedničky) a symboly pro neostré a ostré uspořádání.
Teorie T v aritmetickém jazyce je korektní, jestliže $\mathbb{N} \models T$, tj. jestliže $\mathbb{N}$ je jedním z modelů teorie T, neboli jestliže každá sentence dokazatelná v T platí v $\mathbb{N}$.

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$ splňujících nerovnosti $\forall i(r_i < q_i)$ existuje číslo $a < \prod_{i=1}^{n}$ takové, že $\forall i(\mathrm{Mod}(a, q_i) = r_i)$.

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$ splňujících nerovnosti $\forall i(r_i < q_i)$ existuje číslo $a < \prod_{i=1}^{n}$ takové, že $\forall i(\mathrm{Mod}(a, q_i) = r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$ splňujících nerovnosti $\forall i(r_i < q_i)$ existuje číslo $a < \prod_{i=1}^{n}$ takové, že $\forall i(\mathrm{Mod}(a, q_i) = r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?
Ano, 321.

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$ splňujících nerovnosti $\forall i(r_i < q_i)$ existuje číslo $a < \prod_{i=1}^{n}$ takové, že $\forall i(q_i \mid a - r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?
Ano, 321.

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$
existuje číslo $a < \prod_{i=1}^{n}$ takové, že $\forall i(q_i \mid a - r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?
Ano, 321.

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$
existuje číslo a takové, že $\forall i(q_i \mid a - r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?
Ano, 321.

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$
existuje číslo a takové, že $\forall i(q_i \mid a - r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?
Ano, 321.

Logická analýza důkazu čínské zbytkové věty vede (může vést) k rozhodnutí uvažovat dělitelnost (nikoliv dělení) v oboru celých (nikoliv přirozených) čísel a k teorii T, jejíž jazyk je $\{+, \cdot, 0, 1\}$ a jejíž axiomy jsou axiomy komutativního okruhu, plus

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$
existuje číslo a takové, že $\forall i(q_i \mid a - r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?
Ano, 321.

Logická analýza důkazu čínské zbytkové věty vede (může vést) k rozhodnutí uvažovat dělitelnost (nikoliv dělení) v oboru celých (nikoliv přirozených) čísel a k teorii T, jejíž jazyk je $\{+, \cdot, 0, 1\}$ a jejíž axiomy jsou axiomy komutativního okruhu, plus

ID: $\forall x \forall y(x \cdot y = 0 \rightarrow x = 0 \vee y = 0)$

Příklad logické analýzy: čínská zbytková věta

Věta

Nechť $q_1, \ldots, q_n$ jsou po dvou nesoudělná čísla (moduly). Pak pro každou n-tici čísel $r_1, \ldots, r_n$
existuje číslo a takové, že $\forall i(q_i \mid a - r_i)$.

Příklad

Existuje číslo, které při dělení moduly $7, 8, 9$ dává zbytky $6, 1, 6$?
Ano, 321.

Logická analýza důkazu čínské zbytkové věty vede (může vést) k rozhodnutí uvažovat dělitelnost (nikoliv dělení) v oboru celých (nikoliv přirozených) čísel a k teorii T, jejíž jazyk je $\{+, \cdot, 0, 1\}$ a jejíž axiomy jsou axiomy komutativního okruhu, plus

ID: $\forall x \forall y(x \cdot y = 0 \rightarrow x = 0 \vee y = 0)$

B: $\forall x \forall y \exists u \exists v(x \cdot u + y \cdot v \mid x \ \& \ x \cdot u + y \cdot v \mid y)$.

Aplikace v oboru polynomů

Pozorování

Axiomy teorie T platí nejen v oboru celých čísel, ale i v oboru polynomů s racionálními koeficienty (příklad: $\frac{5}{4}x^3 - x - \frac{2}{7}$).

