Algoritmicky nerieši teľné problémy

Lev Bukovský

Ústav matematických vied, Prírodovedecká fakulta UPJŠ

Košice, 20. apríla 2004

Obsah

1 Úvod **2**

2 Čiastočne rekurzívne funkcie **2**

3 Gödelova β-funckia **4**

4 Ekvivalentná definícia rekurzívnosti **5**

5 Predikátový počet **7**

6 Teória prirodzených čísiel **9**

7 Definovateľnosť v teórii **12**

8 Aritmetizácia **14**

9 Tarského Veta **16**

10 Gödelova veta o neúplnosti **19**

11 Gödelova veta podľa Rossera **21**

12 Iná nerozhodnuteľná veta Peanovej aritmetiky **23**

13 Diofantické rovnice a diofantické množiny **24**

14 Pellova rovnica **28**

15 Niektoré diofantické funkcie **34**

16 Veta o ohraničenom kvantifikátore **36**

17 Čiastočne rekurzívna funkcia je diofantická **38**

18 10. Hilbertov problém a iné dôsledky **38**

Literatúra **42**

1 Úvod

Poslucháč pozná problém, ktorý sa nedá riešiť algoritmicky, pod názvom "Halting Problem": problém zastavenia sa Turingovho stroja. Známy výsledok A. Turinga hovorí: neexistuje algoritmus, ktorý by rozhodol, či daný Turingov stroj pri danom vstupe sa zastaví alebo nie.

V prednáške predvedieme ďalšie dva výsledky podobného typu. Prvým výsledkom je Tarského veta 9.1 o neexistencii algoritmu, ktorý by rozhodol, či daná formula je dokázateľná v Peanovej aritmetike alebo nie je. Prezentujeme aj jej najdôležitejšie dôsledky, ktoré však historicky boli známe skôr. Druhým výsledkom je veta o neexistencii algoritmu, ktorý by rozhodol, či daná diofantická rovnica má riešenie alebo nie. Je to riešenie známeho 10. Hilbertovho problému.

V častiach 5 až 12 pracujeme v metamatematike. Logické spojky a kvantifikátory sú predmetom nášho bádania. Rozlišujeme medzi metamatematickým prirodzeným číslom n a jeho názvom termom Δ_n. Metamatematické premenné píšeme kurzívou, premenné ako znaky jazyka teórie píšeme románskym písmom. Pojem "veta" a "dôkaz" sú objektom nášho skúmania. Preto naše výsledky budú formulované ako tvrdenia a budeme ich overovať (nie dokazovať).

V časti 13 sa vraciame do matematiky a logické spojky a kvantifikátory majú obvyklý význam. Výsledky budeme znova formulovať ako vety a budeme ich dokazovať.

Označenie a terminológiu používam tak, ako bola zavedená v učebných textoch [BL1] a [BL2]. K použitiu vety 4.1 ma inšpiroval Martin Davis [DM1]. Výklad Tarského a Gödelovej vety je spracovaný podľa práce A. Tarského [Ta2] a monografie S. C. Kleeneho [K1]. Dôkaz neexistencie algoritmu pre riešenie 10. Hilbertového problému sleduje článok Martina Davisa [DM2].

2 Čiastočne rekurzívne funkcie

Upozorníme na potrebné poznatky z teórie rekurzívnych funckcií.

Základné funkcie sú tieto funkcie:

$$\mathrm{Z}(x) = 0,\ \mathrm{S}(x) = x + 1,\ \mathrm{P}^i_k(x_1, \ldots, x_k) = x_i.$$

Operácie nad funkciami: substitúcia, primitívna rekurzia, minimalizácia a regulárna minimalizácia. Funckia sa nazýva čiastočne (všeobecne) rekurzívna, ak vznikla zo základných funkcií použitím operácií substitúcie, primitívnej rekurzie a (regulárnej) minimalizácie.

Základný výsledok teórie vypočítateľnosti, ktorý budeme potrebovať je zhrnutie výsledkov viet 10.2 a 11.1 z [BL1].

Veta 2.1 (S. C. Kleene) *Existuje primitívne rekurzívna výroková funkcia* T_k *a primitívne rekurzívna funkcia* U *taká, že platí nasledovné: pre každú čiastočne rekurzívnu funkciu* f *existuje prirodzené číslo* e *(číslo Turingovho stroja, ktorý počíta funkciu* f*) také, že pre ľubovoľné prirodzené čísla* $x_1, \ldots, x_k$ *je*

$$f(x_1, \ldots, x_k) = \mathrm{U}((\min y)\mathrm{T}_k(e, y, x_1, \ldots, x_k)), \tag{2.1}$$

pričom hodnota funkcie na ľavej strane rovnosti je definovaná práve vtedy, keď je definovaná hodnota funkcie na pravej strane rovnosti, t.j. keď

$$(\exists \mathrm{y})\, \mathrm{T}_k(e, y, x_1, \ldots, x_k).$$

Naviac, ak platí $\mathrm{T}_k(e, y, x_1, \ldots, x_k)$*, tak hodnota funckie* $f(x_1, \ldots, x_k)$ *je definovaná a je rovná* $\mathrm{U}(y)$*.*

Množina $A \subseteq \mathbb{N}^k$ sa nazýva rekurzívna, ak jej charakteristická funkcia je všeobecne rekurzívna. Výroková funkcia $\mathcal{V}(x_1, \ldots, x_k)$ je rekurzívna, ak je taká množina

$$\{[x_1, \ldots, x_k] \in \mathbb{N}^k; \mathcal{V}(x_1, \ldots, x_k)\}.$$

Množina $A \subseteq \mathbb{N}^k$ sa nazýva rekurzívne očíslovateľná, ak existuje rekurzívna výroková funkcia $\mathcal{V}$ taká, že platí

$$[x_1, \ldots, x_k] \in A \equiv (\exists y)\, \mathcal{V}(x_1, \ldots, x_k, y).$$

Podobne pre výrokovú funkciu.

Pripomíname dva klasické výsledky.

Veta 2.2 *Nech* $A \subseteq \mathbb{N}$*. Potom nasledujúce podmienky sú ekvivaletné:*

a) *A je rekurzívne očíslovateľná;*

b) *$A = \emptyset$ alebo existuje všeobecne (dokonca primitívne) rekurzívna funkcia f taká, že $A = \mathcal{H}(f)$;*

c) *existuje číslo e také, že pre každé $n \in \mathbb{N}$ platí*

$$n \in A \equiv (\exists y)\mathrm{T}_1(e, y, n).$$

Veta 2.3 (E. Post) *Výroková funkcia $\mathcal{V}$ je rekurzívna vtedy a len vtedy keď výrokové funkcie $\mathcal{V}$ a $\neg\mathcal{V}$ sú rekurzívne očíslovateľné.*

Párujúca funkcia $\pi : \mathbb{N} \times \mathbb{N} \xrightarrow[\text{onto}]{1-1} \mathbb{N}$ je definovaná predpisom

$$\pi(n, m) = \frac{1}{2}(n + m)(n + m + 1) + m.$$

λ a ρ sú ľavá a pravá inverzná k párujúcej funkcii. Teda pre každé prirodzené čísla n, m, k platí

$$\pi(\lambda(k), \rho(k)) = k, \quad \lambda(\pi(n, m)) = n, \quad \rho(\pi(n, m)) = m.$$

Funkcie π, λ, ρ sú primitívne rekurzívne.

Ak $f : A \longrightarrow \mathbb{N}$, kde $A \subseteq \mathbb{N}^k$, tak **graf funkcie** f je množina

$$\mathrm{G}(f) = \{[x_1, \ldots, x_k, y] \in \mathbb{N}^{k+1}; [x_1, \ldots, x_k] \in A \wedge f(x_1, \ldots, x_k) = y\}.$$

Veta 2.4 *Funkcia f je čiastočne rekurzívna vtedy a len vtedy, keď jej graf* $\mathrm{G}(f)$ *je rekurzívne očíslovateľná množina.*

Dôkaz: Nech f je čiastočne rekurzívna funkcia. Nech e je číslo Turingovho stroja, ktorý ju počíta. Potom

$$[x_1, \ldots, x_k, y] \in \mathrm{G}(f) \equiv (\exists z)\,(\mathrm{T}_k(e, z, x_1, \ldots, x_k) \wedge y = \mathrm{U}(z)).$$

Naopak, nech $\mathrm{G}(f)$ je rekurzívne očíslovateľná množina. Nech $\mathcal{V}$ je rekurzívna výroková funkcia taká, že

$$[x_1, \ldots, x_k, y] \in \mathrm{G}(f) \equiv (\exists z)\,\mathcal{V}(z, x_1, \ldots, x_k, y).$$

Potom

$$f(x_1, \ldots, x_k) = \lambda((\min z)\,\mathcal{V}(\rho(z), x_1, \ldots, x_k, \lambda(z))).$$

q.e.d.

V ďalšom budeme potrebovať funkcie súčtu, súčinu a odpočítania. Bude výhodné ich označiť[1]

$$\mathrm{add}(x, y) = x + y, \quad \mathrm{prod}(x, y) = x \cdot y, \quad \mathrm{odc}(x, y) = x \div y.$$

V teórii rekurzívnych funckií sme využili základnú vetu aritmetiky o rozklade prirodzených čísiel na súčin prvočísiel ako prostriedok ku kódovaniu postupností čísiel. Konkrétne, p_0, p_1, $\ldots$, p_n, $\ldots$ je rastúca postupnosť všetkých prvočísiel. Ak pre prirodzené číslo $n > 1$ platí

$$n = p_0^{\alpha_0} \cdot \ldots \cdot p_k^{\alpha_k} \text{ a } \alpha_k \neq 0,$$

tak

$$\mathrm{dl}(n) = k, \quad (n)_i = \alpha_i.$$

Teda pre $n > 1$ platí

$$n = p_0^{(n)_0} \cdot \ldots \cdot p_{\mathrm{dl}(n)}^{(n)_{\mathrm{dl}(n)}}.$$

V našich ďalších úvahách budeme potrebovať podobné kódovanie, ktoré sa dá jednoducho vyjadriť pomocou funckií add, prod a odc. Opíšeme ho v ďalšej časti.

3 Gödelova β-funckia

Začneme jedným jednoduchým tvrdením z teórie čísiel. Najprv nový pojem a označenia. Postupnosť $m_0, \ldots, m_k$ prirodzených čísiel sa nazýva **prijateľná postupnosť modulov**, ak pre každé $i \neq j$, čísla m_i a m_j sú nesúdeliteľné. Ak x, y sú prirodzené čísla, označíme $\mathrm{rm}(x, y)$ zvyšok čísla x pri delení číslom y, ak $y > 0$ a $\mathrm{rm}(x, 0) = 0$.

[1] Pripomíname, že $x \div y = x - y$ ak $x \geq y$ a $= 0$ v opačnom prípade.

Veta 3.1 (Čínska veta o zvyškoch) *Nech $m_0, \ldots, m_k$ je prijateľná postupnosť modulov, $a_0, \ldots, a_k$ sú prirodzené čísla. Potom existuje ľubovoľne veľké číslo x také, že*

$$x \equiv a_0 \bmod m_0, \quad \ldots \quad , x \equiv a_k \bmod m_k. \tag{3.2}$$

Overenie: Zrejme tvrdenie (3.2) je ekvivalentné tvrdeniu

$$\mathrm{rm}(x, m_0) = \mathrm{rm}(a_0, m_0), \quad \ldots \quad , \mathrm{rm}(x, m_k) = \mathrm{rm}(a_k, m_k)$$

Ak $\mathrm{rm}(c, m_i) = \mathrm{rm}(d, m_i)$, $c < d$, tak $m_i \mid (d-c)$. Keďže $m_0, \ldots, m_k$ je prijateľná postupnosť modulov, tak z rovností

$$\mathrm{rm}(c, m_0) = \mathrm{rm}(d, m_0), \ \ldots \ , \mathrm{rm}(c, m_k) = \mathrm{rm}(d, m_k)$$

vyplýva, že $m_0 \cdot \ldots \cdot m_k$ delí rozdiel $d - c$, špeciálne $m_0 \cdot \ldots \cdot m_k \leq d - c$.

Všetkých $(k+1)$-tic čísiel $[y_0, \ldots, y_k]$, $0 \leq y_i < m_i$ je $m_0 \cdot \ldots \cdot m_k$. Nech c je ľubovoľné prirodzené číslo. Ak x nadobúda postupne hodnoty od $c+1$ po číslo $c + m_0 \cdot \ldots \cdot m_k$, tak $[\mathrm{rm}(x, m_0), \ldots, \mathrm{rm}(x, m_k)]$ prebieha všetky takéto $(k+1)$-tice. Špeciálne, pre nejaké x, $c < x \leq m_0 \cdot \ldots \cdot m_k$, je to $(k+1)$-tica $[\mathrm{rm}(a_0, m_0), \ldots, \mathrm{rm}(a_k, m_k)]$.

q.e.d.

Ak $k! \mid d$, tak čísla $1+(1+0)d, 1+(1+1)d, \ldots, 1+(1+k)d$ tvoria prijateľnú postupnosť modulov. Naozaj, žiadny prvočíselný deliteľ p čísla $1+(1+i)d$ nedelí číslo d a teda $p > k$. Teda ak $p \mid (1+(1+i)d)$ a $p \mid (1+(1+j)d)$, tak $p \mid j - i$, čo je možné len ak $p = 1$.

To nás inšpiruje definovať **Gödelovu β-funkciu** predpisom

$$\beta(x, d, i) = \mathrm{rm}(x, 1 + (1+i)d).$$

Na základe vety 3.1 dostávame

Dôsledok 3.2 *Nech $a_0, \ldots, a_k$ sú kladné prirodzené čísla. Potom existujú ľubovoľne veľké čísla x, d také, že*

$$\beta(x, d, i) = a_i \ \textit{pre}\ i = 0, \ldots, k.$$

4 Ekvivalentná definícia rekurzívnosti

Pri overovaní tvrdení 7.1 a 17.1 schéma definície funkcie primitívnou rekurziou by robila dosť veľké nepríjemnosti (aj keď sa to dá urobiť). Aby sme sa tomu vyhli, dáme jednu jednoduchú ekvivalentnú definíciu všeobecne a čiastočne rekurzívnych funkcií.

Veta 4.1 *Funkcia je čiastočne (všeobecne) rekurzívna práve vtedy, keď ju možno získať z funkcií*

$$\mathrm{Z},\ \mathrm{S},\ \mathrm{P}_i^k,\ \mathrm{add},\ \mathrm{prod},\ \mathrm{odc} \tag{4.3}$$

pomocou operácií substitúcie a (regulárnej) minimalizácie.

Overenie: Nech $\mathcal{F}$ je množina všetkých funkcií, ktoré možno získať z funkcí (4.3) pomocou substitúcií a minimalizázií (prípadne regulárnych minimalizácií). Ak $\mathcal{V}$ je výroková funkcia, tak zápisom $\mathcal{V} \in \mathcal{F}$ vyjadrujeme $\mathrm{ch}_{\mathcal{V}} \in \mathcal{F}$.

Zrejme stačí ukázať toto:

ak funkcia f vznikla z funkcií g, $h \in \mathcal{F}$ primitívnou rekurziou, tak $f \in \mathcal{F}$.

Ukážeme dve veci:

1) $\beta \in \mathcal{F}$,
2) primitívnu rekurziu vyjadríme pomocou minimalizácie a funkcie β.

Postupne definujeme funkcie patriace do $\mathcal{F}$:

$$\begin{aligned}
\mathrm{sg}(x) &= (\min y)\, xy = x,\\
\mathrm{ch}_{=}(x,y) &= 1 \div (x \div y + y \div x),\\
x < y &\equiv \mathrm{sg}(y \div x) = 1,\\
\left[\frac{x}{y}\right] &= (\min z)\,((z+1)y > x \vee (y = 0 \wedge z = 0)),\\
\mathrm{rm}(x,y) &= \mathrm{sg}(y) \cdot (x - y \left[\frac{x}{y}\right]),\\
\beta(x,d,i) &= \mathrm{rm}(x, 1 + (1+i)d),\\
\pi(n,m) &= (\min k)\,(2k = (n+m)(n+m+1) + 2m),\\
\lambda(k) &= (\min n)\,\pi(n, (\min m)\,\pi(n,m) = k) = k,\\
\rho(k) &= (\min m)\,\pi((\min n)\,\pi(n,m) = k, m) = k,\\
\theta(u,i) &= \beta(\lambda(u), \rho(u), i).
\end{aligned}$$

Zrejme všetky uvedené funkcie patria do $\mathcal{F}$ a pre ľubovoľné čísla $a_0, \ldots, a_k$ existuje ľubovoľne veľké číslo u také, že

$$\theta(u,i) = a_i \text{ pre } i = 0, \ldots, k.$$

Nech funckia f vznikla z funckií g a h primitívnou rekurziou, t.j.

$$\begin{aligned}
f(0, x_1, \ldots, x_k) &= g(x_1, \ldots, x_k),\\
f(y+1, x_1, \ldots, x_k) &= h(y, x_1, \ldots, x_k, f(y, x_1, \ldots, x_k)).
\end{aligned}$$

Ľahko vidieť, že platí

$$f(y, x_1, \ldots, x_k) = \theta(u, y),$$

kde

$$\begin{aligned}
u = (\min z)\,(&\theta(z,0) = g(x_1, \ldots, x_k) \wedge\\
&(\forall i < y)\,\theta(z, i+1) = h(i, x_1, \ldots, x_k, \theta(z,i)).
\end{aligned}$$

Využijeme takýto trik: v definícii čísla u číslo y bolo také, že pre všetky od neho menšie platila určitá podmienka. Vyjadríme to ekvivalentne tak, že y je najmenšie, pre ktoré táto podmienka neplatí. Nech

$$p(y, z, x_1, \ldots, x_k) = (\min v)\,(\theta(z, v+1) \neq h(v, x_1, \ldots, x_k, \theta(z,v)) \vee v = y).$$

Potom

$$f(y, x_1, \ldots, x_k) = \theta((\min z)\,(\theta(z, 0) = g(x_1, \ldots, x_k) \wedge y = p(y, z, x_1, \ldots, x_k)), y).$$

q.e.d.

