Kapitola 1

Nerozhodnutelnost a neúplnost

V této, závěrečné kapitole se budeme zabývat tím, jak lze s teoriemi pracovat algoritmicky. Zlatým hřebem budou *Gödelovy věty o neúplnosti* z roku 1930, které ukazují limity formálního přístupu, a které zastavily desetiletí trvající program formalizace matematiky. Nemáme zde dostatek prostoru k uvedení formálních definic a úplných důkazů, proto se místy budeme pohybovat na poněkud intuitivní úrovni. Zaměříme se na pochopení smyslu tvrzení a myšlenek důkazů.

Pojem *algoritmu* budeme chápat také jen intuitivně. Pokud bychom ho chtěli formalizovat, potom nejběžnější (ale zdaleka ne jedinou) volbou je koncept *Turingova stroje*.[1]

1.1 Rekurzivní axiomatizace a rozhodnutelnost

V důkazových systémech, kterými jsme se zabývali (tablo metoda, rezoluce, hilbertův kalkulus) jsme povolili, aby teorie T, ve které dokazujeme, byla nekonečná. Vůbec jsem se ale zatím nezabývali tím, jak je zadaná. Pokud chceme ověřit, že je daný objekt (tablo, rezoluční strom, posloupnost formulí) korektním důkazem, potřebujeme nějaký algoritmický přístup ke všem axiomům T.

Jednou z možností by bylo požadovat *enumerátor* T, tj. algoritmus, který vypisuje na výstup axiomy z T, a každý axiom někdy vypíše.[2] Potom by bylo snadné potvrdit, že je daný důkaz korektní. Pokud bychom ale dostali důkaz, který použil chybný axiom, který v T není, nikdy bychom se to nedozvěděli: nekonečně dlouho bychom čekali, zda jej enumerátor přeci jen nevypíše. Požadujeme proto silnější vlastnost, která umožňuje rozpoznat i chybné důkazy *rekurzivní axiomatizaci*:[3]

Definice 1.1.1 (Rekurzivní axiomatizace)**.** Teorie T je *rekurzivně axiomatizovaná*, pokud existuje algoritmus, který pro každou vstupní formuli φ doběhne a odpoví, zda $\varphi \in T$.

Poznámka 1.1.2. Ve skutečnosti by nám stačil enumerátor pro T, pokud by bylo garantováno, že vypisuje axiomy v lexikografickém uspořádání. To už je ekvivalentní rekurzivní axiomatizaci. (Rozmyslete si proč.)

[1] Viz přednáška NTIN090 Základy složitosti a vyčíslitelnosti.

[2] Nutným předpokladem je, aby T byla spočetná. K tomu stačí předpokládat, že jazyk je spočetný.

[3] Slovo *rekurzivní* zde neznamená běžně známou rekurzi, ale odkazuje na formalizaci algoritmu pomocí ‘rekurzivních funkcí’ od Gödela. Rekurzivní funkce zde znamená totéž, co vyčíslitelná nějakým Turingovým strojem, a teorii vyčíslitelnosti (*computability theory*) se někdy také říká *recursion theory*.

Zaměříme se na otázku, zda můžeme v dané teorii T 'algoritmicky rozhodovat pravdu' (tj. platnost vstupní formule). Pokud ano, říkáme, že je teorie *rozhodnutelná.* To je ale poměrně silná vlastnost, definujeme proto také *částečnou rozhodnutelnost*, která znamená, že pokud formule platí, algoritmus nám to řekne, ale pokud neplatí, nikdy se nemusíme dočkat odpovědi.

Definice 1.1.3 (Rozhodnutelnost)**.** O teorii T říkáme, že je

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

Můžeme jako obvykle předpokládat, že φ v definici je sentence. Ukážeme si jednoduché tvrzení:

Tvrzení 1.1.4. *Nechť T je rekurzivně axiomatizovaná. Potom:*

(i) T je částečně rozhodnutelná,

(ii) je-li T navíc kompletní, potom je rozhodnutelná.