Aplikace v oboru polynomů

Pozorování

Axiomy teorie T platí nejen v oboru celých čísel, ale i v oboru polynomů s racionálními koeficienty (příklad: $\frac{5}{4}x^3 - x - \frac{2}{7}$).
Přitom když $a_1, \ldots, a_n$ jsou navzájem různá racionální čísla, lineární polynomy $x - a_1$ až $x - a_n$ jsou navzájem nesoudělné. Takže

Aplikace v oboru polynomů

Pozorování

Axiomy teorie T platí nejen v oboru celých čísel, ale i v oboru polynomů s racionálními koeficienty (příklad: $\frac{5}{4}x^3 - x - \frac{2}{7}$).
Přitom když $a_1, \ldots, a_n$ jsou navzájem různá racionální čísla, lineární polynomy $x - a_1$ až $x - a_n$ jsou navzájem nesoudělné. Takže čínská zbytková věta je aplikovatelná a poskytuje polynom, který při dělení polynomy $x - a_1$ až $x - a_n$ dává předem požadované zbytky $r_1, \ldots, r_n$.

Aplikace v oboru polynomů

Pozorování

Axiomy teorie T platí nejen v oboru celých čísel, ale i v oboru polynomů s racionálními koeficienty (příklad: $\frac{5}{4}x^3 - x - \frac{2}{7}$). Přitom když $a_1, \ldots, a_n$ jsou navzájem různá racionální čísla, lineární polynomy $x - a_1$ až $x - a_n$ jsou navzájem nesoudělné. Takže čínská zbytková věta je aplikovatelná a poskytuje polynom, který při dělení polynomy $x - a_1$ až $x - a_n$ dává předem požadované zbytky $r_1, \ldots, r_n$. Ale z rovnosti

$$p(x) = (x - a_i) \cdot q(x) + r_i$$

Aplikace v oboru polynomů

Pozorování

Axiomy teorie T platí nejen v oboru celých čísel, ale i v oboru polynomů s racionálními koeficienty (příklad: $\frac{5}{4}x^3 - x - \frac{2}{7}$). Přitom když $a_1, \ldots, a_n$ jsou navzájem různá racionální čísla, lineární polynomy $x - a_1$ až $x - a_n$ jsou navzájem nesoudělné. Takže čínská zbytková věta je aplikovatelná a poskytuje polynom, který při dělení polynomy $x - a_1$ až $x - a_n$ dává předem požadované zbytky $r_1, \ldots, r_n$. Ale z rovnosti

$$p(x) = (x - a_i) \cdot q(x) + r_i$$

plyne $r_i = p(a_i)$.

Aplikace v oboru polynomů

Pozorování

Axiomy teorie T platí nejen v oboru celých čísel, ale i v oboru polynomů s racionálními koeficienty (příklad: $\frac{5}{4}x^3 - x - \frac{2}{7}$). Přitom když $a_1, \ldots, a_n$ jsou navzájem různá racionální čísla, lineární polynomy $x - a_1$ až $x - a_n$ jsou navzájem nesoudělné. Takže čínská zbytková věta je aplikovatelná a poskytuje polynom, který při dělení polynomy $x - a_1$ až $x - a_n$ dává předem požadované zbytky $r_1, \ldots, r_n$. Ale z rovnosti

$$p(x) = (x - a_i) \cdot q(x) + r_i$$

plyne $r_i = p(a_i)$. Takže máme polynom, který v daných bodech $a_1, \ldots, a_n$ má požadované hodnoty $p(a_1), \ldots, p(a_n)$.

Aplikace v oboru polynomů

Pozorování

Axiomy teorie T platí nejen v oboru celých čísel, ale i v oboru polynomů s racionálními koeficienty (příklad: $\frac{5}{4}x^3 - x - \frac{2}{7}$).
Přitom když $a_1, \ldots, a_n$ jsou navzájem různá racionální čísla, lineární polynomy $x - a_1$ až $x - a_n$ jsou navzájem nesoudělné. Takže čínská zbytková věta je aplikovatelná a poskytuje polynom, který při dělení polynomy $x - a_1$ až $x - a_n$ dává předem požadované zbytky $r_1, \ldots, r_n$. Ale z rovnosti