5 Predikátový počet

Teraz naše úvahy **prechádzajú do metamatematiky**. Pojmy typu "dôkaz", "veta" a podobne, budú predmetom nášho bádania. Preto výsledky formulujeme ako tvrdenia a budeme ich overovať.

Nasledujúce znaky sú znaky predikátového počtu:

premenné:	x_0, x_1, x_2, $\ldots$, x_n, $\ldots$
logické spojky:	$\neg$, $\wedge$, $\vee$, $\rightarrow$, $\equiv$,
kvantifikátory	$\forall$, $\exists$,
zátvorky:	(,),
predikáty:	P, Q, R, $\ldots$
individuálne konštanty:	a, b, c, $\ldots$
názvy operácií:[2]	f, g, h, $\ldots$

U každého predikátu a názvu operácie je udaná **árnosť**, t.j. počet miest, do ktorých sa dosadzuje.

Každú podmnožinu tohoto jazyka, ktorá obsahuje všetky znaky prvých štyroch riadkov a aspoň jeden predikát, nazývame **jazyk predikátového počtu**. Keďže znaky prvých štyroch riadkov sú "povinné" v každom jazyku, obyčajne ich neuvádzame ako prvky príslušného jazyka.

Definujeme pojem **vytvárajúca postupnosť termu**, **term**, **atomická formula**, **vytvárajúca postupnosť formuly** a **formula**. Ďalej máme pojem **voľná** a **viazaná** premenná. Formula, ktorá neobsahuje voľne žiadnu premennú, sa nazýva **uzavretá**. **Uzáver formuly** $\varphi(\mathrm{x}_1, \ldots, \mathrm{x}_k)$ (obsahuje voľne len vyznačené premenné) je formula

$$(\forall \mathrm{x}_1) \ldots (\forall \mathrm{x}_k)\, \varphi(\mathrm{x}_1, \ldots, \mathrm{x}_k).$$

Stručne ju budeme zapisovať $(\forall \ldots)\, \varphi$.

Množina uzavretých formúl $\mathbf{T}$ sa nazýva **teória**. Prvky množiny $\mathbf{T}$ sa nazývajú **axiómy teórie T**. Jazyk $\mathcal{L}_{\mathbf{T}}$ teórie $\mathbf{T}$ obsahuje predikáty, názvy operácií a individuálne konštanty, ktoré sa vyskytujú v axiómach teórie $\mathbf{T}$. Z praktických dôvodov často budeme uvažovať teóriu ako množinu formúl – nie nutne uzavretých. Vtedy je potrebné každú axiómu nahradiť jej uzáverom. Ak $\mathbf{T}$ je teória a φ je formula, tak teóriu $\mathbf{T} \cup \{\varphi\}$ stručne označujeme $\mathbf{T} + \varphi$.

V ďalšom upresníme pojem teórie. Budeme pracovať len s takou teóriou, v ktorej vieme algoritmicky rozhodnúť, či daná formula je axióma tejto teórie alebo nie.

Postupnosť formúl

$$\varphi_1, \ldots, \varphi_n$$

sa nazýva **dôkaz v teórii T**, ak pre každý člen tejto postupnosti, t.j. pre každé $i = 1, \ldots, n$ platí jedna z podmienok

D1) φ_i je axióma predikátového počtu,

D2) φ_i je axióma teórie **T**,

D3) existujú také $k, j < i$, že φ_k je formula $\varphi_j \to \varphi_i$,

D4) existuje $j < i$ a formuly φ, ψ, formula ψ neobsahuje premennú x, také, že φ_j je $\psi \to \varphi(\mathrm{x}, \ldots)$ a φ_i je formula $\psi \to (\forall \mathrm{x})\, \varphi(\mathrm{x}, \ldots)$,

D5) existuje $j < i$ a formuly φ, ψ, formula ψ neobsahuje premennú x, také, že φ_j je $\varphi(\mathrm{x}, \ldots) \to \psi$ a φ_i je formula $(\exists \mathrm{x})\, \varphi(\mathrm{x}, \ldots) \to \psi$.

Samozrejme, musíme povedať, čo je to **axióma predikátového počtu**, skrátene **APP**. Axióma predikátového počtu nemusí byť uzavrertá formula. Budeme mať tri skupiny axióm predikátového počtu. Axiómy prvej skupiny budeme často nazývať axiómy výrokového počtu. Ak φ, ψ, σ sú formuly, tak nasledujúce formuly sú APP:

$$\begin{array}{ll}
\varphi \to \varphi & \varphi \to (\psi \to \varphi) \\
(\varphi \to \psi) \to ((\psi \to \sigma) \to (\varphi \to \sigma)) & (\varphi \to \psi) \to (\neg\psi \to \neg\varphi) \\
(\varphi \to \psi) \to ((\varphi \to (\psi \to \sigma)) \to (\varphi \to \sigma)) & \\
\varphi \to (\psi \to (\varphi \wedge \psi)) & (\varphi \wedge \psi) \to \varphi \\
(\varphi \wedge \psi) \to (\psi \wedge \varphi) & \\
(\varphi \to \sigma) \to ((\psi \to \sigma) \to ((\varphi \vee \psi) \to \sigma)) & \varphi \to (\varphi \vee \psi) \\
(\varphi \vee \psi) \to (\psi \vee \varphi) & \\
(\varphi \to \psi) \to ((\psi \to \varphi) \to (\varphi \equiv \psi)) & (\varphi \equiv \psi) \to (\varphi \to \psi) \\
(\varphi \equiv \psi) \to (\psi \equiv \varphi) & \\
\varphi \vee \neg\varphi & \neg\neg\varphi \equiv \varphi \\
(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi) &
\end{array}$$

Druhú skupinu tvoria axiómy o vynechaní veľkého kvantifikátora a zavedení malého kvantifikátora. Ak $\varphi(\mathrm{x}, \ldots)$ je formula, $\mathbf{t}$ je term, ktorý neobsahuje premennú x, tak nasledujúce formuly sú APP:

$$\begin{aligned}
(\forall \mathrm{x})\, \varphi(\mathrm{x}, \ldots) &\to \varphi(\mathbf{t}, \ldots), \\
\varphi(\mathbf{t}, \ldots) &\to (\exists \mathrm{x})\, \varphi(\mathrm{x}, \ldots).
\end{aligned}$$

Prvú axiómu môžeme nazvať "vynechanie $\forall$" a druhú "zavedenie $\exists$".

Tretia skupina axióm predikátového počtu sú tzv. de Morganove pravidlá pre negovanie kvantifikátorov. Ak φ je formula, tak nasledujúce formuly sú APP:

$$\neg(\forall \mathrm{x})\, \varphi \equiv (\exists \mathrm{x})\, \neg\varphi, \qquad \neg(\exists \mathrm{x})\, \varphi \equiv (\forall \mathrm{x})\, \neg\varphi.$$

Podmienka D3) predstavuje odvodzovacie pravidlo modus ponens. Podmienky D4) a D5) opisujú použitie odvodzovacích pravidiel

$$\frac{\psi \to \varphi(\mathrm{x},\ldots)}{\psi \to (\forall \mathrm{x})\,\varphi(\mathrm{x},\ldots)} \quad \text{zav } \forall, \qquad \frac{\varphi(\mathrm{x},\ldots) \to \psi}{(\exists \mathrm{x})\,\varphi(\mathrm{x},\ldots) \to \psi} \quad \text{vyn } \exists,$$

za predpokladu, že formula ψ neobsahuje premennú x.

Ak existuje dôkaz $\varphi_1, \ldots, \varphi_n$ v teórii $\mathbf{T}$ taký, že $\varphi_n = \varphi$, tak hovoríme, že formula φ **je dokázateľná v teórii T**, píšeme $\mathbf{T} \vdash \varphi$. Hovoríme tiež, že φ je **veta teórie T**.

Teória $\mathbf{T}$ je **protirečivá**, ak existuje uzavretá formula φ taká, že $\mathbf{T} \vdash \varphi$ a $\mathbf{T} \vdash \neg\varphi$. V opačnom prípade teória $\mathbf{T}$ je **neprotirečivá**. Metódu dôkazu sporom môžeme preformulovať takto: $\mathbf{T} \nvdash \varphi$ vtedy a len vtedy, keď teória $\mathbf{T} + \neg\varphi$ je neprotirečivá.

Uzavretá formula φ je **nerozhodnuteľná veta** teórie $\mathbf{T}$, ak $\mathbf{T} \nvdash \varphi$ a $\mathbf{T} \nvdash \neg\varphi$. Teória $\mathbf{T}$ je **úplná**, ak v nej neexistuje nerozhodnuteľná veta.

Je potrebné zdôrazniť rozdiel medzi slovami "neriešiteľný" a "nerozhodnuteľný". Angličania pre prvý termín používajú slovo "unsolvable" a pre druhý "undecidable". Termín neriešiteľný znamená, že pre daný problém (ktorý má spravidla nekonečne mnoho prípadov) neexistuje určitý spôsob riešenia; v našom prípade pomocou algoritmu. Druhý termín sa používa v situácii, keď dané prostriedky nestačia k rozhodnutiu položenej otázky. V našom prípade to znamená, že axiómy danej teórie nestačia k tomu, aby sme mohli rozhodnúť o danej formule: nevieme ju ani dokázať ani vyvrátiť, t.j. dokázať jej negáciu. V ďalšom však uvidíme, že historicky sa zaužívalo aj nesprávne používanie týchto slov.

Teória $\mathbf{T}_1$ je **slabšia** ako teória $\mathbf{T}_2$, ak $\mathcal{L}_{\mathrm{T}_1} \subseteq \mathcal{L}_{\mathrm{T}_2}$ a ak každá formula v jazyku $\mathcal{L}_{\mathbf{T}_1}$ dokázateľná v teórii $\mathbf{T}_1$ je dokázateľná aj v teórii $\mathbf{T}_2$. Hovoríme tiež, že teória $\mathbf{T}_2$ je **silnejšia** ako teória $\mathbf{T}_1$. Zrejme teória $\mathbf{T}_1$ je slabšia ako teória $\mathbf{T}_2$ práve vtedy, keď každá axióma teórie $\mathbf{T}_1$ je dokázateľná v teórii $\mathbf{T}_2$. Špeciálne, ak $\mathbf{T}_1 \subseteq \mathbf{T}_2$, tak $\mathbf{T}_1$ je slabšia ako $\mathbf{T}_2$.

Nech $\mathbf{T}_1$ je slabšia ako $\mathbf{T}_2$. Ak $\mathbf{T}_2$ je neprotirečivá, tak je neprotirečivá aj $\mathbf{T}_1$. Ak $\mathbf{T}_1$ je úplná, tak je úplná aj $\mathbf{T}_2$.

Definícia nového pojmu v danej teórii znamená určitú skratku, skrátené vyjadrovanie. Napr. definovať nový binárny predikát Q v teórii $\mathbf{T}$ znamená pridať do jazyka $\mathcal{L}_{\mathbf{T}}$ nový predikát Q a do teórie novú axiómu $(\forall x, y)\,\mathrm{Q}(\mathrm{x},\mathrm{y}) \equiv \varphi(\mathrm{x},\mathrm{y})$, kde formula φ je príslušná "definícia". Podobne pre názvy operácií a individuálne konštanty.

6 Teória prirodzených čísiel

Začneme jednou technickou poznámkou. Základné znaky aritmetiky budeme používať v dvoch významoch: ako označenie v metamatematike alebo názvy vo formalizovanej teórii. V obidvoch prípadoch budeme používať tie isté symboly s jediným rozdielom: v metamatematike budú písané ako $=, <, \leq, +, \cdot, 0, 1$ a ako znaky jazyka, ich názvy, budú písané matematickým tučným písmom

$=, <, \leq, +, \cdot, \mathbf{0}, \mathbf{1}$. Žiaľ, nie vždy je dobre rozoznateľný rozdiel. V prípade premenných použijeme inú konvenciu: metamatematické premenné budú písané (ako doteraz) kurzívou $x, y, z, n, m, k, \ldots$ a znaky pre premenné daného jazyka budú písané románskym písmom $\mathrm{x}, \mathrm{y}, \mathrm{z}, \ldots$. Dúfam, že nevýraznosť rozdielu odstráni kontext.

Giuseppe Peano v roku 1891 podal jednoduchú axiomatiku teórie prirodzených čísiel. Dodnes matematici nenašli vhodnejšiu teóriu, ktorá by opisovala vlastnosti prirodzených čísiel. Z určitých technických dôvodov budeme potrebovať aj dve iné teórie prirodzených čísiel slabšie ako Peanova teória.

Jazyk aritmetiky okrem povinných znakov prvých štyroch riadkov obsahuje binárny predikát rovnosti $=$, dva názvy binárnych operácií $+, \cdot$ a dve individuálne konštanty **0, 1**. Budeme používať aj ďalšie binárne predikáty $\leq, <$, ktoré definujeme pomocou formúl $(\exists \mathrm{z})\,\mathrm{x}{+}\mathrm{z}{=}\mathrm{y}$ a $(\exists \mathrm{z})\,(\mathrm{x}{+}\mathrm{z}){+}\mathbf{1} = \mathrm{y}$.

Pre každé prirodzené číslo n definujeme term Δ_n nasledovne: Δ_0 je $\mathbf{0}$, Δ_1 je $\mathbf{1}$ a pre $n \geq 1$ definujeme Δ_{n+1} ako $\Delta_n{+}\mathbf{1}$.

Každá z uvažovaných teórií je teóriou s rovnosťou a teda uzávery nasledovných formúl sú axiómy každej z nich:

$$\begin{aligned}
&\mathrm{x}{=}\mathrm{x},\\
&\mathrm{x}{=}\mathrm{y} \to \mathrm{y}{=}\mathrm{x},\\
&\mathrm{x}{=}\mathrm{y} \to (\mathrm{y}{=}\mathrm{z} \to \mathrm{x}{=}\mathrm{z}),\\
&(\mathrm{x}{=}\mathrm{y} \wedge \mathrm{u}{=}\mathrm{v}) \to \mathrm{x} + \mathrm{u}{=}\mathrm{y} + \mathrm{v},\\
&(\mathrm{x}{=}\mathrm{y} \wedge \mathrm{u}{=}\mathrm{v}) \to \mathrm{x} \cdot \mathrm{u}{=}\mathrm{y} \cdot \mathrm{v}.
\end{aligned}$$

Robinsonova aritmetika $\mathbf{T}_{\mathrm{Rob}}$ okrem uvedených axióm rovnosti má za axiómy naviac nasledujúce formuly alebo ich uzávery:

$$\begin{aligned}
&\mathrm{x}{+}\mathbf{0} = \mathrm{x},\\
&\mathrm{x}{+}(\mathrm{y} + \mathbf{1}){=}(\mathrm{x}{+}\mathrm{y}){+}\mathbf{1},\\
&\mathrm{x}{\cdot}\mathbf{0} = \mathbf{0},\\
&\mathrm{x}{\cdot}(\mathrm{y}{+}\mathbf{1}){=}(\mathrm{x}{\cdot}\mathrm{y}){+}\mathrm{x},\\
&\neg(\exists \mathrm{x})\,\mathrm{x}{+}\mathbf{1} = \mathbf{0},\\
&\mathrm{x}{+}\mathbf{1} = \mathrm{y}{+}\mathbf{1} \to \mathrm{x}{=}\mathrm{y},\\
&\neg\,\mathrm{x}{=}\,\mathbf{0} \to (\exists \mathrm{y})\,\mathrm{x}{=}\mathrm{y}{+}\mathbf{1}.
\end{aligned}$$

Dôležitá je tá skutočnosť, že teória $\mathbf{T}_{\mathrm{Rob}}$ má konečne mnoho axióm. **Presburgerova aritmetika** $\mathbf{T}_{\mathrm{Pres}}$ má nekonečne mnoho axióm. Okrem uvedených axióm rovnosti, pre každé prirodzené čísla n, m nasledujúce formuly sú axiómy tejto teórie:

$$\begin{aligned}
\Delta_{n+m} &= \Delta_n{+}\Delta_m\\
\Delta_{n\cdot m} &= \Delta_n{\cdot}\Delta_m,\\
\neg\Delta_n &= \Delta_m, \qquad \text{ak } n \neq m,\\
(\forall \mathrm{x})(\mathrm{x} &\leq \Delta_n \to (\mathrm{x}{=}\Delta_0 \vee \ldots \vee \mathrm{x}{=}\Delta_n)),\\
(\forall \mathrm{x})\,(\mathrm{x} &\leq \Delta_n \vee \Delta_n{\leq}\mathrm{x}).
\end{aligned}$$

V prvom riadku znamienko + vystupuje v dvoch úlohách. Na pravej strane je to názov operácie sčítania. Na ľavej strane predstavuje súčet metamatematických prirodzených čísiel. Podobne je to aj so znamienkom ·. Vzhľadom na asociatívnosť disjunkcie v štvrtom riadku nemusíme písať zátvorky.