Důkaz. Algoritmem ukazujícím částečnou rozhodnutelnost je konstrukce systematického tabla pro Fφ.[4] Pokud φ v T platí, konstrukce skončí v konečně mnoha krocích a snadno ověříme, že je tablo sporné, jinak ale skončit nemusí.

Je-li T kompletní, víme, že $T \vdash \varphi$ právě když $T \not\vdash \varphi$. Budeme tedy paralelně konstruovat tablo pro Fφ a tablo pro Tφ (důkaz a zamítnutí φ z T): jedna z konstrukcí po konečně mnoha krocích skončí. □

1.1.1 Rekurzivně spočetná kompletace

Požadavek kompletnosti je příliš silný, ukážeme, že stačí pokud jsme schopni efektivně popsat všechny kompletní jednoduché extenze.[5]

Definice 1.1.5 (Rekurzivně spočetná kompletace)**.** Řekneme, že teorie T má *rekurzivně spočetnou kompletaci*, pokud (nějaká) množina až na ekvivalenci všech jednoduchých kompletních extenzí teorie T je *rekurzivně spočetná*, tj. existuje algoritmus, který pro danou vstupní dvojici přirozených čísel (i, j) vypíše na výstup i-tý axiom j-té extenze (v nějakém pevně daném uspořádání[6]), nebo odpoví, že takový axiom už neexistuje.[7]

Tvrzení 1.1.6. *Pokud je teorie T rekurzivně axiomatizovaná a má rekurzivně spočetnou kompletaci, potom je T rozhodnutelná.*

[4] Zde nám stačí enumerátor axiomů T, nebo postupně generujeme všechny sentence (např. v lexikografickém pořadí) a pro každou testujeme, zda je axiomem.

[5] Tj. 'všechny modely až na elementární ekvivalenci'.

[6] Zde potřebujeme, aby byl jazyk spočetný.

[7] Jeli extenzí méně než j, nebo má-li j-tá extenze méně než i axiomů.

Důkaz. Pro danou sentenci φ buď $T \vdash \varphi$, nebo existuje protipříklad $\mathcal{A} \not\models \varphi$, tedy kompletní jednoduchá extenze T_i teorie T taková, že $T_i \nvdash \varphi$. Z kompletnosti ale plyne, že $T_i \vdash \neg\varphi$. Náš algoritmus bude paralelně konstruovat tablo důkaz φ z T a (postupně) tablo důkazy $\neg\varphi$ ze všech kompletních jednoduchých extenzí $T_1, T_2, \ldots$ teorie T.[8] Víme, že alespoň jedno z paralelně konstruovaných tabel je sporné, a můžeme předpokládat, že konečné (neprodlužujeme-li sporné větve tabla), tedy algoritmus ho po konečně mnoha krocích zkonstruuje. $\square$

Cvičení 1.1. Ukažte, že následující teorie mají rekurzivně spočetnou kompletaci:

- Teorie čisté rovnosti (prázdná teorie v jazyce $L = \langle\rangle$ s rovností),
- Teorie unárního predikátu (prázdná teorie v jazyce $L = \langle U \rangle$ s rovností, kde U je unární relační symbol),
- Teorie hustých lineárních uspořádání DeLO* (kompletní jednoduché extenze jsou popsané v Důsledku **??**),

Jde o rekurzivně axiomatizované teorie (neboť jsou konečné), jsou tedy rozhodnutelné.

Příklad 1.1.7. Na závěr uveďme bez důkazu několik dalších příkladů rozhodnutelných teorií:

- Teorie Booleových algeber (Alfred Tarski 1940),
- Teorie algebraicky uzavřených těles (Tarski 1949),
- Teorie komutativních grup (Wanda Szmielew 1955).

Tyto teorie jsou také nekompletní, ale rekurzivně axiomatizované a mají rekurzivně spočetnou kompletaci.