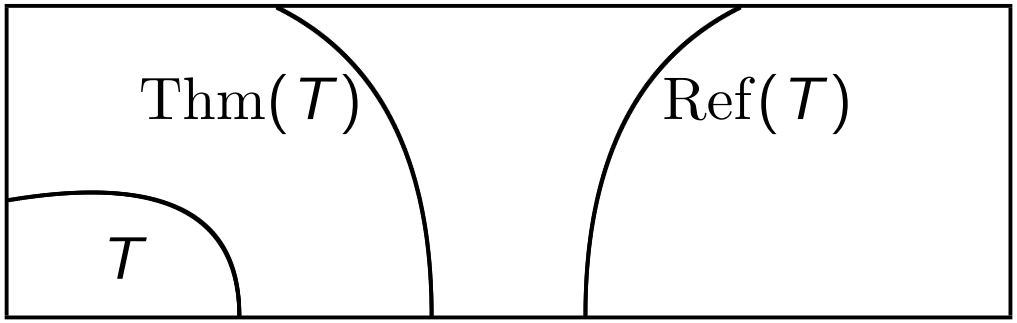
$$p(x) = (x - a_i) \cdot q(x) + r_i$$

plyne $r_i = p(a_i)$. Takže máme polynom, který v daných bodech $a_1, \ldots, a_n$ má požadované hodnoty $p(a_1), \ldots, p(a_n)$.

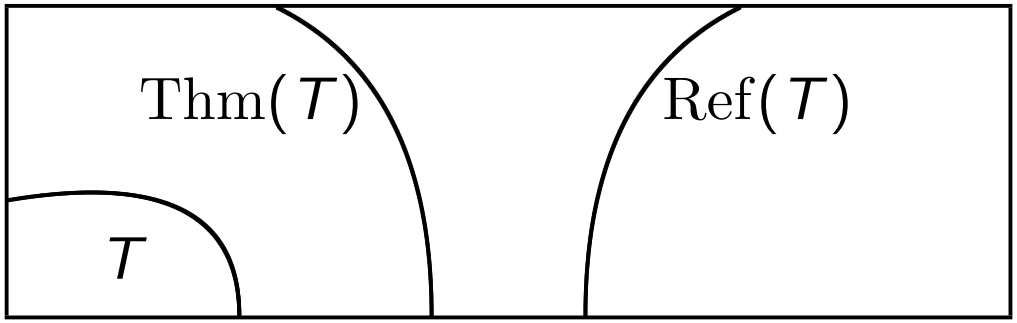
Závěr

Lagrangeova interpolační metoda je převlečená čínská zbytková věta.

Dokazatelné a vyvratitelné sentence



Dokazatelné a vyvratitelné sentence

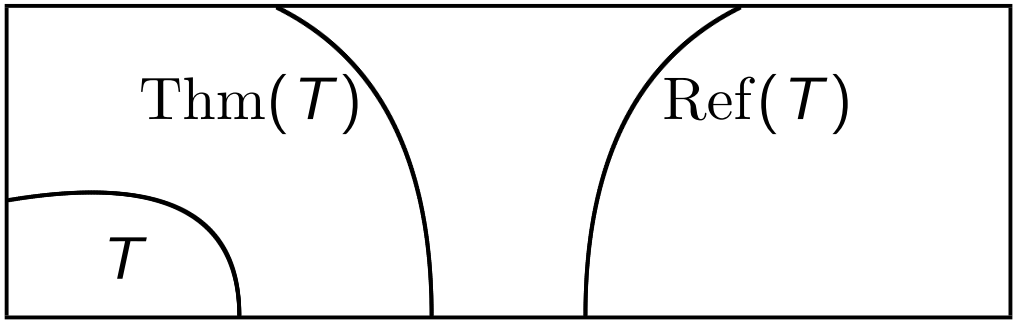


Příklady

Když T je jako výše, pak v $\mathrm{Thm}(T)$ jsou například sentence

$$1 \neq 0, \quad 1 \neq 1+1, \quad \forall x \forall y \forall z (x \mid y \ \& \ x \mid z \rightarrow x \mid (y+z)),$$