Konečne Peanova aritmetika $\mathbf{T}_{\mathrm{P}}$ vznikne z Robinsonovej aritmetiky pridaním nekonečne mnoha axióm indukcie. Pre každú formulu φ uzáver nasledujúcej formuly je axióma Peanovej aritmetiky

$$(\varphi(\mathbf{0},\ldots)\wedge(\forall \mathrm{x})\,(\varphi(\mathrm{x},\ldots)\rightarrow\varphi(\mathrm{x}{+}\mathbf{1},\ldots)))\rightarrow(\forall \mathrm{y})\,\varphi(\mathrm{y},\ldots).$$

Teda Robinsonova aritmetika je slabšia ako Peanova aritmetika.

Tvrdenie 6.1 *Presburgerova aritmetika je slabšia ako Robinsonova aritmetika.*

Overenie: Ukážeme napríklad, že

$$\mathbf{T}_{\mathrm{Rob}}\vdash\Delta_{m+n}{=}\Delta_n{+}\Delta_m \tag{6.4}$$

pre každé metamatematické prirodzené čísla m, n. Ukážeme to metamatematickou indukciou cez m. n je pevné.

Kvôli ilustrácii pojmu "dôkaz" napíšeme dôkaz formuly $\Delta_{n+0}{=}\Delta_n{+}\Delta_0$ v teórii $\mathbf{T}_{\mathrm{Rob}}$.

1. $(\forall x)\,(x{+}\mathbf{0}{=}x)$,	ax. $\mathbf{T}_{\mathrm{Rob}}$
2. $(\forall x)\,(x{+}\mathbf{0}{=}x)\rightarrow(\Delta_n{+}\mathbf{0}{=}\Delta_n)$	APP
3. $\Delta_n{+}\mathbf{0}{=}\Delta_n$	m.p. $2,1$
4. $(\forall x)(\forall y)\,(x{=}y\rightarrow y{=}x)$	ax. rovnosti
5. $(\forall x)(\forall y)\,(x{=}y\rightarrow y{=}x)\rightarrow(\forall y)\,(\Delta_n{+}\mathbf{0}{=}y\rightarrow y{=}\Delta_n{+}\mathbf{0})$	APP
6. $(\forall y)\,(\Delta_n{+}\mathbf{0}{=}y\rightarrow y{=}\Delta_n{+}\mathbf{0})$	m.p. $5,4$
7. $(\forall y)\,(\Delta_n{+}\mathbf{0}{=}y\rightarrow y{=}\Delta_n{+}\mathbf{0})\rightarrow(\Delta_n{+}\mathbf{0}{=}\Delta_n\rightarrow\Delta_n{=}\Delta_n{+}\mathbf{0})$	APP
8. $(\Delta_n{+}\mathbf{0}{=}\Delta_n\rightarrow\Delta_n{=}\Delta_n{+}\mathbf{0})$	m.p. $7,6$
9. $\Delta_n{=}\Delta_n{+}\mathbf{0}$	m.p. $8,3$

Predpokladajme, že platí (6.4). Chceme ukázať, že formula

$$\Delta_{m+n+1}{=}\Delta_n{+}\Delta_{m+1} \tag{6.5}$$

je dokázateľná v $\mathbf{T}_{\mathrm{Rob}}$. Podľa definície termu Δ_p, term Δ_{m+1} je term $\Delta_m{+}\mathbf{1}$ a term Δ_{m+n+1} je term $\Delta_{m+n}{+}\mathbf{1}$. Teda formula (6.5) je formula

$$\Delta_n{+}(\Delta_m{+}\mathbf{1})\Delta_{m+n}{+}\mathbf{1}{=}\Delta_n{+}(\Delta_m{+}\mathbf{1}).$$

Ak do druhej axiómy Robinsonovej aritmetiky dosadíme za x term Δ_n a za y term Δ_n, dostaneme formulu

$$\Delta_n{+}(\Delta_m{+}\mathbf{1})\,{=}(\Delta_m{+}\Delta_n){+}\mathbf{1}$$

dokázateľnú v $\mathbf{T}_{\mathrm{Rob}}$. Použitím axióm rovnosti spolu s indukčným predpokladom (6.4) dostaneme, že formula (6.5) je dokázateľná v $\mathbf{T}_{\mathrm{Rob}}$.

Ukážeme ešte, že $\mathbf{T}_{\mathrm{Rob}} \vdash \neg\Delta_n{=}\Delta_m$ ak $n \neq m$. Použijeme metódu dôkazu sporom a teda pridáme novú axiómu $\Delta_n{=}\Delta_m$ ak $n \neq m$. Môžeme predpokladať, že $n < m$. Podľa definície Δ_n je term

$$(\ldots(\mathbf{0}+\underbrace{\mathbf{1})+\ldots\mathbf{1}}_{n})$$

a Δ_m je term

$$(\ldots(\mathbf{0}+\underbrace{\mathbf{1})+\ldots\mathbf{1}}_{m}).$$

n-násobným použitím axiómy

$$\mathrm{x}{+}\mathbf{1} = \mathrm{y}{+}\mathbf{1} \rightarrow \mathrm{x}{=}\mathrm{y}$$

dostaneme

$$\mathbf{0} = (\ldots(\mathbf{0}+\underbrace{\mathbf{1})+\ldots\mathbf{1}}_{m-n}),$$

čo je spor s piatou axiómou $\mathbf{T}_{\mathrm{Rob}}$.

q.e.d.

7 Definovateľnosť v teórii

V ďalšom $\mathbf{T}$ bude matematická teória s rovnosťou, ktorá má term Δ_n pre každé metamatematické prirodzené číslo n. Nech $f : \mathbb{N}^k \longrightarrow \mathbb{N}$ je (metamatematická) funkcia, φ je formula v jazyku teórie $\mathbf{T}$. Budeme hovoriť, že formula[3] $\varphi(\mathrm{x}_0, \ldots, \mathrm{x}_k)$ **definuje funkciu** f, ak pre ľubovoľné metamatematické prirodzené čísla $n_1, \ldots, n_k, m$ platí

(df1) ak $f(n_1, \ldots, n_k) = m$, tak $\mathbf{T} \vdash \varphi(\Delta_m, \Delta_{n_1}, \ldots, \Delta_{n_k})$;

(df2) ak $f(n_1, \ldots, n_k) \neq m$, tak $\mathbf{T} \vdash \neg\varphi(\Delta_m, \Delta_{n_1}, \ldots, \Delta_{n_k})$;

(df3) $\mathbf{T} \vdash (\forall x)(\forall y)\,((\varphi(\mathrm{x}, \Delta_{n_1}, \ldots, \Delta_{n_k}) \wedge \varphi(\mathrm{y}, \Delta_{n_1}, \ldots, \Delta_{n_k})) \rightarrow \mathrm{x}{=}\mathrm{y})$.

Podobne, ak $\mathcal{V}$ je výroková funkcia, tak formula ψ **definuje výrokovú funkciu** $\mathcal{V}$, ak pre ľubovoľné metamatematické prirodzené čísla $n_1, \ldots, n_k$ platí

(dv1) ak platí $\mathcal{V}(n_1, \ldots, n_k)$, tak $\mathbf{T} \vdash \psi(\Delta_{n_1}, \ldots, \Delta_{n_k})$;

(dv2) ak neplatí $\mathcal{V}(n_1, \ldots, n_k)$, tak $\mathbf{T} \vdash \neg\psi(\Delta_{n_1}, \ldots, \Delta_{n_k})$.

Nakoniec, funkcia f je **definovateľná v teórii** $\mathbf{T}$, ak existuje formula, ktorá ju definuje. Podobne pre výrokovú funkciu.

Z podmienok (df1) a (df3) vyplýva nasledujúce: ak ψ definuje funkciu f v teórii $\mathbf{T}$ a $f(n_1, \ldots, n_k) = m$ tak

$$\mathbf{T} \vdash (\forall x)\,(\varphi(\mathrm{x}, \Delta_{n_1}, \ldots, \Delta_{n_k}) \rightarrow \mathrm{x}{=}\Delta_m). \tag{7.6}$$

[3] Všimnite si, že premenná x_0 vyjadruje hodnotu funkcie!

Tvrdenie 7.1 *Ak teória* $\mathbf{T}$ *je silnejšia ako Presburgerova aritmetika* $\mathbf{T}_{\mathrm{Pres}}$*, tak každá všeobecne rekurzívna funkcia a každá rekurzívna výroková funkcia je definovateľná v teórii* $\mathbf{T}$*.*

Overenie: Princíp overenia je takýto. Ak funkcia f je definovateľná v teórii $\mathbf{T}_1$ a teória $\mathbf{T}_2$ je od nej silnejšia, tak f je definovateľná aj v teórii $\mathbf{T}_2$. Teda stačí overiť, že každá rekurzívna funkcia je definovateľná v teórii $\mathbf{T}_{\mathrm{Pres}}$.

Budeme sledovať ekvivalentnú definíciu všeobecne rekurzívnej funkcie podľa vety 4.1.
a) Každá funkcia zo zoznamu (4.3) je definovateľná v teórii $\mathbf{T}$. Naozaj, stačí zobrať postupne formuly

$$\begin{array}{ll}
\mathrm{Z}(n) = 0 & \mathrm{x}_0 = \mathbf{0}, \\
\mathrm{S}(n) = n + 1 & \mathrm{x}_0 = \mathrm{x}_1 + \mathbf{1}, \\
\mathrm{P}^{\mathrm{i}}_{\mathrm{k}}(n_1, \ldots, n_k) = n_i & \mathrm{x}_0 = \mathrm{x}_i, \\
\mathrm{add}(n, m) = k & \mathrm{x}_0 = \mathrm{x}_1 + \mathrm{x}_2, \\
\mathrm{prod}(n, m) = k & \mathrm{x}_0 = \mathrm{x}_1 \cdot \mathrm{x}_2, \\
\mathrm{odc}(n, m) = k & (\mathrm{x}_2 + \mathrm{x}_0 = \mathrm{x}_1) \vee (\mathrm{x}_1 < \mathrm{x}_2 \wedge \mathrm{x}_0 = \mathbf{0}).
\end{array}$$

b) Nech $f(x_1, \ldots, x_k) = h(f_i(x_1, \ldots, x_k), \ldots, f_n(x_1, \ldots, x_k))$ a predpokladáme, že formuly $\varphi_1, \ldots, \varphi_n, \psi$ definujú postupne funkcie $f_1, \ldots, f_n, h$. Potom formula

$$(\forall \mathrm{y}_1) \ldots (\forall \mathrm{y}_n) \left((\varphi_1(\mathrm{y}_1, \mathrm{x}_1, \ldots, \mathrm{x}_k) \wedge \ldots \wedge \varphi_n(\mathrm{y}_n, \mathrm{x}_1, \ldots, \mathrm{x}_k)) \rightarrow \right. \\ \left. \rightarrow \psi(\mathrm{x}_0, \mathrm{y}_1, \ldots, \mathrm{y}_n) \right)$$

definuje funkciu f. Overenie nechávame na čitateľa.
c) Ak funkcia f vznikla z funkcie h regulárnou minimalizáciou

$$f(n_1, \ldots, n_k) = (\min p)\, h(n_1, \ldots, n_k, p) = 0,$$

a formula ψ definuje funkciu h, tak čitateľ ľahko overí, že nasledujúca formula definuje funkciu f:

$$\psi(\Delta_0, \mathrm{x}_1, \ldots, \mathrm{x}_k, \mathrm{x}_0) \wedge (\forall \mathrm{y})\, (y < \mathrm{x}_0 \rightarrow \neg \psi(\Delta_0, \mathrm{x}_1, \ldots, \mathrm{x}_k, \mathrm{y})).$$

Skutočne, ak $f(n_1, \ldots, n_k) = m$, tak $h(n_1, \ldots, n_k, m) = 0$ a $h(n_1, \ldots, n_k, p) \neq 0$ pre $p < m$. Teda

$$\mathbf{T}_{\mathrm{Pres}} \vdash \psi(\Delta_0, \Delta_{n_1}, \ldots, \Delta_{n_k}, \Delta_m), \quad \mathbf{T}_{\mathrm{Pres}} \vdash \neg \psi(\Delta_0, \Delta_{n_1}, \ldots, \Delta_{n_k}, \Delta_p)$$

pre $p < m$. Použitím predposlednej axiómy Presburgerovej aritmetiky dostaneme

$$\psi(\Delta_0, \mathrm{x}_1, \ldots, \mathrm{x}_k, \Delta_m) \wedge (\forall \mathrm{y})\, (y < \Delta_m \rightarrow \neg \psi(\Delta_0, \mathrm{x}_1, \ldots, \mathrm{x}_k, \mathrm{y})).$$

Podobne by sme overili podmienky (df2) a (df3).

q.e.d.

8 Aritmetizácia

Pripomenieme si základy aritmetizácie formálnych jazykov, napríklad tak, ako boli prezentované v [BL1].

Prvočísla očíslujeme podľa veľkosti

$$p_0, p_1, \ldots, p_n, \cdots.$$

Teda napr. $p_0 = 2$, $p_3 = 7$ a $p_{10} = 31$. Nech $\mathcal{A} = \{a_0, \ldots, a_k\}$ je konečná alebo $\mathcal{A} = \{a_0, \ldots, a_k, \ldots\}$ je nekonečná spočítateľná abeceda. Každému znaku $a \in \mathcal{A}$ priradíme kladné prirodzené číslo $\mathrm{Gčz}(a)$, ktoré nazveme **Gödelovo číslo znaku** a. Priradenie bude vždy prosté. Teda rôznym znakom priradíme rôzne čísla.

Pripomeňme, ž $p_0, p_1, \ldots, p_n, \ldots$ je očíslovanie prvočísiel podľa veľkosti. Ak $\alpha = a_{i_0} \ldots a_{i_n}$ je slovo v abecede $\mathcal{A}$, tak **Gödelovo číslo slova** α bude číslo

$$\mathrm{Gčs}(\alpha) = p_0^{\mathrm{Gčz}(a_{i_0})} \cdot \ldots \cdot p_n^{\mathrm{Gčz}(a_{i_n})}.$$

Pre neprázdne slovo α v našej abecede platí, že jeho dĺžka je

$$\mathrm{dls}(\alpha) = \mathrm{dl}(\mathrm{Gčs}(\alpha)).$$

Ak α, β sú slová v našej abecede, tak pre číslo ich zreťazenia zrejme platí

$$\mathrm{Gčs}(\alpha * \beta) = \mathrm{Gčs}(\alpha) * \mathrm{Gčs}(\beta).$$

Musíme si uvedomiť, že symbol $*$ v uvedenej rovnosti hrá dve rozličné úlohy: na ľavej strane označuje operáciu zreťazenia dvoch slov a na pravej strane je to primitívne rekurzívna funkcia dvoch premenných definovaná v [BL1], str. 45.

Ak $\alpha_0, \ldots, \alpha_n$ je postupnosť slov, tak **Gödelove číslo** tejto **postupnosti** bude číslo

$$\mathrm{Gčp}(\alpha_0, \ldots, \alpha_n) = p_0^{\mathrm{Gčs}(\alpha_0)} \cdot \ldots \cdot p_n^{\mathrm{Gčs}(\alpha_n)}.$$

Ak $\mathcal{L}$ je jazyk predikátového počtu, tak príslušná abeceda, ktorú očíslujeme, vznikne tak, že k znakom jazyka $\mathcal{L}$ pridáme všetky "povinné" znaky, t.j. logické spojky, kvantifikátory, zátvorky a premenné a takto získané znaky zoradíme do postupnosti. Ich Gödelove čísla budú postupne kladné prirodzené čísla. Napríklad, jazyk aritmetiky $\mathcal{L}_{\mathrm{P}}$ indukuje abecedu a Gödelove čísla znakov tejto abecedy

$$\begin{array}{llllllllllllllllll} \neg, & \wedge, & \vee, & \rightarrow, & \equiv, & \forall, & \exists, & (, &), & =, & +, & \cdot, & \mathbf{0}, & \mathbf{1}, & \mathrm{x}_0, & \mathrm{x}_1, & \ldots, & \mathrm{x}_n, & \ldots \\ 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 11, & 12, & 13, & 14, & 15, & 16, & \ldots, & n+15, & \ldots. \end{array}$$

Ak máme definované nerovnosti, tak jazyk aritmetiky indukuje abecedu

$$\neg, \wedge, \vee, \rightarrow, \equiv, \forall, \exists, (,), =, \leq, <, +, \cdot, \mathbf{0}, \mathbf{1}, \mathrm{x}_0, \mathrm{x}_1, \ldots, \mathrm{x}_n, \ldots$$

s príslušne modifikovanými Gödelovými číslami.

Teraz môžeme upresniť pojem teórie, ako sme sľúbili v časti 5. Ak $\mathbf{T}$ je teória, tak výrokovú funkciu "n je číslo axiómy teórie $\mathbf{T}$" označíme $Axiom_{\mathbf{T}}(n)$. Budeme uvažovať len také teórie, pre ktoré $Axiom_{\mathbf{T}}$ **je rekurzívna výroková funkcia**.

Presburgerova a Peanova aritmetika majú nekonečne mnoho axióm. Ľahko vidieť, že v obidvoch prípadoch výrokové funkcie $Axiom_{\mathbf{T}_{\mathrm{Pres}}}$ a $Axiom_{\mathbf{T}_{\mathrm{P}}}$ sú primitívne rekurzívne.

Tvrdenie 8.1 *Nech $\mathcal{L}$ je jazyk predikátového počtu. Potom nasledujúce výrokové funkcie sú primitívne rekurzívne:*

$Term_{\mathcal{L}}(n)$	n je číslo termu v jazyku $\mathcal{L}$,
$Formula_{\mathcal{L}}(n)$	n je číslo formuly v jazyku $\mathcal{L}$,
$Form_{\mathcal{L}}(n)$	n je číslo uzavretej formuly v jazyku $\mathcal{L}$.