1.1.2 Rekurzivní axiomatizovatelnost

V předchozí kapitole, konkrétně v Sekci **??**, jsme se zabývali otázkou, kdy lze popsat nějakou třídu struktur [resp. teorii] pomocí axiomů [určitého tvaru]. Nyní se zaměřme na otázku, kdy to lze udělat *algoritmicky.*

Definice 1.1.8 (Rekurzivní axiomatizovatelnost)**.** Třída L-struktur $K \subseteq \mathrm{M}_L$ je *rekurzivně axiomatizovatelná*, pokud existuje rekurzivně axiomatizovaná L-teorie T taková, že $K = M_L(T)$. Teorie T' je *rekurzivně axiomatizovatelná*, pokud je rekurzivně axiomatizovatelná třída jejích modelů, neboli pokud je T' ekvivalentní nějaké rekurzivně axiomatizované teorii.

Poznámka 1.1.9. Podobně bychom mohli definovat *rekurzivně spočetnou axiomatizovatelnost.*

Ukažme si následující jednoduché tvrzení:

Tvrzení 1.1.10. *Je-li $\mathcal{A}$ konečná struktura v konečném jazyce s rovností, potom je teorie* $\mathrm{Th}(\mathcal{A})$ *rekurzivně axiomatizovatelná.*

Poznámka 1.1.11. Z toho plyne i že $\mathrm{Th}(\mathcal{A})$ je rozhodnutelná, což ale není překvapivé: platnost sentence φ v konečné struktuře $\mathcal{A}$ můžeme snadno ověřit.

[8] Nevadí, že je jich nekonečně mnoho, můžeme využít tzv. *dovetailing*: Provedeme 1. krok konstrukce 1. tabla, potom 2. krok 1. tabla a 1. krok 2. tabla, 3. krok 1. tabla, 2. krok 2. tabla, 1. krok 3. tabla, atd.

Důkaz. Očíslujme prvky domény jako $A = \{a_1, \dots, a_n\}$. Teorii $\mathrm{Th}(\mathcal{A})$ lze axiomatizovat jedinou sentencí, která je tvaru 'existuje právě n prvků $a_1, \dots, a_n$ splňujících právě ty *základní vztahy* o funkčních hodnotách a relacích, které platí ve struktuře $\mathcal{A}$'.[9] $\square$

Uveďme několik standardních příkladů struktur, které lze 'algoritmicky popsat':

Příklad 1.1.12. Pro následující struktury je $\mathrm{Th}(\mathcal{A})$ rekurzivně axiomatizovatelná, a tedy i rozhodnutelná:

- $\langle \mathbb{Z}, \leq \rangle$, jde o tzv.teorii *diskrétních lineárních uspořádání*,
- $\langle \mathbb{Q}, \leq \rangle$, jde o teorii DeLO,
- $\langle \mathbb{N}, S, 0 \rangle$, teorie *následníka s nulou*,
- $\langle \mathbb{N}, S, +, 0 \rangle$, *Presburgerova aritmetika*,
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, teorie *reálně uzavřených těles*,[10]
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, teorie *algebraicky uzavřených těles charakteristiky 0.*

Důsledek 1.1.13. *Pro struktury uvedené v Příkladu 1.1.12 platí, že* $\mathrm{Th}(\mathcal{A})$ *je rozhodnutelná.*

Poznámka 1.1.14. Jak ale vyplývá z První Gödelovy věty o neúplnosti (viz níže), teorie *standardního modelu aritmetiky*, tj. struktury $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ *nemá* rekurzivně axiomatizovatelnou teorii.

1.2 Aritmetika

Vlastnosti přirozených čísel hrají důležitou roli nejen v matematice, ale například také v kryptografii. Připomeňme, že jazyk aritmetiky je jazyk $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností. Jak jsme zmínili v Poznámce 1.1.14, tzv. *standardní model aritmetiky* $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ nemá rekurzivně axiomatizovatelnou teorii. Proto používáme rekurzivně axiomatizované teorie, které se snaží vlastnosti $\underline{\mathbb{N}}$ popsat částečně; těmto teoriím říkáme *aritmetiky.*