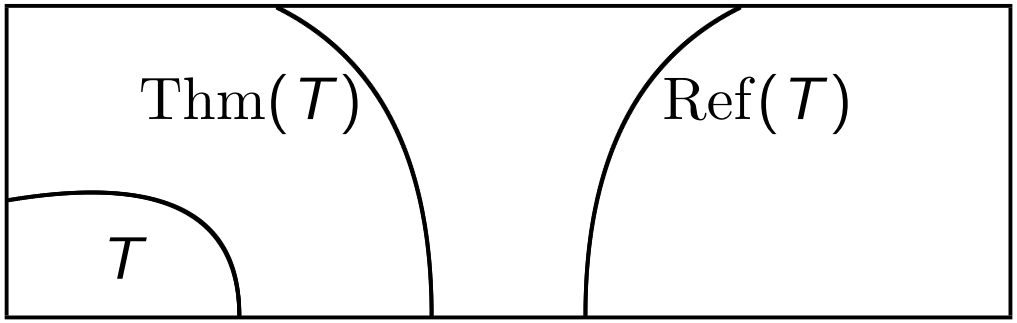
Dokazatelné a vyvratitelné sentence



Příklady

Když T je jako výše, pak v $\mathrm{Thm}(T)$ jsou například sentence
$1 \neq 0$, $1 \neq 1+1$, $\forall x \forall y \forall z (x \mid y \ \& \ x \mid z \rightarrow x \mid (y+z))$,
kdežto v $\mathrm{Ref}(T)$ jsou třeba $1 = 0$ a $\forall x \exists y (x \cdot y = 1)$.

Dokazatelné a vyvratitelné sentence



Příklady

Když T je jako výše, pak v $\mathrm{Thm}(T)$ jsou například sentence $1 \neq 0$, $1 \neq 1+1$, $\forall x \forall y \forall z (x \mid y \ \& \ x \mid z \rightarrow x \mid (y+z))$, kdežto v $\mathrm{Ref}(T)$ jsou třeba $1 = 0$ a $\forall x \exists y (x \cdot y = 1)$. Příklady sentencí, které nejsou v $\mathrm{Thm}(T) \cup \mathrm{Ref}(T)$ (tj. jsou nezávislé) jsou $1+1 \neq 0$ a $\forall x (x \mid 1 \rightarrow x = 1 \vee x = -1)$.

Rekurzívní, omezené (tj. Δ_0) a *RE* množiny

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívní, jestliže je algoritmicky rozhodnutelná.

Příklady: Množina všech sudých čísel, relace dělitelnosti, množina všech prvočísel.

Rekurzívní, omezené (tj. Δ_0) a *RE* množiny

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívní, jestliže je algoritmicky rozhodnutelná.

Příklady: Množina všech sudých čísel, relace dělitelnosti, množina všech prvočísel.

Množina je omezená (Δ_0, bounded), jestliže ji lze popsat (vyjádřit) bez neomezených kvantifikátorů:

$$\{\, n \,;\, \exists k{\leq}n(n = 2k) \,\}, \qquad \{\, [n, m] \,;\, \exists k{\leq}m(n \cdot k = m) \,\},$$
$$\{\, n \,;\, 1 < n \;\&\; \forall k{<}n(k \mid n \Rightarrow k = 1) \,\}.$$

Rekurzívní, omezené (tj. Δ_0) a *RE* množiny

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívní, jestliže je algoritmicky rozhodnutelná.

Příklady: Množina všech sudých čísel, relace dělitelnosti, množina všech prvočísel.