Overenie: Najprv skúmame výrokovú funckiu $VPT_{\mathcal{L}}(n)$, ktorá hovorí, že n číslo vytvárajúcej postupnosti termu v jazyku $\mathcal{L}$. Ľahko vidieť, že $VPT_{\mathcal{L}}(n)$ je primitívne rekurzívna. Napríklad, pre abecedu aritmetiky $\mathcal{L} = \mathcal{L}_{\mathrm{P}}$ výroková funkcia $VPT_{\mathcal{L}}(n)$ je ekvivalentná výrokovej funkcii

$$\begin{aligned}&\text{pre každé } i \le \mathrm{dl}(n)\ \ \{((n)_i = 13 \text{ alebo } (n)_i = 14 \text{ alebo } (n)_i > 14)) \text{ alebo}\\ &\quad (\text{existujú } j,k < i \ \text{ také, že } (n)_i = 2^8 * (n)_j * 2^{11} * (n)_k * 2^9) \text{ alebo}\\ &\quad (\text{existujú } j,k < i \ \text{ také, že } (n)_i = 2^8 * (n)_j * 2^{12} * (n)_k * 2^9)\}.\end{aligned}$$

Uvedená výroková funkcia je primitívne rekurzívna.

Ak m je číslo termu $\mathbf{t}$, tak existuje vytvárajúca postupnosť $\mathbf{t}_0, \ldots, \mathbf{t}_k$ termu $\mathbf{t} = \mathbf{t}_k$ taká, že číslo každého termu $\mathbf{t}_i$ nie je väčšie ako číslo termu $\mathbf{t}$ a dĺžka tejto postupnosti je $k \le m$. Teda číslo tejto vytvárajúcej postupnosti nie je väčšie ako

$$l = \prod_{i=0}^{m} p_i^m.$$

Potom výroková funkci $Term_{\mathcal{L}}(m)$ je ekvivalentná výrokovej funkcii

$$\text{existuje } n \le l \text{ také, že } (VPT_{\mathcal{L}}(n) \text{ a } (n)_{\mathrm{dl}(n)} = m).$$

Podobne v ostatných prípadoch.

q.e.d.

Výrokovú funkciu "m je číslo dôkazu formuly s číslom n v teórii $\mathbf{T}$" označíme $\mathrm{Dokaz}_{\mathbf{T}}(m,n)$.

Tvrdenie 8.2 *Ak výroková funckia* $\mathrm{Axiom}_{\mathbf{T}}(n)$ *je (primitívne) rekurzívna, tak je (primitívne) rekurzívna aj výroková funkcia* $\mathrm{Dokaz}_{\mathbf{T}}(m,n)$.

Overenie: Stačí prepísať definíciu pojmu dôkaz do reči Gödelových čísiel príslušných pojmov.

q.e.d.

Funkciu $diag_{\mathcal{L}}$ definujeme takto:

ak n je číslo formuly $\varphi(\mathrm{x}_0, \ldots, \mathrm{x}_k)$, ktorá obsahuje premennú x_0 volne, tak $diag_{\mathcal{L}}(n)$ je číslo formuly $\varphi(\Delta_n, \mathrm{x}_1, \ldots, \mathrm{x}_k)$;

ak n nie je také číslo, tak $diag_{\mathcal{L}}(n) = n$.

Tvrdenie 8.3 *Funkcia $diag_{\mathcal{L}}$ je primitívne rekurzívna.*

Ak jazyk $\mathcal{L}$ je jazyk teórie $\mathbf{T}$, tak namiesto indexu $\mathcal{L}$ budeme písať index $\mathbf{T}$. Naviac, ak jazyk $\mathcal{L}$ alebo teória $\mathbf{T}$ sú zrejmé z kontextu, tak index $\mathcal{L}$ alebo $\mathbf{T}$ budeme vynechávať.

9 Tarského Veta

Nech $Dok_{\mathbf{T}}(n)$ označuje výrokovú funkciu "n je číslo uzavretej formuly dokázateľnej v teórii $\mathbf{T}$". Zrejme $Dok_{\mathbf{T}}(n)$ je ekvivalentné výrokovej funkcii

$$Form_{\mathbf{T}}(n) \text{ a existuje } m \text{ také, že } Dokaz_{\mathbf{T}}(m, n).$$

Teda, ak $Axiom_{\mathbf{T}}$ je rekurzívna (ale to je náš základný predpoklad), tak $Dok_{\mathbf{T}}$ je rekurzívne očíslovateľná. Ukážeme, že táto výroková funkcia je spravidla nerekurzívna.

Tvrdenie 9.1 *(A. Tarski) Ak teória $\mathbf{T}$ je neprotirečivá, tak funkcia $diag_{\mathbf{T}}$ a výroková funkcia $Dok_{\mathbf{T}}$ nie sú súčasne definovateľné v teórii $\mathbf{T}$.*

Overenie: Predpokladajme opak, že obidve funkcie $diag_{\mathbf{T}}$ a $Dok_{\mathbf{T}}$ sú definovateľné v teórii $\mathbf{T}$ a to formulami χ a ψ. Teda

(t1) ak $diag_{\mathbf{T}}(n) = m$, tak $\mathbf{T} \vdash \chi(\mathbf{\Delta_m}, \mathbf{\Delta_n})$,

(t2) ak $diag_{\mathbf{T}}(n) \neq m$, tak $\mathbf{T} \vdash \neg\chi(\mathbf{\Delta_m}, \mathbf{\Delta_n})$,

(t3) pre každé n je $\mathbf{T} \vdash (\forall \mathrm{x})(\forall \mathrm{y})\,((\chi(\mathrm{x}, \mathbf{\Delta_n}) \wedge \chi(\mathrm{y}, \mathbf{\Delta_n}) \rightarrow \mathrm{x}{=}\mathrm{y})$,

(t4) ak platí $Dok_{\mathbf{T}}(n)$, tak $\mathbf{T} \vdash \psi(\mathbf{\Delta_n})$,

(t5) ak neplatí $Dok_{\mathbf{T}}(n)$, tak $\mathbf{T} \vdash \neg\psi(\mathbf{\Delta_n})$.

Nech k je Gödelovo číslo formuly

$$(\forall \mathrm{y})\,(\chi(\mathrm{y}, \mathrm{x}_0) \rightarrow \neg\psi(\mathrm{y})).$$

Potom $n = diag_{\mathbf{T}}(k)$ je číslo formuly

$$(\forall \mathrm{y})\,(\chi(\mathrm{y}, \Delta_k) \rightarrow \neg\psi(\mathrm{y})),$$

ktorú označíme Ω. Podľa (7.6) máme

$$\mathbf{T} \vdash \chi(\mathrm{y}, \Delta_k) \rightarrow \mathrm{y}{=}\Delta_n. \tag{9.7}$$

Predpokladajme, že $\mathbf{T} \vdash \Omega$. Potom platí $Dok_{\mathbf{T}}(n)$ a na základe podmienky (t4) máme $\mathbf{T} \vdash \psi(\Delta_n)$. Z druhej strany, na základe (t1) a definície Ω máme $\mathbf{T} \vdash \neg\psi(\Delta_n)$, čo nie je možné na základe predpokladu neprotirečivosti teórie $\mathbf{T}$. Teda $\mathbf{T} \nvdash \Omega$.

Potom neplatí $Dok_{\mathbf{T}}(n)$ a podľa (t5) dostávame $\mathbf{T} \vdash \neg\psi(\Delta_n)$. Zrejme potom máme aj

$$\mathbf{T} \vdash \mathrm{y} = \Delta_n \rightarrow \neg\psi(\mathrm{y}).$$

Toto spolu s (9.7) dáva

$$\mathbf{T} \vdash \Omega,$$

čo je spor.

q.e.d.

Korektný názov nasledujúcej vety by mal byť "o nedefinovateľnosti dokazateľnosti". Prikláňame sa k názvu, ktorý použil A. Tarski v [Ta1].

Tvrdenie 9.2 (Tarského veta o nedefinovateľnosti pravdy) *Ak teória* $\mathbf{T}$ *je neprotirečivá a silnejšia ako Presburgerova aritmetika* $\mathbf{T}_{\mathrm{Pres}}$*, tak* $Dok_{\mathbf{T}}$ *nie je definovateľná v teórii* $\mathbf{T}$*.*

Overenie: Každá rekurzívna funkcia je definovateľná v teórii $\mathbf{T}$, špeciálne aj funkcia $diag_{\mathbf{T}}$. Ak $\mathbf{T}$ je neprotirečivá, tak podľa vety 9 výroková funckia $Dok_{\mathbf{T}}$ nie je definovateľná v teórii $\mathbf{T}$.

q.e.d.

Tvrdenie 9.3 (Tarského veta o nerozhodnuteľnosti aritmetiky) *Ak teória* $\mathbf{T}$ *je neprotirečivá a silnejšia ako Presburgerova aritmetika* $\mathbf{T}_{\mathrm{Pres}}$*, tak* $Dok_{\mathbf{T}}$ *nie je rekurzívna. Inými slovami, neexistuje algoritmus, ktorý by rozhodol, či daná uzavretá formula je dokázateľná v teórii* $\mathbf{T}$ *alebo nie.*

Overenie: Keďže výroková funckia $Dok_{\mathbf{T}}$ nie je definovateľná v teórii $\mathbf{T}$, tak nie je rekurzívna.

q.e.d.

Ak výroková funkcia $Dok_{\mathbf{T}}$ nie nie je rekurzívna, tak podľa A. Tarského [Ta2] teória $\mathbf{T}$ sa nazýva **nerozhodnuteľná**. Tento názov nie je v súlade s tým, čo sme povedali o pojmoch "neriešiteľný" a "nerozhodnuteľný" v časti 5. Termín sa však v literatúre ustálil – pozri napr. [Sh], [HPu]. Tarského veta 9.3 teda tvrdí, že ak teória $\mathbf{T}$ je neprotirečivá a silnejšia ako Presburgerova aritmetika, tak je nerozhodnuteľná. Dokonca je nerozhodnuteľná každá od nej silnejšia neprotirečivá teória (s rekurzívnym $\mathrm{Axiom}_{\mathbf{T}}$). Tarski takúto teóriu nazval **podstatne nerozhodnuteľná**.

Využijeme uvedený výsledok pre informáciu o predikátovom počte.

Dôsledok 9.4 *Ak Robinsonova aritmetika je neprotirečivá, tak neexistuje algoritmus, ktorý by rozhodol, ktorá uzavretá formula v jazyku uvedenom v časti 5 je dokázateľná v predikátovom počte (teda v prázdnej množine axióm) a ktorá nie je.*

Overenie: Podľa tvrdenia 9.2 neexistuje taký algoritmus pre Robinsonovu aritmetiku. Nech ψ je konjunkcia axióm Robinsonovej aritmetiky (môžeme ju utvoriť, lebo Robinsonova aritmetika má konečne mnoho axióm - dvanásť). Podľa

vety o dedukcii pre ľubovoľnú uzavretú formulu φ platí

$$\mathbf{T}_{Rob} \vdash \varphi \text{ vtedy a len vtedy, keď } \emptyset \vdash \psi \to \varphi.$$

Z uvedenej ekvivalencie bezprostredne vyplýva tvrdenie dôsledku.

q.e.d.

Zavedieme označenie, ktoré výhodne využijeme. Množina

$$F_{\mathbf{T}} = \{n \in \mathbb{N}; Form_{\mathbf{T}}(n)\}$$

je rekurzívna. Pre $n \in F_{\mathbf{T}}$ nech δ_n je uzavretá formula s číslom n. Označíme

$$P_{\mathbf{T}} = \{n \in F_{\mathbf{T}}; \mathbf{T} \vdash \delta_n\},$$
$$R_{\mathbf{T}} = \{n \in F_{\mathbf{T}}; \mathbf{T} \vdash \neg\delta_n\}.$$

Tarského veta o nedefinovateľnosti pravdy teda tvrdí, že množina $P_{\mathbf{T}}$ nie je rekurzívna. Keďže predpokladáme, že $Axiom_{\mathbf{T}}$ je rekurzívna, tak obidve množiny sú rekurzívne očíslovateľné, lebo[4]

$$n \in P_{\mathbf{T}} \iff \text{existuje } m \text{ také, že } Dokaz_{\mathbf{T}}(m, n),$$
$$n \in R_{\mathbf{T}} \iff \text{existuje } m \text{ také, že } Dokaz_{\mathbf{T}}(m, 2^1 * n).$$

Zrejme podmienka neprotirečivosti teórie $\mathbf{T}$ je ekvivalentná podmienke

$$P_{\mathbf{T}} \cap R_{\mathbf{T}} = \emptyset.$$

Tvrdenie 9.5 (Gödelova veta o neúplnosti aritmetiky) *Ak* $\mathbf{T}$ *je neprotirečivá teória silnejšia ako Presburgerova aritmetika* $\mathbf{T}_{\text{Pres}}$*, tak* $\mathbf{T}$ *nie je úplná, t.j. existuje uzavretá formula* φ *v jazyku teórie* $\mathbf{T}$ *taká, že* $\mathbf{T} \nvdash \varphi$ *a* $\mathbf{T} \nvdash \neg\varphi$.

Overenie: Keby $P_{\mathbf{T}} \cup R_{\mathbf{T}} = F_{\mathbf{T}}$, tak na základe neprotirečivosti teórie $\mathbf{T}$ máme $P_{\mathbf{T}} \cap R_{\mathbf{T}} = \emptyset$. Keďže obidve množiny $P_{\mathbf{T}}$ a $R_{\mathbf{T}}$ sú rekurzívne očíslovateľné, tak podľa Postovej vety by množina $P_{\mathbf{T}}$ bola rekurzívna, čo je spor s vetou 9.2.

Teda existuje prirodzené číslo $n \in F_{\mathbf{T}}$, $n \notin P_{\mathbf{T}} \cup R_{\mathbf{T}}$. Potom $\mathbf{T} \nvdash \delta_n$ a $\mathbf{T} \nvdash \neg\delta_n$.

q.e.d.

Predvedený dôkaz Gödelovej vety je nekonštruktívny. Neuviedli sme príklad nerozhodnuteľnej vety. Vieme len, že existuje. V ďalších dvoch častiach podáme konštrukciu takejto formuly.

Napriek nekonštruktívnosti prezentovaný dôkaz Gödelovej vety je dôležitý z nasledujúceho dôvodu: dáva do súvisu dva základné pojmy. Ukazuje, že z neriešiteľnosti problému dokazateľnosti vyplýva existencia nerozhodnuteľnéj vety.

[4] pripomínam, že $\text{Gčz}(\neg) = 1$.

10 Gödelova veta o neúplnosti

V tejto časti prezentujeme klasickú Gödelovu konštrukciu nerozhodnuteľnej vety. K ukázaniu jej nerozhodnuteľnosti však potrebujeme silnejšie predpoklady o teórii. Tento nedostatok odstránime v ďalšej časti.

V tvrdení 9.1 sme zostrojili formulu Ω, ktorá hovorila "ja nie som dokázateľná". Avšak táto formula bola zostrojená za predppokladov, ktoré nakoniec viedli k sporu. Teraz zostrojíme takú formulu bez akýchkoľvek ďalších predpokladov na teóriu $\mathbf{T}$. Jediné čo predpokladáme je, že $\mathbf{T}$ je ω-neprotirečivá (definíciu pozri ďalej) teória silnejšia ako Presburgerova aritmetika $\mathbf{T}_{\mathrm{Pres}}$, pre ktorú je množina jej axióm rekurzívna.

Za uvedených predpokladov je výroková funkcia $Dokaz_{\mathbf{T}}$ rekurzívna a teda existuje formula φ, ktorá ju definuje v teórii $\mathbf{T}$. Teda
(g1) ak platí $Dokaz_{\mathbf{T}}(m,n)$, tak $\mathbf{T} \vdash \varphi(\Delta_m, \Delta_n)$,
(g2) ak neplatí $Dokaz_{\mathbf{T}}(m,n)$, tak $\mathbf{T} \vdash \neg\varphi(\Delta_m, \Delta_n)$.
Nech formula χ definuje funkciu $diag_{\mathbf{T}}$, teda platia podmienky (t1) – (t3). Nech l je číslo formuly

$$(\forall \mathrm{y})\,(\chi(\mathrm{y}, \mathrm{x}_0) \to \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \mathrm{y})).$$

Potom $m = diag(l)$ je číslo formuly

$$(\forall \mathrm{y})\,(\chi(\mathrm{y}, \Delta_l) \to \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \mathrm{y})).$$

Označíme ju Θ. Potom

$$\mathbf{T} \vdash \Theta \to (\chi(\Delta_m, \Delta_l) \to \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \Delta_m))$$

a na základe (t1)

$$\mathbf{T} \vdash \Theta \to \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \Delta_m).$$

Na základe (g1) a (g3) máme

$$\mathbf{T} \vdash \chi(\mathrm{y}, \Delta_l) \to \mathrm{y} = \Delta_m \tag{10.8}$$

a teda

$$\mathbf{T} \vdash \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \Delta_m) \to (\chi(\mathrm{y}, \Delta_l) \to \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \mathrm{y})).$$

Úhrnom máme

$$\mathbf{T} \vdash \Theta \equiv \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \Delta_m)). \tag{10.9}$$

Keby bolo $\mathbf{T} \vdash \Theta$, tak existuje dôkaz tejto formuly v teórii $\mathbf{T}$ s číslom p. Teda platilo by $Dokaz_{\mathbf{T}}(p, m)$, podľa podmienky (dv1) aj $\mathbf{T} \vdash \varphi(\Delta_p, \Delta_m)$ a teda $\mathbf{T} \vdash (\exists \mathrm{u})\,\varphi(\mathrm{u}, \Delta_m)$, čo je spor s (10.9).