1.2.1 Robinsonova a Peanova aritmetika

Uvedeme jen dva nejdůležitější příklady aritmetik: *Robinsonovu* a *Peanovu.*

Definice 1.2.1 (Robinsonova aritmetika)**.** *Robinsonova aritmetika* je teorie Q v jazyce aritmetiky sestávající z následujících (konečně mnoha) axiomů:

$$\begin{array}{ll}
\neg S(x) = 0 & x \cdot 0 = 0 \\
S(x) = S(y) \to x = y & x \cdot S(y) = x \cdot y + x \\
x + 0 = x & \neg x = 0 \to (\exists y)(x = S(y)) \\
x + S(y) = S(x + y) & x \leq y \leftrightarrow (\exists z)(z + x = y)
\end{array}$$

[9] Například, pokud $f^{\mathcal{A}}(a_4, a_2) = a_{17}$, přidáme do konjunkce atomickou formuli $f(x_{a_4}, x_{a_2}) = x_{a_{17}}$ (kde x_{a_i} jsou proměnné odpovídající jednotlivým prvkům). A pokud $(a_3, a_3, a_1) \in R^{\mathcal{A}}$, přidáme $R(x_{a_3}, x_{a_3}, x_{a_1})$.

[10] Tento významný výsledek A. Tarského (1949) také znamená, že lze algoritmicky rozhodovat, které vlastnosti platí v Euklidovské geometrii.

Robinsonova aritmetika je velmi slabá, nelze v ní dokázat například komutativitu ani asociativitu sčítání či násobení, nebo tranzitivitu uspořádání.

Na druhou stranu v ní lze dokázat všechna *existenční tvrzení o numerálech*, která jsou pravdivá v $\underline{\mathbb{N}}$. Tím myslíme formule, které v prenexním tvaru mají pouze existenční kvantifikátory, a do kterých jsme za volné proměnné substituovali *numerály* $\underline{n} = S(\dots S(0)\dots)$.

Příklad 1.2.2. Například, pro formuli $\varphi(x,y)$ tvaru $(\exists z)(x+z=y)$ je $Q \vdash \varphi(\underline{1},\underline{2})$, kde $\underline{1} = S(0)$ a $\underline{2} = S(S(0))$.

Platí tedy následující tvrzení, které ponecháme bez důkazu.

Tvrzení 1.2.3. *Je-li $\varphi(x_1,\dots,x_n)$ existenční formule a $a_1,\dots,a_n \in \mathbb{N}$, potom platí:*

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

Užitečným rozšířením Robinsonovy aritmetiky je tzv. Peanova aritmetika, ve které lze *dokazovat indukcí*:

Definice 1.2.4 (Peanova aritmetika)**.** *Peanova aritmetika PA* je extenze Robinsonovy aritmetiky Q o *schéma indukce*, tj. pro každou L-formuli $\varphi(x,\overline{y})$ přidáme následující axiom:

$$(\varphi(0,\overline{y}) \land (\forall x)(\varphi(x,\overline{y}) \to \varphi(S(x),\overline{y}))) \to (\forall x)\varphi(x,\overline{y})$$

Peanova aritmetika je mnohem lepší aproximací teorie $\mathrm{Th}(\underline{\mathbb{N}})$, lze v ní dokázat všechny 'základní' vlastnosti platné v $\underline{\mathbb{N}}$ (například komutativitu a asociativitu sčítání). Stále ale existují sentence v jazyce aritmetiky, které platí v $\underline{\mathbb{N}}$, ale v Peanově aritmetice jsou nezávislé.[11]

Poznámka 1.2.5. Pokud bychom se přesunuli do logiky *2. řádu*, potom bychom už mohli strukturu $\underline{\mathbb{N}}$ axiomatizovat (až na izomorfismus), a to extenzí Peanovy aritmetiky o následující formuli 2. řádu, tzv. *axiom indukce*:

$$(\forall X)((X(0) \land (\forall x)(X(x) \to X(S(x)))) \to (\forall x)X(x))$$

Připomeňme, že X reprezentuje (libovolnou) unární relaci, neboli podmnožinu univerza. Použitím axiomu indukce na množinu následníků 0 získáme, že každý prvek (daného modelu) je následníkem nuly. Tak můžeme sestrojit izomorfismus s $\underline{\mathbb{N}}$.