Množina je omezená (Δ_0, bounded), jestliže ji lze popsat (vyjádřit) bez neomezených kvantifikátorů:

$$\{\, n \,;\, \exists k{\leq}n(n = 2k) \,\}, \qquad \{\, [n, m] \,;\, \exists k{\leq}m(n \cdot k = m) \,\},$$
$$\{\, n \,;\, 1 < n \;\&\; \forall k{<}n(k \mid n \Rightarrow k = 1) \,\}.$$

Věta

Každá Δ_0 množina $A \subseteq \mathbb{N}^k$ je v $\mathbb{N}$ definovatelná v tom smyslu, že k ní existuje aritmetická Δ_0-formule $\varphi(x_1, \ldots, x_k)$ taková, že

$$\forall n_1 \ldots \forall n_k([n_1, \ldots, n_k] \in A \Leftrightarrow \mathbb{N} \models \varphi[n_1, \ldots, n_k]).$$

Rekurzívní, omezené (tj. Δ_0) a *RE* množiny

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívní, jestliže je algoritmicky rozhodnutelná.

Příklady: Množina všech sudých čísel, relace dělitelnosti, množina všech prvočísel.

Množina je omezená (Δ_0, bounded), jestliže ji lze popsat (vyjádřit) bez neomezených kvantifikátorů:

$$\{\, n \,;\, \exists k{\leq}n(n = 2k) \,\}, \qquad \{\, [n, m] \,;\, \exists k{\leq}m(n \cdot k = m) \,\},$$
$$\{\, n \,;\, 1 < n \;\&\; \forall k{<}n(k \mid n \;\Rightarrow\; k = 1) \,\}.$$

Věta

Každá Δ_0 množina $A \subseteq \mathbb{N}^k$ je v $\mathbb{N}$ definovatelná v tom smyslu, že k ní existuje aritmetická Δ_0-formule $\varphi(x_1, \ldots, x_k)$ taková, že

$$\forall n_1 \ldots \forall n_k([n_1, \ldots, n_k] \in A \Leftrightarrow \mathbb{N} \models \varphi[n_1, \ldots, n_k]).$$

Příklad: $n \mid m \Leftrightarrow \mathbb{N} \models \exists v{\leq}y\,(x \cdot v = y)[n, m]$.

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívně spočetná (*RE*), jestliže

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívně spočetná (*RE*), jestliže

- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je rekurzívní, nebo

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívně spočetná (*RE*), jestliže

- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je rekurzívní, nebo
- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je Δ_0.

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívně spočetná (*RE*), jestliže

- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je rekurzívní, nebo
- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je Δ_0.

Příklad

Množina všech dvojic $[P, D]$, kde P je program (ve formě zdrojového kódu v našem oblíbeném programovacím jazyce) a D jsou vstupní data taková, že P se při jejich zpracování dopočítá.

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathrm{N}^k$ je rekurzívně spočetná (*RE*), jestliže

- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je rekurzívní, nebo
- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je Δ_0.

Příklad

Množina všech dvojic $[P, D]$, kde P je program (ve formě zdrojového kódu v našem oblíbeném programovacím jazyce) a D jsou vstupní data taková, že P se při jejich zpracování dopočítá.

Příklad

Když (množina axiomů) teorie T je rekurzívní, pak množina $\mathrm{Thm}(T)$ je *RE*.

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathrm{N}^k$ je rekurzívně spočetná (*RE*), jestliže

- je tvaru $\{\, [n_1, \ldots, n_k] \,;\, \exists m R(\underline{n}, m) \,\}$, kde R je rekurzívní, nebo
- je tvaru $\{\, [n_1, \ldots, n_k] \,;\, \exists m R(\underline{n}, m) \,\}$, kde R je Δ_0.

Příklad

Množina všech dvojic $[P, D]$, kde P je program (ve formě zdrojového kódu v našem oblíbeném programovacím jazyce) a D jsou vstupní data taková, že P se při jejich zpracování dopočítá.

Příklad

Když (množina axiomů) teorie T je rekurzívní, pak množina $\mathrm{Thm}(T)$ je *RE*.

Platí

Každá rekurzívní množina je *RE*.

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathrm{N}^k$ je rekurzívně spočetná (*RE*), jestliže

- je tvaru $\{\, [n_1, .., n_k] \,;\, \exists m R(\underline{n}, m) \,\}$, kde R je rekurzívní, nebo
- je tvaru $\{\, [n_1, .., n_k] \,;\, \exists m R(\underline{n}, m) \,\}$, kde R je Δ_0.