Takže

$$\mathbf{T} \nvdash \Theta \tag{10.10}$$

a podľa (10.9) dostávame

$$\mathbf{T} \nvdash \neg(\exists \mathrm{u})\,\varphi(\mathrm{u}, \Delta_m). \tag{10.11}$$

Z druhej strany, žiadne prirodzené číslo nemôže byť číslom dôkazu formuly s číslom m, t.j. pre žiadne p neplatí $Dokaz_{\mathbf{T}}(p, m)$. Podľa (dv2) dostávame, že

$$\mathbf{T} \vdash \neg\varphi(\Delta_p, \Delta_m) \text{ pre každé prirodené číslo } p. \tag{10.12}$$

Z (10.11) dostávame

$$\mathbf{T} \nvdash (\forall \mathrm{u})\, \neg\varphi(\mathrm{u}, \Delta_m).$$

Všimnite si kontrast medzi posledným tvrdením a (10.12).

Teória $\mathbf{T}$ sa nazýva **ω-protirečivá**, ak existuje formula ψ taká,že

$$\mathbf{T} \vdash (\exists \mathrm{u})\, \psi(\mathrm{u}) \text{ a } \mathbf{T} \vdash \neg\psi(\Delta_p) \text{ pre každé číslo } p.$$

Teória je **ω-neprotirečivá**, ak nie je ω-protirečivá. Zrejme ω-neprotirečivá teória je neprotirečivá. Naopak to neplatí.

Skutočne, podľa (10.11) teória $\mathbf{T}_1 = \mathbf{T} + (\exists \mathrm{u})\, \varphi(\mathrm{u}, \Delta_m)$ je neprotirečivá. Podľa (10.12) však teória $\mathbf{T}_1$ je ω-protirečivá – úlohu formuly $\psi(\mathrm{x})$ hrá formula $\varphi(\mathrm{x}, \Delta_m)$.

Tvrdenie 10.1 (Gödelova veta o neúplnosti) *Ak* $\mathbf{T}$ *je ω-neprotirečivá teória silnejšia ako Presburgerova aritmetika, tak* Θ *je nerozhodnuteľná veta tejto teórie, t.j.* $\mathbf{T}$ *nie je úplná.*

Overenie: Podľa (10.10) je $\mathbf{T} \nvdash \Theta$. Podľa (10.12) a ω-neprotirečivosti dostávame

$$\mathbf{T} \nvdash (\exists \mathrm{u})\, \varphi(\mathrm{u}, \Delta_m).$$

Podľa (10.9) potom máme $\mathbf{T} \nvdash \neg\Theta$.

q.e.d.

Ak pripustíme existenciu aktuálneho nekonečna, tak Peanova aritmetika $\mathbf{T}_{\mathrm{P}}$ je neprotirečivá a aj ω-neprotirečivá.

Z teórie množín je známe, že existencia aktuálneho nekonečna je ekvivalentná s existenciou množiny prirodzených čísiel $\mathbb{N}$. Potom $\mathcal{N} = \langle \mathbb{N}, =, +, \cdot, 0, 1 \rangle$ je model Peanovej aritmetiky $\mathbf{T}_{\mathrm{P}}$. Nech ψ je taká formula, že $\mathbf{T}_{\mathrm{P}} \vdash \neg\psi(\Delta_n)$ pre každé prirodzené číslo $n \in \mathbb{N}$. Pre ľubovoľné ohodnotenie premenných v platí $v(\Delta_n) = n$. Žiadne ohodnotenie v sa nedá zmeniť na iné ohodnotenie u také, aby $\mathcal{N} \nvDash_u \psi(\mathrm{x})$. Skutočne, pre ľubovoľné ohodnotenie u je $u(x) = n$ pre nejaké $n \in \mathbb{N}$. Podľa predpokladu však $\mathcal{N} \vDash \neg\psi(n)$. Podľa definície relácie $\models$ dostávame $\mathcal{N} \nvDash (\exists \mathrm{x})\, \psi(\mathrm{x})$. Potom $\mathbf{T}_{\mathrm{P}} \nvdash (\exists \mathrm{x})\, \psi(\mathrm{x})$. Teda teória $\mathbf{T}_{\mathrm{P}}$ je ω-neprotirečivá.

Špeciálne, za predpokladu existencie aktuálneho nekonečna je $\mathbf{T}_{\mathrm{P}} \nvdash \neg\Theta$.

Zostrojíme príklad dôležitej ω-protirečivej teórie silnejšej ako Peanova aritmetika. Do jazyka aritmetiky pridáme novú individuálnu konštantu ∞, ktorá bude označovať "nekonečne veľké" prirodzené číslo. Nech α_n je formula $\Delta_n < \infty$. Teória $\mathbf{T}_{\mathrm{NA}}$, ktorú nazveme **neštandartná aritmetika**, vznikne z Peanovej aritmetiky $\mathbf{T}_{\mathrm{P}}$ pridaním nekonečne mnoha axióm α_n, n metamatematické prirodzené číslo. Podľa vety o kompaktnosti teória $\mathbf{T}_{\mathrm{NA}}$ je neprotirečivá vtedy a len vtedy, keď je neprotirečivá každá jej konečná podteória. Ak $\mathbf{T}$ je konečná podteória teórie $\mathbf{T}_{\mathrm{NA}}$, tak existuje len konečne mnoho axióm α_n teórie $\mathbf{T}$. Potom

existuje prirodzené číslo m také, že $n < m$ pre každú axiómu α_n teórie $\mathbf{T}$. Zostrojíme syntaktický model teórie $\mathbf{T}$ v teórii $\mathbf{T}_{\mathrm{P}}$: všetky objekty interpretujeme identicky a induviduálnu konštantu ∞ ako Δ_m. Teda, ak $\mathbf{T}_{\mathrm{P}}$ je neprotirečivá, tak aj teória $\mathbf{T}$ je neprotirečivá. Potom podľa spomenutej vety o kompaktnosti je neprotirečivá aj teória $\mathbf{T}_{\mathrm{NA}}$.

Nech ψ je formula $\mathrm{u} > \infty$. Zrejme $\mathbf{T}_{\mathrm{NA}} \vdash (\exists \mathrm{u})\, \psi(\mathrm{u})$ a $\mathbf{T}_{\mathrm{NA}} \vdash \neg\psi(\Delta_n)$ pre každé metamatematické prirodzené číslo n. Teda $\mathbf{T}_{\mathrm{NA}}$ je ω-protirečivá.

11 Gödelova veta podľa Rossera

V tejto časti podáme konštruktívny dôkaz Gödelovej vety o neúplnosti 9.5. Modifikácia pôvodného Gödelovho dôkazu pochádza z roku 1936 a jej autorom je J. B. Rosser.

Overenie: Rovnako ako vyššie, $\mathbf{T}$ je neprotirečivá teória silnejšia ako Presburgerova aritmetika s rekurzívnou množinou axióm.

Ľahko vidieť, že nasledujúce výrokové funkcie sú rekurzívne, dokonca primitívne rekurzívne:

$\mathcal{V}_1(n, m)$	m je číslo formuly $\varphi(\mathrm{x}_0)$ a n je číslo dôkazu formuly $\varphi(\Delta_m)$;
$\mathcal{V}_2(n, m)$	m je číslo formuly $\varphi(\mathrm{x}_0)$ a n je číslo dôkazu formuly $\neg\varphi(\Delta_m)$.

Potom obidve sú definovateľné v teórii $\mathbf{T}$. Nech ν_1 a ν_2 sú formuly, ktoré ich definujú. Musíme si uvedomiť, že formuly ν_1 a ν_2 závisia od teórie $\mathbf{T}$, presnejšie od formuly, ktorá definuje výrokovú funkciu $Axiom_{\mathbf{T}}$.

Ak q je číslo formuly

$$(\forall \mathrm{u})\, (\nu_1(\mathrm{u}, \mathrm{x}_0) \to (\exists \mathrm{v})\, (\mathrm{v} \leq \mathrm{u} \wedge \nu_2(\mathrm{v}, \mathrm{x}_0))),$$

tak $p = diag(q)$ je číslo formuly

$$\Gamma = (\forall \mathrm{u})\, (\nu_1(\mathrm{u}, \Delta_q) \to (\exists \mathrm{v})\, (\mathrm{v} \leq \mathrm{u} \wedge \nu_2(\mathrm{v}, \Delta_q))).$$

Ukážeme, že Γ je nerozhodnuteľná veta teórie $\mathbf{T}$.

Predpokladajme, že $\mathbf{T} \vdash \Gamma$. Potom existuje dôkaz v teórii $\mathbf{T}$ formuly Γ. Nech r je jeho číslo. Teda platí $\mathcal{V}_1(r, q)$ a podľa (dv1) aj $\mathbf{T} \vdash \nu_1(\Delta_r, \Delta_q)$. Potom

$$\mathbf{T} \vdash (\exists \mathrm{v})(\mathrm{v} \leq \Delta_r \wedge \nu_2(\mathrm{v}, \Delta_q)). \tag{11.13}$$

Nasledujúca formula je axióma Presburgerovej aritmetiky

$$\mathrm{v} \leq \Delta_r \to (\mathrm{v} = \Delta_0 \vee \mathrm{v} = \Delta_1 \vee \ldots \vee \mathrm{v} = \Delta_r). \tag{11.14}$$

Na základe predpokladu neprotirečivosti teórie $\mathbf{T}$ neplatí ani jeden z výrokov $\mathcal{V}_2(0, q), \ldots, \mathcal{V}_2(r, q)$ a teda

$$\mathbf{T} \vdash \neg\nu_2(\Delta_0, \Delta_q),\ \ldots\ , \mathbf{T} \vdash \neg\nu_2(\Delta_r, \Delta_q),$$

čo je spor s (11.13) a (11.14). Teda $\mathbf{T} \nvdash \Gamma$.

Predpokladajme teraz, že $\mathbf{T} \vdash \neg\Gamma$. Teda existuje dôkaz v $\mathbf{T}$ formuly $\neg\Gamma$. Ak s je jeho číslo, tak platí $\mathcal{V}_2(s, q)$ a podľa (dv1) aj $\mathbf{T} \vdash \nu_2(\Delta_s, \Delta_q)$ a teda

$$\mathbf{T} \vdash \Delta_s < \mathrm{u} \rightarrow (\exists \mathrm{v})\,(\mathrm{v} \leq \mathrm{u} \wedge \nu_2(\mathrm{v}, \Delta_q). \tag{11.15}$$

Na základe neprotirečivosti žiadne číslo nie je číslo dôkazu formuly Γ, teda špeciálne $\mathcal{V}_1(i, q)$ neplatí pre žiadne $i \leq s$. Teda

$$\mathbf{T} \vdash \neg\nu_1(\Delta_0, \Delta_q) \wedge \ldots \wedge \neg\nu_1(\Delta_s, \Delta_q).$$

Odtiaľ pomocou štvrtej axiómy Presburgerovej aritmetiky dostávame

$$\mathbf{T} \vdash (\mathrm{u} \leq \Delta_s \rightarrow \neg\nu_1(\mathrm{u}, \Delta_q).$$

a pomocou piatej axiómy

$$\mathbf{T} \vdash (\nu_1(\mathrm{u}, \Delta_q) \rightarrow \Delta_s < \mathrm{u}). \tag{11.16}$$

(11.15) a (11.16) spolu dávajú $\mathbf{T} \vdash \Gamma$, čo je spor. Teda $\mathbf{T} \nvdash \neg\Gamma$.

q.e.d.

Nech φ je formula, ktorá definuje výrokovú funkciu $Dokaz_{\mathbf{T}}$ – pozri overenie v predchádzajúcej časti. Teória $\mathbf{T}$ silnejšia ako Presburgerova aritmetika je neprotirečivá vtedy a len vtedy, keď formula $\neg\mathbf{0} = \mathbf{1}$ nie je dokazateľná v $\mathbf{T}$. Uvedená formula má Gödelove číslo $r = 2^1 \cdot 3^{13} \cdot 5^{10} \cdot 7^{14}$. Teda neprotirečivosť teórie $\mathbf{T}$ je ekvivalentná výrokovej funkcii "neexistuje také m, že $Dokaz_{\mathbf{T}}(m, r)$". Za formalizáciu tohoto výroku môžeme pokladať formulu $\neg(\exists \mathrm{x}_0)\,\varphi(\mathrm{x}_0, \Delta_r)$, ktorú skrátene označíme $\mathrm{Cons}_{\mathbf{T}}$.

Tvrdenie 11.1 (Druhá Gödelova veta) *Ak teória* $\mathbf{T}$ *je silnejšia ako Peanova aritmetika a je neprotiračivá, tak* $\mathbf{T} \nvdash \mathrm{Cons}_{\mathbf{T}}$.

Matematici sú presvedčemí, že každé finitné overenie, t.j. také, ktoré používa len konštruktívne úvahy a nepoužíva aktuálne nekonečno, možno "formalizovať" v Peanovej aritmetike a teda aj v silnejších teóriách. Keby sme teda finitnými prostriedkami overili neprotirečivosť Peanovej aritmetiky, tak toto overenie môžeme sformalizovať a získať tak dôkaz formuly $\mathrm{Cons}_{\mathbf{T}_P}$ v $\mathbf{T}_P$ - podľa druhej Gödelovej vety to však nie je možné, jedine v prípade, že $\mathbf{T}_P$ je protirečivá. Záver: ak finitnými prostriedkami "ukážete" neprotirečivosť Peanovej aritmetiky, tak ukážete, že je protirečivá.

Podobný výsledok platí aj pre teóriu množín. Podobne ako pre Peanovu aritmetiku možno ukázať aj pre teóriu množín **ZF** "druhú Gödelovu vetu": ak teória **ZF** je neprotirečivá, tak $\mathbf{ZF} \nvdash \mathrm{Cons}_{\mathbf{ZF}}$. A podobne: ak metódami teórie množín ukážete, že **ZF** je neprotirečivá, tak toto overenie možno formalizovať v **ZF** a teda toto overenie je overením toho, že **ZF** je protirečivá.

12 Iná nerozhodnuteľná veta Peanovej aritmetiky

V kombinatorike sú známe **vety Ramseyovho typu**[5]. Sformulujeme základné pojmy.

Ak X je množina, $[X]^k$ označuje množinu všetkých jej k-prvkových podmnožín. Nech $F : [X]^k \longrightarrow \{1, \ldots, n\}$. Zobrazenie F sa nazýva farbenie. Množina $Y \subseteq X$ sa nazýva **homogenná**[6] ak existuje $i \in \{1, \ldots, n\}$ také, že $F(u) = i$ pre každé $u \in [Y]^k$. **Relácia delenia** $p \longrightarrow (m)^k_n$ znamená: pre každé zobrazenie $F : \{1, 2, \ldots, p\}^k \longrightarrow \{1, \ldots, n\}$ existuje homogenná podmnožina $Y \subseteq \{1, \ldots, p\}$ mohutnosti m.

Typická veta Ramseyovho typu je

Veta 12.1

$$(\forall k, m, n)(\exists p)\, p \longrightarrow (m)^k_n$$

Môžete sa pokúsiť dokázať, že platí

$$6 \longrightarrow (3)^2_2, \quad 24 \longrightarrow (4)^2_2, \quad 17 \longrightarrow (3)^2_3.$$

Definujeme **silnejšiu reláciu delenia**. $p \stackrel{*}{\longrightarrow} (m)^k_n$ znamená: pre každé zobrazenie $F : \{1, \ldots, p\}^k \longrightarrow \{1, \ldots, n\}$ existuje homogenná podmnožina $Y \subseteq \{1, \ldots, p\}$ mohutnosti m taká, že najmenší prvok množiny Y nie je väčší ako m.

Zrejme definované relácie delenia vieme formulovať aj bez použitia jazyka teórie množín, len v jazyku aritmetiky. Potom použitím techník kódovania postupností prirodzených čísiel možno zostrojiť formulu aritmetiky $\varphi(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4)$ ktorá definuje výrokovú funkciu $p \stackrel{*}{\longrightarrow} (m)^k_n$ v Peanovej aritmetike $\mathbf{T}_P$. Poradie premenných v poslednej je p, m, k, n.

Tvrdenie 12.1 (L. Harrington a J. Paris)

a) *Ak Peanova aritmetika* $\mathbf{T}_P$ *je neprotirečivá, tak*

$$\mathbf{T}_P \nvdash (\forall \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4)(\exists \mathrm{x}_1)\, \varphi(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4).$$

b) *Ak* **ZF** *označuje Zermelovu-Fraenkelovu teóriu množín tak*

$$\mathbf{ZF} \vdash (\forall \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4)(\exists \mathrm{x}_1)\, \varphi(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4).$$

Teda, ak Peanova aritmetika je neprotirečivá, tak

$$(\forall \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4)(\exists \mathrm{x}_1)\, \varphi(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4)$$

je jej nerozhodnuteľná veta.

[5] Je zaujímavé, že výsledky tohoto typu boli objavené pre potreby matematickej logiky a tam boli aj intenzívne využité.

[6] alebo jednofarebná,

Overenie časti a) spočíva v tom, že možno ukázať

$$\mathbf{T}_P \vdash ((\forall \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4)(\exists \mathrm{x}_1)\, \varphi(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4) \to \mathrm{Cons}_{\mathbf{T}_P})$$

a potom tvrdenie vyplýva z druhej Gödelovej vety 11.1.

Overenie časti b) je triviálny dôsledok známej Ramseyovej vety, ktorú možno ľahko dokázať v **ZF**:

$$(\forall k, n)\, \omega \longrightarrow (\omega)^k_n.$$

Znak ω označuje spočítateľnú nekonečnú množinu.

Detaily a overenie možno nájsť v práci [HPa] alebo monografii [HPu].[7]

Ďaší príklad nerozhodnuteľnej vety Peanovej aritmetiky uvedieme v časti 18.

13 Diofantické rovnice a diofantické množiny

Vraciame sa do matematiky. Budeme znovu dokazovať vety.

Nech

$$p(x_1, \ldots, x_k) = \sum_{i_1=0}^{n_1} \ldots \sum_{i_k=0}^{n_k} a_{i_1 \ldots i_k} x_1^{i_1} \cdot \ldots \cdot x_k^{i_k}$$

je polynóm s celočíselnými koeficientami, t.j. $a_{i_1 \ldots i_k} \in \mathbb{Z}$. Rovnica

$$p(x_1, \ldots, x_k) = 0 \tag{13.17}$$

kde riešenia $x_1, \ldots, x_k$ sú celé čísla, sa nazýva **diofantická rovnica**.

David Hilbert v svojej prednáške na Medzinárodnom kongrese matematikov v Paríži v roku 1900 sformuloval 23 problémov pre matematiku 20. storočia - pozri napr. [HD]. 10. problém žiada nájsť algoritmus, ktorý pre danú diofantickú rovnicu rozhodne, či táto má riešenie alebo nie. Tento problém bol vyriešený ako posledný v roku 1969. Odpoveď znie: taký algoritmus neexistuje. V ďalšom ukážeme základné myšlienky dôkazu tohoto výsledku.

Najprv ukážeme, že problém riešenia diofantických rovníc sa dá zredukovať na podobnú otázku vyjadrenú pomocou prirodzených čísiel.

Ľahko vidieť, že rovnica (13.17) sa dá ekvivalentne vyjadriť rovnicou

$$q_1(x_1, \ldots, x_k) = q_2(x_1, \ldots, x_k), \tag{13.18}$$

v ktorej polynómy q_1, q_2 majú koeficienty prirodzené čísla.

Nech

$$P(x_1, \ldots, x_k) = \Pi_{j_1, \ldots, j_k} p((-1)^{j_1} x_1, \ldots, (-1)^{j_k} x_k),$$

kde súčin prebieha cez všetky k-tice núl a jednotiek (teda 2^k súčiniteľov). Rovnica $P(x_1, \ldots, x_k) = 0$ má riešenie v prirodzených číslach vtedy a len vtedy, ak rovnica (13.17) má celočíselná riešenie.

[7] V monografii [HPu] je výsledok chybne formulovaný. V označení tejto knihy má byť $x = 1$.

Známa Lagrangeova veta hovorí, že každé prirodzené číslo n možno vyjadriť v tvare $n = z_1^2 + z_2^2 + z_3^2 + z_4^2$, kde z_1, z_2, z_3, z_4 sú celé čísla. Teda rovnica (13.17) má riešenie v prirodzených číslach vtedy a len vtedy, ak rovnica

$$p(z_{11}^2 + z_{12}^2 + z_{13}^2 + z_{14}^2, \ldots, z_{k1}^2 + z_{k2}^2 + z_{k3}^2 + z_{k4}^2) = 0$$

má riešenie v celých číslach $z_{11}, \ldots, z_{k4}$.

Polynóm $\sum_{i=1}^{k}(x_i - r_i)^2$ má jediné riešenie a to k-ticu $[r_1, \ldots, r_k]$.

Sústava l rovníc

$$\begin{aligned} p_1(x_1, \ldots, x_k) &= 0 \\ &\ldots \\ p_l(x_1, \ldots, x_k) &= 0 \end{aligned}$$

má tie isté korene, ako rovnica

$$p_1^2(x_1, \ldots, x_k) + \ldots + p_l^2(x_1, \ldots, x_k) = 0.$$

Odteraz (ak nepovieme inak) premenné označujú prirodzené čísla. Koeficienty polynómu sú spravidla celé čísla.

Množina $A \subseteq \mathbb{N}^k$ sa nazýva **diofantická množina**, ak existuje polynóm (s celočíselnými koeficientami) $p(y_1, \ldots, y_l, x_1, \ldots, x_k)$ taký, že pre všetky prirodzené čísla $x_1, \ldots, x_k$ platí

$$[x_1, \ldots, x_k] \in A \equiv (\exists y_1) \ldots (\exists y_l)\, p(y_1, \ldots, y_l, x_1, \ldots, x_k) = 0. \qquad (13.19)$$

Niekedy budeme žiadať, aby riešenia $y_1, \ldots, y_l$ boli kladné. Dosiahneme to tým, že pridáme diofantickú podmienku

$$(\exists z_1) \ldots (\exists z_l)\, (y_1 = 1 + z_l \wedge \ldots \wedge y_l = 1 + z_l).$$

Funckia $f : A \longrightarrow \mathbb{N}$ sa nazýva **diofantická funkcia**, ak jej graf $\mathrm{G}(f)$ je diofantická množina.

Zrejme každý polynóm p je diofantická funkcia. Totiž

$$[x_1, \ldots, x_k, y] \in \mathrm{G}(p) \equiv p(x_1, \ldots, x_k) - y = 0.$$

Veta 13.1 *Diofantická množina je rekurzívne očíslovateľná a diofantická funkcia je čiastočne rekurzívna.*

Overenie: Zrejme množina A je diofantická práve vtedy, ak existujú polynómy q_1, q_2 s koeficiantami prirodzené čísla také, že

$$[x_1, \ldots, x_k] \in A \equiv (\exists y_1) \ldots (\exists y_l)\; q_1(y_1, \ldots, y_l, x_1, \ldots, x_k) = \\ = q_2(y_1, \ldots, y_l, x_1, \ldots, x_k).$$

Polynómy q_1, q_2 sú primitívne rekurzívne funkcie, teda množina A je rekurzívne očíslovateľná.

Ak funkcia f je diofantická, tak jej graf je rekurzívne očíslovateľná množina a podľa vety 2.4 funkcia f je čiastočne rekurzívna.

q.e.d.

Výroková funkcia $\mathcal{V}$ sa nazýva **diofantická**, ak existuje polynóm (s celočíselnými koeficientami) $p(y_1, \ldots, y_l, x_1, \ldots, x_k)$ taký, že pre všetky prirodzené čísla $x_1, \ldots, x_k$ platí

$$\mathcal{V}(x_1, \ldots, x_k) \equiv (\exists y_1) \ldots (\exists y_l)\, p(y_1, \ldots, y_l, x_1, \ldots, x_k) = 0. \tag{13.20}$$

Teda, množina A je diofantická práve vtedy, keď je diofantická výroková funkcia $[x_1, \ldots, x_k] \in A$. Dôležitejší je tento triviálny dôsledok: funkcia f je diofantická práve vtedy, keď výroková funkcia

$$f(x_1, \ldots, x_k) = x$$

je diofantická. Rovnosť interpretujeme tak, že ak hodnota funkcie $f(x_1, \ldots, x_k)$ nie je definovaná, tak výroková funkcia $f(x_1, \ldots, x_k) = x$ neplatí.

Veta 13.2 *Nech $\mathcal{V}(x_1, \ldots, x_k)$ a $\mathcal{W}(x_1, \ldots, x_k)$ sú diofantické výrokové funkcie, $0 < i < k$. Potom aj výrokové funkcie $\mathcal{V}(x_1, \ldots, x_k) \wedge \mathcal{W}(x_1, \ldots, x_k)$, $\mathcal{V}(x_1, \ldots, x_k) \vee \mathcal{W}(x_1, \ldots, x_k)$ a $(\exists x_1) \ldots (\exists x_i)\, \mathcal{V}(x_1, \ldots, x_k)$ sú diofantické.*

Overenie: Nech p, q sú diofantické polynómy také, že platí

$$\begin{aligned}
\mathcal{V}(x_1, \ldots, x_k) &\equiv (\exists y_1) \ldots (\exists y_l)\, p(y_1, \ldots, y_l, x_1, \ldots, x_k) = 0, \\
\mathcal{W}(x_1, \ldots, x_k) &\equiv (\exists y_1) \ldots (\exists y_l)\, q(y_1, \ldots, y_l, x_1, \ldots, x_k) = 0.
\end{aligned}$$

Potom

$$\begin{aligned}
&\mathcal{V}(x_1, \ldots, x_k) \wedge \mathcal{W}(x_1, \ldots, x_k) \equiv \\
&\qquad (\exists y_1) \ldots (\exists y_l)(\exists z_1) \ldots (\exists z_l)\, p^2(y_1, \ldots, y_l, x_1, \ldots, x_k) + \\
&\qquad\qquad q^2(z_1, \ldots, z_l, x_1, \ldots, x_k) = 0. \\
&\mathcal{V}(x_1, \ldots, x_k) \vee \mathcal{W}(x_1, \ldots, x_k) \equiv \\
&\qquad (\exists y_1) \ldots (\exists y_l)\, p(y_1, \ldots, y_l, x_1, \ldots, x_k) \cdot q(y_1, \ldots, y_l, x_1, \ldots, x_k) = 0. \\
&(\exists x_1) \ldots (\exists x_i) \mathcal{V}(x_1, \ldots, x_k) \equiv \\
&\qquad (\exists y_1) \ldots (\exists y_l)(\exists x_1) \ldots (\exists x_i)\, p(y_1, \ldots, y_l, x_1, \ldots, x_k) = 0.
\end{aligned}$$

q.e.d.

Použitím tejto vety a vety 4.1 možno "takmer" ukázať, že každá rekurzívne očíslovateľná množina je diofantická. To "takmer" spočíva v tom, že potrebujeme ukázať, že výroková funkcia $(\forall k < n)\, \mathcal{V}$ je diofantické za predpokladu, že je taká $\mathcal{V}$. K tomu zase stačí ukázať, že funkcia n^k je diofantická. Všetko je takmer triviálne, ale posledné odolávalo matematikom aspoň dve desaťročia. Jurij Matijasievič v [Ma] ukázal, že n^k je diofantická. V ďalšom podáme dôkaz tohoto tvrdenia založený na modifikácii podľa M. Davisa [DM2]

Z toho potom vyplýva riešenie 10. Hilbertovho problému.

Veta 13.3 *Ak každá rekurzívne očíslovateľná množina je diofantická, tak neexistuje algoritmus, ktorý pre danú diofantickú rovnicu rozhodne, či táto má riešenie alebo nie.*

Overenie: Vieme, že existuje rekurzívne očíslovateľná množina $K \subseteq \mathbb{N}$, ktorá nie je rekurzívna, napríklad množina z vety o probléme zastavenia sa Turingovho stroja

$$K = \{x \in \mathbb{N}; (\exists y)\, \mathrm{T}_1(x, y, x)\}.$$

Množina K je diofantická, teda existuje polynóm s celočíselnými koeficientmi p taký, že

$$x \in K \equiv (\exists y_1) \ldots (\exists y_l)\, p(y_1, \ldots, y_l, x) = 0. \tag{13.21}$$

Pre každé pevné prirodzené číslo x

$$p(y_1, \ldots, y_l, x) = 0$$

máme diofantickú rovnicu s premennými $y_1, \ldots, y_l$. Keby existoval algoritmus, ktorý rozhodne, či pre dané x táto rovnica má riešenie alebo nie, tak tento algoritmus podľa (13.21) rozhodne, či $x \in K$ alebo nie. Taký algoritmus však neexistuje, lebo množina K nie je rekurzívna.

q.e.d.

Medzi diofantickými množinami a diofantickými funkciami musí byť rovnaký vzťah, ako medzi rekurzívne očíslovateľnými množinami a čiastočne rekurzívnymi funkciami.

Veta 13.4 *Množina $A \subseteq \mathbb{N}$ je diofantická vtedy a len vtedy, keď existuje polynóm p taký, že A je množina všetkých jeho nezáporných hodnôt, t.j.*

$$A = \mathcal{H}(p) \cap \mathbb{N}.$$

Overenie: Nech $A = \mathcal{H}(p) \cap \mathbb{N}$. Potom

$$y \in A \equiv (\exists x_1) \ldots (\exists x_k)\, p(x_1, \ldots, x_k) - y = 0$$

a teda množina A je diofantická.

Nech naopak, množina $A \subseteq \mathbb{N}$ je diofantická a platí

$$x \in A \equiv (\exists y_1) \ldots (\exists y_l)\, p(y_1, \ldots, y_l, x) = 0.$$

Potom množina A je množina nezáporných hodnôt polynómu

$$x \cdot (1 - 2 \cdot p^2(y_1, \ldots, y_l, x)).$$

q.e.d.

14 Pellova rovnica

Cieľom tejto časti je ukázať tvrdenie 14.1. Mnohé technické detaily z priestorových dôvodov vynecháme, ale čitateľ ich môže nájsť v práci M. Davisa [DM2] alebo s určitou námahou rekonštruovať sám.

Veta 14.1 *Funkcia $m = n^k$ je diofantická.*

Historicky boli známe všetky výsledky ďalších častí skôr, ako sa podarilo ukázať, že funkcia exponenciála je diofantická. V šesťdesiatych rokoch 20. storočia matematici už vedeli, že stačí nájsť jednu diofantickú funckiu, ktorá rastie exponenciaálne. Na prekvapenie všetkých mladý ruský matematik z Petrohradu[8], Jurij Matijasevič v roku 1969 ukázal, že takou funkciou je dobre známa Fibonacciova postupnosť. Potom matematici našli ďalšie podobné postupnosti. Jednou z nich je postupnosť riešení tzv. Pellovej rovnice[9]. Prezentujeme základné výsledky.

Rovnica

$$x^2 - dy^2 = 1, \text{ kde } d = a^2 - 1, \quad a > 1 \tag{14.22}$$

s podmienkou, že riešenia x, y sú prirodzené čísla, sa nazýva **Pellova rovnica**.

Ak by sme vzali $a = 1$ dostaneme triviálnu rovnicu. Pre $a = 0$ však dostaneme rovnicu $x^2 + y^2 = 1$. Jej riešenia (nie nutne celočíselné) vieme vyjadriť pomocou funkcií sínus a kosínus. Všimnite si, že niektoré výsledky o riešeniach Pellovej rovnice budú pripomínať známe vlastnosti funkcií sínus a kosínus. Iné výsledky budú pripomínať známe vlastnosti Fibonacciovej postupnosti. Nie je to náhoda, lebo Pellova rovnica s Fibonacciovou postupnosťou súvisí.

Dvojice čísiel $x = 1$, $y = 0$ a $x = a$, $y = 1$ sú zrejme riešenia Pellovej rovnice.

Lema 14.2 *Neexistujú celé čísla x, y také, že sú riešením rovnice* (14.22) *a platí*

$$1 < x + y\sqrt{d} < a + \sqrt{d}. \tag{14.23}$$

Dôkaz: Ak x, y sú riešenia rovnice (14.22), tak

$$(x + y\sqrt{d})(x - y\sqrt{d}) = 1 = (a + \sqrt{d})(a - \sqrt{d}). \tag{14.24}$$

Keby platili nerovnosti (14.23), tak z uvedenej rovnosti dostaneme

$$-1 < -x + y\sqrt{d} < -a + \sqrt{d}.$$

Sčítaním tejto nerovnosti a nerovnosti (14.23) dostávame $0 < 2y\sqrt{d} < 2\sqrt{d}$, t.j. $0 < y < 1$, čo nie je možné.

q.e.d.

[8] Vtedy to bol Leningrad.

[9] Problém riešenia rovnice (14.22) položil Pierre de Fermat v roku 1657. Riešenia tejto rovnice našiel - bez dôkazu - Lord Brouncker. V roku 1958 úplnú odpoveď dal J. Wallis. Leonard Euler omylom rovnicu nazval Pellova rovnica a tento termín sa v literatúre ustálil.

Lema 14.3 *Nech x, y a x', y' sú celočíselné riešenia rovnice* (14.22). *Nech*

$$x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d}).$$

Potom

$$x'' - y''\sqrt{d} = (x - y\sqrt{d})(x' - y'\sqrt{d}) \tag{14.25}$$

a x'', y'' je riešenie (14.22).

Dôkaz: Zrejme

$$x'' = xx' + dyy', \qquad y'' = xy' + x'y. \tag{14.26}$$

Z toho bezprostredne vyplýva rovnosť (14.25) a vynásobením dostávame tvrdenie.

q.e.d.

Definícia: Nech $x_n(a)$, $y_n(a)$ sú prirodzené čísla, pre ktoré platí

$$x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n.$$

Ak číslo a je zrejmé z kontextu, tak ho nepíšeme.

Veta 14.4 *Pre každé prirodzené číslo n dvojica $x_n(a)$, $y_n(a)$ je riešením Pellovej rovnice. Naopak, ak x, y je riešenie Pellovej rovnice, tak existuje také prirodzené číslo n, že $x = x_n(a)$ a $y = y_n(a)$.*

Dôkaz: Použitím lemy 14.3 matematickou indukciou dostaneme, že x_n, y_n sú riešenia Pellovej rovnice, špeciálne

$$(x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = 1.$$

Nech x, y je riešenie Pellovej rovnice. Postupnosť $(a + \sqrt{d})^n$ je rastúca a neohraničená, teda existuje také n, že platí

$$(a + \sqrt{d})^n \le x + y\sqrt{d} < (a + \sqrt{d})^{n+1}.$$

Ak platí rovnosť, sme hotoví. Nech teda rovnosť neplatí, t.j.

$$x_n + y_n\sqrt{d} < x + y\sqrt{d} < (x_n + y_n\sqrt{d})(a + \sqrt{d}).$$

Vynásobením kladným číslom $x_n - y_n\sqrt{d}$ dostávame

$$1 < (x + y\sqrt{d})(x_n + y_n\sqrt{d}) < a + \sqrt{d},$$

čo je v spore s lemou 14.2 a 14.3.

q.e.d.