Příklad

Množina všech dvojic $[P, D]$, kde P je program (ve formě zdrojového kódu v našem oblíbeném programovacím jazyce) a D jsou vstupní data taková, že P se při jejich zpracování dopočítá.

Příklad

Když (množina axiomů) teorie T je rekurzívní, pak množina $\mathrm{Thm}(T)$ je *RE*.

Platí

Každá rekurzívní množina je *RE*. Když *RE* množina A není rekurzívní, pak její komplement $-A$ není *RE*.

Rekurzívní, . . . množiny, pokračování

Množina (relace) $A \subseteq \mathbb{N}^k$ je rekurzívně spočetná (*RE*), jestliže

- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je rekurzívní, nebo
- je tvaru $\{ [n_1, .., n_k] ; \exists m R(\underline{n}, m) \}$, kde R je Δ_0.

Příklad

Množina všech dvojic $[P, D]$, kde P je program (ve formě zdrojového kódu v našem oblíbeném programovacím jazyce) a D jsou vstupní data taková, že P se při jejich zpracování dopočítá.

Příklad

Když (množina axiomů) teorie T je rekurzívní, pak množina $\mathrm{Thm}(T)$ je *RE*.

Platí

Každá rekurzívní množina je *RE*. Když *RE* množina A není rekurzívní, pak její komplement $-A$ není *RE*. Ke každé $A \in RE$ existuje formule $\varphi(x) \in \Sigma_1$ taková, že $\forall n(n \in A \Leftrightarrow \mathbb{N} \models \varphi[n])$.

Gödelova věta a její strukturální důkaz

Věta

Každá rekurzívně axiomatizovatelná a korektní teorie obsahující Robinsonovu aritmetiku Q je neúplná (a nerozhodnutelná).

Gödelova věta a její strukturální důkaz

Věta

Každá rekurzívně axiomatizovatelná a korektní teorie obsahující Robinsonovu aritmetiku Q je neúplná (a nerozhodnutelná).

Důkaz

Vezměme množinu $A \subseteq \mathbb{N}$, $A \in RE$, která není rekurzívní. K ní vezměme Σ_1-formuli $\varphi(x)$, která ji definuje v $\mathbb{N}$:

$$\forall n(n \in A \Leftrightarrow \mathbb{N} \models \varphi[n]).$$

Gödelova věta a její strukturální důkaz

Věta

Každá rekurzívně axiomatizovatelná a korektní teorie obsahující Robinsonovu aritmetiku Q je neúplná (a nerozhodnutelná).

Důkaz

Vezměme množinu $A \subseteq \mathbb{N}$, $A \in RE$, která není rekurzívní. K ní vezměme Σ_1-formuli $\varphi(x)$, která ji definuje v $\mathbb{N}$:

$$\forall n(n \in A \Leftrightarrow \mathbb{N} \models \varphi[n]).$$

Místo $\varphi[n]$ pišme $\varphi(\overline{n})$, tj. místo ohodnocení volné proměnné x číslem n uvažujme dosazení numerálu $\overline{n}$ za x. Platí také ekvivalence

$$\forall n(n \in A \Leftrightarrow T \vdash \varphi(\overline{n})),$$

Gödelova věta a její strukturální důkaz

Věta

Každá rekurzívně axiomatizovatelná a korektní teorie obsahující Robinsonovu aritmetiku Q je neúplná (a nerozhodnutelná).

Důkaz

Vezměme množinu $A \subseteq \mathbb{N}$, $A \in RE$, která není rekurzívní. K ní vezměme Σ_1-formuli $\varphi(x)$, která ji definuje v $\mathbb{N}$:

$$\forall n(n \in A \Leftrightarrow \mathbb{N} \models \varphi[n]).$$

Místo $\varphi[n]$ pišme $\varphi(\overline{n})$, tj. místo ohodnocení volné proměnné x číslem n uvažujme dosazení numerálu $\overline{n}$ za x. Platí také ekvivalence

$$\forall n(n \in A \Leftrightarrow T \vdash \varphi(\overline{n})),$$

kterou lze také psát jako

$$\forall n(n \in A \Leftrightarrow \varphi(\overline{n}) \in \mathrm{Thm}(T)).$$

Gödelova věta a její strukturální důkaz

Věta

Každá rekurzívně axiomatizovatelná a korektní teorie obsahující Robinsonovu aritmetiku Q je neúplná (a nerozhodnutelná).