V ďalšom budeme bez komentára využívať rovnosti

$$x_0(a) = 1, \quad y_0(a) = 0, \quad x_1(a) = a, \quad y_1(a) = 1.$$

Lema 14.5 *Pre každé $m \leq n$ platí*

$$x_{n\pm m} = x_n x_m \pm d y_n y_m, \qquad y_{n\pm m} = y_n x_m \pm y_m x_n, \tag{14.27}$$

$$x_{n+1} = 2a x_n - x_{n-1}, \qquad y_{n+1} = 2a y_n - y_{n-1}. \tag{14.28}$$

Dôkaz: Rovnosti (14.27) pre $n+m$ vyplývajú priamo z definície:

$$x_{n+m} + y_{n+m}\sqrt{d} = (a+\sqrt{d})^{n+m} = (a+\sqrt{d})^n \cdot (a+\sqrt{d})^m =$$
$$(x_n + y_n\sqrt{d})(x_m + y_m\sqrt{d}) = (x_n x_m + y_n y_m d) + (y_n x_m + y_m x_n)\sqrt{d}.$$

Z rovnosti (14.24) vyplýva

$$x_{n-m} + y_{n-m}\sqrt{d} = (x_m + y_m\sqrt{d}) \cdot (x_n - y_n\sqrt{d})$$

a odtiaľ dostávame rovnosť pre $n-m$.

Pre $m = 1$ dostaneme

$$x_{n+1} = x_n a + d y_n, \quad x_{n-1} = x_n a - d y_n. \tag{14.29}$$

Sčítaním dostaneme prvú rovnosť (14.28). Podobne pre y_n dostaneme tvrdenie z rovníc

$$y_{n+1} = a y_n + x_n, \quad y_{n-1} = a y_n - x_n. \tag{14.30}$$

q.e.d.

Zhrnieme niektoré vlastnosti riešení Pellovej rovnice.

Veta 14.6 *Pre každé prirodzené číslo n platí:*

a) *čísla x_n a y_n sú nesúdeliteľné;*

b) *y_n je párne vtedy a len vtedy, keď n je párne;*

c) *$x_n < x_{n+1}$ a $y_n < y_{n+1}$;*

d) *$a^n \leq x_n(a) \leq (2a)^n$, $y_n \geq n$;*

e) *$y_n(a) \equiv n \bmod a-1$.*

Dôkaz: Tvrdenie a) vyplýva bezprostredne z Pellovej rovnice.

Tvrdenie b) vyplýva matematickou indukciou z druhej rovnice (14.28).

Obidve nerovnosti c) vyplývajú z rovností 14.29 a 14.30. Indukciou z týchto rovností možno získať aj nerovnosti d).

Pre $n = 0, 1$ kongruencia e) evidentne platí. Podľa druhej rovnosti (14.28) dostaneme tvrdenie matematickou indukciou.

q.e.d.

Lema 14.7 $\quad x_n(a) - y_n(a)(a-y) \equiv y^n \bmod 2ay - y^2 - 1.$

Dôkaz: Tvrdenie lemy možno dokázať matematickou indukciou. Pre $n = 0, 1$ dostaneme tvrdenie priamo dosadením. Predpokladajme, že lema platí pre n. Použitím rovností (14.28) postupne dostávame modulo $2ay - y^2 - 1$

$$\begin{aligned} x_{n+1} - y_{n+1}(a-y) &= 2a(x_n - y_n(a-y)) - (x_{n-1} - y_{n-1}(a-y)) \equiv \\ &\equiv 2ay^n - y^{n-1} = y^{n-1}(2ay - 1) \equiv y^{n+1}. \end{aligned}$$

q.e.d.

Lema 14.8 *$y_n | y_m$ vtedy a len vtedy keď $n|m$.*

Dôkaz: Ak $n|m$ tak $m = kn$. Indukciou cez k ukážeme, že $y_n | y_{kn}$. Pre $k = 1$ je to triviálne a indukčný krok vyplýva z rovnosti

$$y_{n(m+1)} = x_n y_{nm} + x_{nm} y_n.$$

Nech teraz $y_n | y_m$ ale $n \nmid m$. Potom $m = kn + r$, $0 < r < n$. Podľa (14.27) máme

$$y_m = x_r y_{kn} + y_r x_{kn}.$$

Keďže x_{kn}, y_{kn} sú nesúdeliteľné, tak aj x_{kn}, y_n sú nesúdeliteľné. Teda $y_n | y_r$. Ale $0 < y_r < y_n$, čo je spor.

q.e.d.

Lema 14.9 *Ak $y_n^2 | y_m$ tak $y_n | m$.*

Dôkaz: Podľa lemy 14.8 máme $n|m$. Teda $m = kn$ pre nejaké k. Z definície čísiel x_n, y_n máme

$$x_{kn} + y_{kn}\sqrt{d} = (x_n + y_n\sqrt{d})^k = \sum_{i=0}^{k} \binom{k}{i} x_n^{k-i} y_n^i d^{i/2}.$$

Potom

$$y_{kn} = \sum_{i>0, i \text{ odd}}^{k} \binom{k}{i} x_n^{k-i} y_n^i d^{(i-1)/2}.$$

Všetky členy s $i > 1$ sú $\equiv 0 \bmod (y_n)^3$. Teda

$$y_{kn} \equiv k x_n^{k-1} y_n \bmod (y_n)^3. \tag{14.31}$$

Potom $(y_n)^2 | k x_n^{k-1} y_n$ a teda $y_n | k x_n$. Keďže x_n a y_n sú nesúdeliteľné, tak $y_n | k$ a teda aj $y_n | m$.

q.e.d.

Lema 14.10 *$y_n^2 | y_{n y_n}$.*

Dôkaz: V kongruencii (14.31) polož $k = y_n$.

q.e.d.

Lema 14.11 *Ak $a \equiv b \bmod c$, tak pre každé n platí*

$$x_n(a) \equiv x_n(b), \quad y_n(a) \equiv y_n(b) \bmod c.$$

Dôkaz: Pre $n = 0, 1$ kongruencie sú fakticky rovnosťami. Pre $n > 1$ dôkaz ide matemamtickou indukciou použijúc (14.28).

q.e.d.

Lema 14.12 *Nech $x_i \equiv x_j \bmod x_n$, $i, j \leq 2n$, $n > 0$. Potom $i = j$ okrem prípadu $a = 2$, $n = 1$, $i = 0$ a $j = 2$.*

Dôkaz: Viacnásobnýn použitím rovnosti (14.27) (začni $2n \pm j = n + (n \pm j)$) dostaneme

$$x_{2n \pm j} \equiv -x_j \bmod x_n \tag{14.32}$$

a teda

$$x_{4n \pm j} \equiv x_j \bmod x_n. \tag{14.33}$$

Predpokladajme napríklad, že x_n je párne. Označíme $q = x_n/2$. Podľa (14.29) je $x_{n-1} \leq x_n/2 = q$.Keby bolo $x_{n-1} = q$, tak podľa (14.27) je $a = 2$, $y_{n-1} = 0$ a teda $n = 1$. Tento prípad sme v tvrdení lemy vylúčili. Teda môžeme predpokladať, že $x_{n-1} < q$.

Čísla

$$-q + 1, -q + 2, \ldots, -1, 0, 1 \ldots, q - 1, q$$

sú všetky možné zvyšky modulo x_n a teda žiadne z nich nie sú kongruentné modulo x_n. Naviac, podľa (14.32) čísla

$$x_{n+1}, x_{n+2}, \ldots, x_{2n-1}, x_{2n}$$

sú postupne kongruentné modulo x_n číslam

$$-x_{n-1}, -x_{n-1}, \ldots, -x_1, -x_0.$$

Teda čísla

$$-q < -x_{n-1} < -x_{n-2} < \ldots < -x_0 = -1 < 1 = x_0 < \ldots x_{n-1} < q$$

sú navzájom nekongruentné modulo x_n. Teda $i = j$.

Podobne postupujeme v prípade keď x_n je nepárne.

q.e.d.

Lema 14.13 *Ak $0 < i \leq n$ a $x_j \equiv x_i \bmod x_n$, tak $j \equiv i$ alebo $j \equiv -i \bmod 4n$.*

Dôkaz: Nech $j = 4nq + k$, $0 \leq k < 4n$. Podľa (14.33) platí $x_j \equiv x_k \bmod x_n$. Ak $k \leq 2n$ tak podľa lemy 14.12 je $i = j$.

Predpokladajme teda, že $2n < k$. Potom $4n - k < 2n$ a $x_k \equiv x_{4n-k} \bmod x_n$. Teda podľa lemy 14.12 máme $i = 4n - k$.

q.e.d.

Veta 14.14 *Pre dané prirodzené čísla $x, k, a > 1$ platí $x_k(a) = x$ vtedy a len vtedy, keď existujú kladné prirodzené čísla $b, c, d, e, p, q, r, s, t, y, u, v$ také, že*

$$\begin{array}{lll} x^2 - (a^2-1)y^2 = 1, & u^2 - (a^2-1)v^2 = 1, & s^2 - (b^2-1)t^2 = 1, \quad \text{(a)} \\ v = ry^2, & b = 1 + 4py, & b = a + qu, \quad \text{(b)} \\ s = x + cu, & t = k + 4(d-1)y, & y = k + e - 1. \quad \text{(c)} \end{array}$$

Teda funkcia $x_n(a)$ je diofantická.

Dôkaz: Nech $x = x_k(a)$. Postupne definujeme požadované hodnoty kladných prirodzených čísiel. Nech $y = y_k(a)$, $m = 2ky_k(a)$, $u = x_m(a)$, $v = y_m(a)$. Potom platia prvé dve rovnosti (a). Podľa lem 14.10 a 14.8 máme $y^2|v$ a teda existuje r spĺňajúce prvú rovnosť (b). Podľa vety 14.6, b), číslo v je párne a teda u je nepárne. Potom možno ukázať, že u a $4yv$ sú nesúdeliteľné. Naozaj, keby prvočíslo p delilo obidve uvedené čísla, tak $p|y$ lebo u je nepárne a čísla u, v sú nesúdeliteľné. Potom $p|v$ lebo $y|v$. To však nie je možné. Podľa čínskej vety o zvyškoch 3.1 existuje $b > 4y$, $b > u$ také, že

$$b \equiv 1 \bmod 4y, \quad b \equiv a \bmod u.$$

Teda existujú kladné prirodzené čísla spĺňajúce druhú a tretiu rovnosť (b).

Naopak, nech $b, c, d, e, p, q, r, s, t, y, u, v$ sú kladné prirodzené čísla spĺňajúce rovnosti (a) – (c). Podľa druhej a tretej rovnosti (b) máme $1 < a < b$. Z rovností (a) vyplýva, že existujú kladné čísla i, j, n také, že

$$x = x_i(a), \quad y = y_i(a), \quad u = x_n(a), \quad v = y_n(a), \quad s = x_j(b), \quad t = y_j(b).$$

Podľa prvej rovnosti (b) je $y \leq v$ a teda aj $i \leq n$. Tretia rovnosť (b) a prvá rovnosť (c) dávajú kongruencie $a \equiv b$ a $x_i(a) \equiv x_j(b)$ modulo $x_n(a)$. Podľa lemy 14.11 potom $x_j(a) \equiv x_j(b)$ a teda $x_i(a) \equiv x_j(a)$ všetko modulo $x_n(a)$. Takže podľa lemy 14.13

$$j \equiv \pm i \bmod 4n. \tag{14.34}$$

Z prvej rovnosti (b) pomocou lemy 14.9 dostávame $y_i(a)|n$. Spolu s (14.34) máme

$$j \equiv \pm i \bmod 4y_i(a). \tag{14.35}$$

Podobne, druhá rovnosť (b) dáva $4y_i(a)|(b-1)$ a podľa vety 14.6, e) potom

$$y_j(b) \equiv j \bmod 4y_i(a). \tag{14.36}$$

Z druhej rovnosti (c) dostaneme

$$y_j(b) \equiv k \bmod 4y_i(a). \tag{14.37}$$

Kongruencie (14.35) – (14.37) dávajú

$$k \equiv \pm i \bmod 4y_i(a). \tag{14.38}$$

Z tretej rovnosti (c) máme $k \leq y_i(a)$.

Čísla

$$-2y+1, -2y+2, \ldots, -1, 0, 1, \ldots, 2y$$

sú navzájom rôznymi zvyškami pri delení číslom $4y = 4y_i(a)$. Keďž aj $i \leq y_i(a)$, tak z kongruencie (14.38) dostávame $k = i$. Potom $x = x_i(a) = x_k(a)$.

q.e.d.

Veta 14.15 *$m = n^k$ vtedy a len vtedy, keď existujú kladné prirodzené čísla $a, b, c, d, e, f, g, h, k, l, p, q, r, s, t, x, y, u, v, w, z$ také, že platia rovnosti* (a) – (c) *a rovnosti*

$$(x - y(a-n) - m)^2 = (f-1)^2(2an - n^2 - 1)^2, \quad m + g = 2an - n^2 - 1, \quad \text{(d)}$$
$$a^2 - (w^2-1)(w-1)^2 z^2 = 1, \quad w = n + h, \quad w = k + l. \quad \text{(e)}$$

Teda funkcia n^k je diofantická.

Dôkaz: Nech platia rovnosti (a) – (e). Z rovností (e) vyplýva, že $a > 1$. Potom podľa vety 14.14 je $x = x_k(a)$ a $y = y_k(a)$. Z prvej rovnosti (d) vyplýva

$$x_k(a) - y_k(a)(a-n) \equiv m \bmod 2an - n^2 - 1.$$

Spolu s lemou 14.7 dostávame

$$m \equiv n^k \bmod 2an - n^2 - 1. \tag{14.39}$$

Z druhej rovnosti (d) máme $m < 2an - n^2 - 1$. Podľa druhej a tretej rovnosti (e) je $k, n < w$. Podľa prvej rovnosti (e) existuje j také, že $a = x_j(w), (w-1)z = y_j(w)$. Podľa vety 14.6, e) je $j \equiv 0 \bmod w-1$ a teda $w - 1 \leq j$. Použijúc vetu 14.6 d) dostaneme

$$n^k < w^{w-1} \leq w^j \leq x_j(w) = a.$$

Odtiaľ jednoduchým výpočtom dostaneme $n^k < 2an - n^2 - 1$. Keďže obidve čísla m a n^k sú menšie ako $2an - n^2 - 1$, tak na základe kongruencie (14.39) sa musia rovnať.

Naopak, ak $m = n^k$ tak stačí zvoliť ľubovoľné číslo $w > n, k$ a položiť $a = x_{w-1}(w)$. Ostatné čísla vyhovujúce rovnostiam (a) – (e) možno ľahko nájsť.

q.e.d.

Veta 14.1 bezprostredne vypýva z vety 14.15.

15 Niektoré diofantické funkcie

Ukážeme, že niektoré jednoduché funkcie a výrokové funkcie sú diofantické. Postupujeme podobne ako v teórii vypočítateľnosti, keď sme ukazovali primitívnu rekurzívnosť niektorých funkcií a výrokových funkcií. Podstatne využijeme skutočnosť, že exponenciálna n^k je diofantická.

Výroková funkcia na ľavej strane je vždy ekvivalentná diofantickej výrokovej funkcii na pravej strane:

$n \mid m$	$(\exists k)\, n \cdot k = m,$
$n < m$	$(\exists k)\, n + k + 1 = m,$
$n \leq m$	$(\exists k)\, n + k = m,$
$\mathrm{rm}(n, m) = k$	$(k < m \wedge (\exists l)\, (lm + k = n)) \vee (m = 0 \wedge k = 0),$
$[n/m] = k$	$(km \leq n \wedge (k + 1) \cdot m > n) \vee (m = 0 \wedge k = 0),$
$n \equiv m \bmod k$	$\mathrm{rm}(n, k) = \mathrm{rm}(m, k),$
$n \div m = k$	$(m \leq n \wedge m + k = n) \vee (n < m \wedge k = 0).$

Veta 15.1 *Nasledujúce funkcie sú diofantické:*

1) $f(n, k) = \binom{n}{k}$,

2) $g(n) = n!$,

3) $h(n, m, k) = \Pi_{i=0}^{k}(n + mi)$.

Dôkaz: Dôkaz je založený na vhodných teoreticko-číselných vzťahoch. Ukážeme napríklad diofantičnosť funkcie f.

Ak $0 < k \leq n$, $u > 2^n$, tak

$$(u + 1)^n / u^k = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} + \sum_{i=k}^{n} \binom{n}{i} u^{i-k}.$$

Ľahko sa zistí, že prvý sčítanec je menší ako 1 a teda

$$[(u + 1)^n / u^k] = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}.$$

Odtiaľ ľahko dostaneme

$$[(u + 1)^n / u^k] \equiv \binom{n}{k} \bmod u.$$

Teda

$$z = \binom{n}{k} \equiv (\exists u, v, w)\, (v = 2^u \wedge v < u \wedge w = [(u + 1)^n / u^k] \wedge \\ \wedge z \equiv w \bmod u \wedge z < u).$$

Dôkaz diofantičnosti funkcie g je podobný a je založený na na identite

$$n! = \left[m^n / \binom{m}{n} \right] \text{ pre } m > (2n)^{n+1}.$$

Dôkaz diofantičnosti funkcie h je založený na kongruencii

$$\Pi_{k=1}^{n}(a + bk) \equiv b^n n! \binom{q + n}{n} \bmod M$$

pre ľubovoľné čísla a, b, q také, že $a \equiv bq \bmod M$.

q.e.d.

Vetu využijeme k tomu, aby sme ukázali, že vlastnosť "byť prvočíslom" je diofantická. Je to typický trik, ktorý sa v danej problematike využíva. Stačí si uvedomiť, že $p > 1$ je prvočíslo práve vtedy, ak je nesúdeliteľné s číslom $(p-1)!$. To je ale ekvivalentné

$$(\exists u, v)\, u(p-1)! + vp = 1.$$

Ak čitateľovi vadí, že u, v teraz označujú celé čísla, tak rovnicu môže ekvivalentne prepísať pomocou trikov uzedených v časti 13 takto

$$(\exists u, v)\, (u(p-1)! + vp = 1 \vee u(p-1)! = 1 + vp \vee 1 + u(p-1)! = vp.$$

Teraz už premenné u, v označujú prirodzené čísla.

16 Veta o ohraničenom kvantifikátore

Celá naša snaha smerovala k tomu, aby sme mohli dokázať dôležitý technický výsledok.

Veta 16.1 *Ak $\mathcal{V}(x_1, \ldots, x_n, y)$ je diofantická výroková funkcia, tak výroková funkcia $(\forall y \leq z)\, \mathcal{V}(x_1, \ldots, x_n, y)$ je diofantická.*

Overenie je založené na dvoch pomocných tvrdeniach.

Lema 16.2

$$(\forall z)_{z \leq y} (\exists y_1) \ldots (\exists y_l)\, p(y, z, y_1, \ldots, y_l, x_1, \ldots, x_k) = 0$$

vtedy a len vtedy, keď

$$(\exists u)(\forall z)_{z \leq y} (\exists y_1)_{y_1 \leq u} \ldots (\exists y_l)_{y_l \leq u}\, p(y, z, y_1, \ldots, y_l, x_1, \ldots, x_k) = 0$$

Overenie: Z dolného tvrdenia triviálne vyplýva horné. Naopak, ak platí ĥorné tvrdenie, tak pre každé $z \leq y$ existujú čísla $y_{1,z}, \ldots, y_{l,z}$ pre ktoré

$$p(y, z, y_{1,z}, \ldots, y_{l,z}, x_1, \ldots, x_k) = 0.$$

Stačí vziať $u = \max\{y_{i,z}; i = 1, \ldots, l, z \leq y\}$.

q.e.d.

Lema 16.3 *Nech q je polynóm pre ktorý platí*

a) $u < q(y, u, x_1, \ldots, x_k)$ *pre každé* $y, u, x_1, \ldots, x_k$,

b) $y < q(y, u, x_1, \ldots, x_k)$ *pre každé* $y, u, x_1, \ldots, x_k$,

c) $|p(y, z, y_1, \ldots, y_l, x_1, \ldots, x_k)| < q(y, u, x_1, \ldots, x_k)$ *pre každé* $y, u, z \leq y$, $y_1 \leq u, \ldots, y_l \leq u, x_1, \ldots, x_k$.

Potom

$$(\forall z)_{z\le y}(\exists y_1)_{y_1\le u}\dots(\exists y_l)_{y_l\le u}\, p(y,z,y_1,\dots,y_l,x_1,\dots,x_k)=0$$

vtedy a len vtedy, keď

$$\begin{gathered}(\exists c,t,a_1,\dots,a_l)\,[1+ct=\Pi_{i=1}^{y}(1+it)\wedge t=q(y,u,x_1,\dots,x_k)!\wedge\\ 1+ct\mid\Pi_{j=1}^{u}(a_1-j)\wedge\cdot\wedge 1+ct\mid\Pi_{j=1}^{u}(a_l-j)\wedge\\ p(y,c,a_1,\dots,a_l,x_1,\dots,x_k)\equiv 0 \bmod 1+ct.\end{gathered}$$

Dôkaz: Ukážeme implikáciu zdola nahor.

Nech $c,t,a_1,\dots,a_l$ sú také čísla, že platí dolná rovnica. Pre každé $z=1,\dots,y$ nech p_z je prvočíselný deliteľ čísla $1+zt$. Nech $y_i^{(z)}$ je zvyšok čísla a_i pri delení číslom p_z. Z predpokladov vyplýva,že $p_z\mid\Pi_{j=1}^{u}(a_i-j)$ a teda $p_k\mid(a_i-j)$ pre nejaké $j\le u$, $j>0$. Teda

$$j\equiv a_i\equiv y_i^{(z)} \bmod p_z. \tag{16.40}$$

Z podmienky pre t vyplýva, že každý deliteľ $1+kt$ musí byť $>u$. Teda $y_i^{(z)}=j$ a teda $y_i^{(z)}\le u$.

Zrejme $p_z\mid(z+zct)$ a $p_z\mid(c+zct)$, teda $p_z\mid(z-c)$. Pomocou (16.40) dostaneme

$$p(y,z,y_1^{(z)},\dots,y_l^{(z)},x_1,\dots,x_k)\equiv p(y,c,a_1,\dots,a_l,x_1,\dots,x_k) \bmod p_z$$

a z poslednej podmienky

$$p(y,z,y_1^{(z)},\dots,y_l^{(z)},x_1,\dots,x_k)\equiv 0 \bmod p_z.$$

Ale

$$|p(y,z,y_1^{(z)},\dots,y_l^{(z)},x_1,\dots,x_k)|\le q(y,u,x_1,\dots,x_k)<p_z$$

a teda

$$p(y,z,y_1^{(z)},\dots,y_l^{(z)},x_1,\dots,x_k)=0.$$

q.e.d.

Dôkaz vety 16.1*:* Na základe lem 16.2 a 16.3 stačí uk azať, že existuje polynóm q, ktorý vyhovuje podmienkam a) – c) lemy 16.3.

Nech

$$p(y,k,y_1^{(k)},\dots,y_l^{(k)},x_1,\dots,x_k)=\sum_{r=0}^{m}B_r,$$

kde

$$B_r=cy^{\alpha}k^{\beta}x_1^{\delta_1}\cdot\ldots\cdot x_k^{\delta_k}y_1^{\gamma_1}\cdot\ldots\cdot y_l^{\gamma_l}.$$

Stačí položiť

$$q(y,u,x_1,\dots,x_k)=\sum_{r=0}^{m}A_r,$$

kde

$$A_r = |c| y^{\alpha+\beta} x_1^{\delta_1} \cdot \ldots \cdot x_k^{\delta_k} u^{\gamma_1+\ldots\gamma_l}.$$

q.e.d.

17 Čiastočne rekurzívna funkcia je diofantická

Cieľom tejto časti je dokázať tvrdenie uvedené v nadpise, teda

Veta 17.1 *Každá čiastočne rekurzívna funkcia je diofantická.*

Overenie: Ľahko sa overí, že každá zo zoznamu funkcií (4.3) je diofantická.

Predpokladajme, že funkcie f, f_1, ... , f_n sú diofantické a funkcia h vznikla z funkcií f, $f_1, \ldots, f_n$ substitúciou, teda

$$h(x_1, \ldots, x_k) = f(f_1(x_1, \ldots, x_k), \ldots, f_n(x_1, \ldots, x_k)).$$

Potom platí

$$\begin{aligned} h(x_1, \ldots, x_k) = x \equiv \\ (\exists y_1) \ldots (\exists y_n)\, (f_1(x_1, \ldots, x_k) = y_1 \wedge \ldots \\ \ldots \wedge f_n(x_1, \ldots, x_k) = y_n \wedge f(x_1, \ldots, x_n) = x). \end{aligned}$$

Podľa vety 13.2 výroková funkcia $h(x_1, \ldots, x_k) = x$ je diofantická.

Nech funkcia h vznikla z funkcie f minimalizáciou, teda

$$h(x_1, \ldots, x_n) = (\min y)\, f(x_1, \ldots, x_n, y) = 0.$$

Potom platí

$$\begin{aligned} h(x_1, \ldots, x_n) = y \equiv \\ (f(x_1, \ldots, x_n, y) = 0 \wedge (\forall z < y)(\exists u)\, (u \neq 0 \wedge f(x_1, \ldots, x_n, z) = u)). \end{aligned}$$

Podľa viet 13.2 a 16.1 výroková funkcia $h(x_1, \ldots, x_n) = y$ je diofantická.

q.e.d.

Dôsledok 17.2 *Množina $A \subseteq \mathbb{N}^k$ je rekurzívne očíslovateľná vtedy a len vtedy, keď je diofantická.*

18 10. Hilbertov problém a iné dôsledky

Na základe vety 13.3 a dôsledku 17.2 dostávame

Veta 18.1 *Neexistuje algoritmus, ktorý pre danú diofantickú rovnicu rozhodne, či táto má riešenie alebo nie.*

Vieme, že množina prvočísiel je rekurzívna. Teda je diofantická a podľa vety 13.4 existuje polynóm taký, že táto množina je množinou nezáporných hodnôt tohoto polynómu. Teda

Veta 18.2 *Existuje polynóm s celočíselnými koeficientami p taký, že prirodzené číslo n je prvočíslo vtedy a, že len vtedy, keď n je hodnota polynómu p.*

Samozrejme zaujíma nás čo najlepší taký polynóm, t.j. najmenšieho možného stupňa a s najmenším možným počtom premenných. Vieme, že existuje polynóm s uvedenou vlastnosťou, ktorý závisí od 10 premenných. Jedna z možností nájsť "čo najlepší" polynóm je založená na tom, že nájdeme jednoduché diofantické vyjadrenie pojmu prvočísla.

Veta 18.3 *Existuje univerzálna diofantická rovnica, t.j existuje diofantický polynóm q taký, že pre každú diofantickú množinu $A \subseteq \mathbb{N}$ existuje prirodzené číslo e také*

$$x \in A \equiv (\exists y_1) \ldots (\exists y_k)\, q(e, x, y_1, \ldots, y_k) = 0.$$

Dôkaz: Výroková funkcia $(\exists y)\, \mathrm{T}_1(e, y, x)$ je diofantická a pre každú rekurzívne očíslovateľnú a teda aj pre každú diofantickú množinu $A \subseteq \mathbb{N}$ existuje e také, že $x \in A \equiv (\exists y)\, \mathrm{T}_1(e, y, x)$. Stačí vziať polynóm q pre ktorý platí

$$(\exists y)\, \mathrm{T}_1(e, y, x) \equiv (\exists y_1) \ldots (\exists y_k)\, q(e, x, y_1, \ldots, y_k) = 0.$$

q.e.d.

Vrátime sa do metamatematiky. Ak $p(x_1, \ldots, x_k)$ je polynóm s koeficientami prirodzené čísla, tak term, ktorý označuje tento polynóm v jazyku aritmetiky označíme $\Delta(p)(\mathrm{x}_1, \ldots, \mathrm{x}_k)$. Tento term dostaneme tak, že každý koeficient m polynómu p nahradíme termom Δ_m, každú premennú x_i polynómu p nahradíme formálnou premennou x_i, a operácie $+, \cdot$ nahradíme ich názvami (funkčnými symbolmi) $+, \cdot$.

Tvrdenie 18.1 *Pre každú neprotirečivú teóriu $\mathbf{T}$ s rekurzívnou výrokovou funkciou $Axiom_{\mathbf{T}}$ existujú polynómy p_1, p_2 s kladnými koeficientami také, že diofantická rovnica*

$$p_1(x_1, \ldots, x_k) = p_2(x_1, \ldots, x_k) \tag{18.41}$$

nemá riešenie v prirodzených číslach, ale

$$\mathbf{T} \nvdash \neg(\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) = \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k).$$

Overenie: Využitím bežných techník kódovania ľahko možno zostrojiť očíslovanie všetkých diofantických rovníc tvaru[10] (18.41) tak, aby platilo:

a) množina D všetkých čísiel takýchto rovníc je rekurzívna,

b) výroková funkcia "rovnica s číslom n má riešenie v prirodzených číslach" je rekurzívne očíslovateľná,

[10] Uvedomme si, že každá diofanická rovnica sa dá ekvivalentne vyjadriť v tomto tvare.

c) funkcia F, ktorá každému číslu $n \in D$ rovnice (18.41) priradí Gödelove číslo uzavretej formuly

$$\neg(\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k)$$

je rekurzívna.

Definujeme dve množiny. M je množina všetkých tých čísiel $n \in D$, pre ktoré rovnica (18.41) má riešenie v prirodzených číslach. N je množina všetkých tých čísiel $n \in D$, pre ktoré je

$$\mathbf{T} \vdash \neg(\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k).$$

Podľa podmienky b) je množina M rekurzívne očíslovateľná. Zrejme platí

$$n \in N \equiv \text{existuje } m \text{ také, že } \mathrm{Dokaz}_{\mathbf{T}}(m, F(n)).$$

Podľa podmienky c) je množina N rekurzívne očíslovateľná.

Ak $n \in M$, tak existuje riešenie $x_1, \ldots, x_k$ rovnice (18.41). Potom

$$\mathbf{T} \vdash \Delta(p_1)(\Delta_{x_1}, \ldots, \Delta_{x_k}) {=} \Delta(p_2)(\Delta_{x_1}, \ldots, \Delta_{x_k})$$

a teda

$$\mathbf{T} \vdash (\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k).$$

Keďže teória $\mathbf{T}$ je neprotirečivá, tak $n \notin N$. Teda $M \cap N = \emptyset$.

Keby bolo $D = M \cup N$, tak obidve množiny M a N by boli rekurzívne. Podľa vety 18.1 množina M však nie je rekurzívna. Teda existuje $n \in D$, ktoré nepatrí ani do M ani do N. Príslušná rovnica je hľadaná rovnica.

q.e.d.

Ak sa dohodneme, že základné deduktívne prostriedky metamatematiky obsahujú (alebo sú totožné) s prostriedkami Peanovej aritmetiky, tak dostaneme

Dôsledok 18.4 *Ak $\mathbf{T}_{\mathrm{P}}$ je neprotirečivá, tak existujú polynómy p_1, p_2 s kladnými koeficientami také, že diofantická rovnica*

$$p_1(x_1, \ldots, x_k) = p_2(x_1, \ldots, x_k)$$

nemá riešenie v prirodzených číslach, ale

$$\mathbf{T}_{\mathrm{P}} \nvdash \neg(\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k)$$

ani

$$\mathbf{T}_{\mathrm{P}} \nvdash (\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k).$$

Teda formula $(\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k)$ je nerozhodnuteľná veta Peanovej aritmetiky.

Overenie: Ak existuje dôkaz formuly

$$(\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k)$$

v Peanovej aritmetike, tak na základe vymedzenia prostriedkov metamatematiky tento dôkaz možno preložiť do overenia tvrdenia, že diofantická rovnica

$$p_1(x_1, \ldots, x_k) = p_2(x_1, \ldots, x_k)$$

má riešenie. To je spor.

q.e.d.

Dôsledok platí pre teórie silnejšie ako Presburgerova aritmetika a slabšie ako Peanova aritmetika. Pre teóriu $\mathbf{T}$ silnejšiu ako Peanova aritmetika nevieme, či

$$\mathbf{T} \vdash (\exists \mathrm{x}_1) \ldots (\exists \mathrm{x}_k)\, \Delta(p_1)(\mathrm{x}_1, \ldots, \mathrm{x}_k) {=} \Delta(p_2)(\mathrm{x}_1, \ldots, \mathrm{x}_k)$$

alebo nie.

Literatúra

[BL1] Bukovský L., Úvod do teórie algoritmov, ES UPJŠ, Košice, 2001.

[BL2] Bukovský L., Úvod do matematickej logiky, text v elektronickej forme UML.Tex prístupný na sieti Novell PF UPJŠ, Košice, 2001.

[DM1] Davis M., Computability & Unsolvability, McGraw-Hill, New York 1958.

[DM2] Davis M., *Hilbert's Tenth problem is Unsolvable,* Amer. Math. Monthly **80** (1973), 233–269.

[GJ] Goldstern M. and Judah H., The Incompleteness Phenomenon, A New Course in Mathematical Logic, A K Peters, Wellesley, Massaschusetts 1995.

[HPu] Hájek P. a Pudlák P., Metamathematics of First-Order Arithmetic, Perspectives in Mathematical Logic, Springer, Berlín 1993.

[HPa] Harrington L. a Paris J., *A mathematical incompletness in Peano Arithmetic,* v knihe: Handbook of Mathematical Logic, ed. Barwise J., North Holland, Amsterdam 1977, 1133–1142, ruský preklad Nauka, Moskva 1983, štvrtý diel.

[HD] Hilbert D., *Mathematical problems,* Bull. Amer. Math. Soc. **37** (2000), 407–436.

[K1] Kleene S. C., Introduction to the Metamathematics, van Nostrand, New York 1952, ruský preklad IIL, Moskva 1957.

[K2] Kleene S. C., Mathematical Logic, John Wiley & Sons, New York 1967, ruský preklad Izdateľstvo Mir, Moskva 1973.

[Ma] Matijasevič Ju. V., *Диофантовы множества,* Usp. Mat. Nauk. **27** (1972), 185–222

[Me] Mendelson E., Introduction to Mathematical Logic, van Nostrand Company, New York 1964, ruský preklad Nauka, Moskva 1984.

[Ro] Rogers H., Theory of Recursive Functions and Effective Computability, McGraw-Hill, New York 1967, ruský preklad Izdateľstvo Mir, Moskva 1972.

[Sh] Shoenfield J. R., Mathematical Logic, Addison-Wesley, Reading 1967, ruský preklad Nauka, Moskva 1975.

[Ta1] Tarski A., *Pojęcie prawdy w językach nauk dedukcyjnych,* Warszawa, 1933, nemecký preklad *Der Wahrheitsbegriff in den formalisierten Sprachen,* Studia Phil. **1** (1936), 261–405.

[Ta2] Tarski A., Undecidable Theories, North Holland, Amsterdam 1950.