Důkaz

Vezměme množinu $A \subseteq \mathbb{N}$, $A \in RE$, která není rekurzívní. K ní vezměme Σ_1-formuli $\varphi(x)$, která ji definuje v $\mathbb{N}$:

$$\forall n(n \in A \Leftrightarrow \mathbb{N} \models \varphi[n]).$$

Místo $\varphi[n]$ pišme $\varphi(\overline{n})$, tj. místo ohodnocení volné proměnné x číslem n uvažujme dosazení numerálu $\overline{n}$ za x. Platí také ekvivalence

$$\forall n(n \in A \Leftrightarrow T \vdash \varphi(\overline{n})),$$

kterou lze také psát jako

$$\forall n(n \in A \Leftrightarrow \varphi(\overline{n}) \in \mathrm{Thm}(T)).$$

Množina $\mathrm{Thm}(T)$, o které víme, že je *RE*, tudíž není rekurzívní. Takže teorie T je nerozhodnutelná. Z toho a z Postovy věty plyne i její neúplnost.

Gödel, Hájek, Vopěnka, . . .

Dle Smoryńského [Smo88], Gödel oznámil svůj výsledek v září 30 na konferenci v Königsbergu:

> *One can (under the assumption of consistency of classical mathematics) even give examples of statements (and even of the sort of Goldbach's or Fermat's), which are conceptually correct but unprovable in the formal system of classical mathematics. Therefore, if one adjoins the negation of such a statement to the axioms of classical mathematics, then one obtains a consistent system in which a conceptually false sentence is provable.*

Po rozpuštění Vopěnkova semináře přibližně v roce 1971

Gödel, Hájek, Vopěnka, . . .

Dle Smoryńského [Smo88], Gödel oznámil svůj výsledek v září 30 na konferenci v Königsbergu:

> *One can (under the assumption of consistency of classical mathematics) even give examples of statements (and even of the sort of Goldbach's or Fermat's), which are conceptually correct but unprovable in the formal system of classical mathematics. Therefore, if one adjoins the negation of such a statement to the axioms of classical mathematics, then one obtains a consistent system in which a conceptually false sentence is provable.*

Po rozpuštění Vopěnkova semináře přibližně v roce 1971 se Petr Hájek začal zabývat metamatematikou aritmetiky, a podnětným zdrojem informací pro něj byl Fefermanův článek [Fef60].

Gödel, Hájek, Vopěnka, . . .

Dle Smoryńského [Smo88], Gödel oznámil svůj výsledek v září 30 na konferenci v Königsbergu:

> *One can (under the assumption of consistency of classical mathematics) even give examples of statements (and even of the sort of Goldbach's or Fermat's), which are conceptually correct but unprovable in the formal system of classical mathematics. Therefore, if one adjoins the negation of such a statement to the axioms of classical mathematics, then one obtains a consistent system in which a conceptually false sentence is provable.*

Po rozpuštění Vopěnkova semináře přibližně v roce 1971 se Petr Hájek začal zabývat metamatematikou aritmetiky, a podnětným zdrojem informací pro něj byl Fefermanův článek [Fef60]. Zesílení Gödelovy věty dokázal okolo roku 1980 Pavel Pudlák.

Literatura

- S. Feferman. Arithmetization of metamathematics in a general setting. *Fundamenta Mathematicae*, 49:35–92, 1960.
- K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38:173–198, 1931.
- C. Smoryński. Metamathematics of Arithmetic, Chapter III: Representability and Semi-Representability. Nepublikovaný rukopis, circa 1978.
- C. Smoryński. Hilbert's programme. *CWI Quarterly*, 1(4), 1988.