1.3 Nerozhodnutelnost predikátové logiky

V této sekci si ukážeme, že nelze (algoritmicky) rozhodovat logickou platnost formulí prvního řádu.[12]

Věta 1.3.1 (O nerozhodnutelnosti predikátové logiky)**.** *Neexistuje algoritmus, který by pro danou vstupní formuli φ rozhodl, zda je logicky platná.*[13]

Protože zatím neznáme potřebný formalismus týkající se algoritmů, např. pojem Turingova stroje, zvolíme jako výchozí bod jiný *nerozhodnutelný problém*. Nejznámějším je tzv. *Halting problem*, tj. otázka, zda se daný program zastaví na daném vstupu.[14] My si ale usnadníme práci tím, že zvolíme jiný nerozhodnutelný problém, tzv. *Hilbertův desátý problém*.[15]

[11] Jak si ukážeme v Gödelově První větě o neúplnosti.

[12] Jinými slovy, že prázdná teorie $T = \emptyset$ není rozhodnutelná.

[13] Tj. zda je formule φ tautologie, neboli zda $\models \varphi$. Zde mluvíme o formulích 1. řádu, v libovolném jazyce.

[14] Jeho nerozhodnutelnost si dokážete v předmětech NTIN071 Automaty a gramatiky a poté znovu v NTIN090 Základy složitosti a vyčíslitelnosti.

[15] Hilbert jej vyslovil v roce 1900, a publikoval v roce 1902 spolu s 22 dalšími problémy, které významně

1.3.1 Hilbertův desátý problém

Mějme polynom $p(x_1, \ldots, x_n)$ s celočíselnými koeficienty. Hilbertův desátý problém se ptá po algoritmu, který rozhodne, zda má takový vstupní polynom celočíselný kořen, neboli zda má *Diofantická rovnice* $p(x_1, \ldots, x_n) = 0$ (celočíselné) řešení:

> "Nalezněte algoritmus, který po konečně mnoha krocích určí, zda daná Diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má celočíselné řešení."

Kdyby se Hilbert dožil vyřešení svého desátého problému v roce 1970, byl by překvapen, že žádný takový algoritmus neexistuje.

Věta 1.3.2 (Matiyasevich, Davis, Putnam, Robinson)**.** *Problém existence celočíselného řešení dané Diofantické rovnice s celočíselnými koeficienty je (algoritmicky) nerozhodnutelný.*

Důkaz zde pro nedostatek místa neuvedeme. K důkazu nerozhodnutelnosti ve skutečnosti použijeme následující důsledek, který mluví o polynomech s přirozenými koeficienty, a o řešení v přirozených číslech.

Důsledek 1.3.3. *Neexistuje algoritmus, který by pro danou dvojici polynomů* $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_n)$ *s* přirozenými *koeficienty rozhodl, zda mají přirozené řešení, tj. zda platí:*

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

Důkaz důsledku. Důkaz je snadný, využívá faktu, že každé celé číslo lze vyjádřit jako rozdíl dvojice přirozených čísel, a naopak, každé přirozené číslo lze vyjádřit jako součet čtyř čtverců (celých čísel).[16] Každou Diofantickou rovnici lze tedy transformovat na rovnici z důsledku, a naopak. □

1.3.2 Důkaz nerozhodnutelnosti

Připomeňme, že Robinsonova aritmetika Q má jen konečně mnoho axiomů, $\underline{\mathbb{N}}$ je jejím modelem, a lze v ní dokázat všechna *existenční tvrzení o numerálech* platná v $\underline{\mathbb{N}}$. Nyní jsme připraveni dokázat Větu o nerozhodnutelnosti predikátové logiky.

Důkaz věty o nerozhodnutelnosti predikátové logiky. Uvažme formuli φ tvaru

$$(\exists x_1) \ldots (\exists x_n)\ p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$$

kde p a q jsou polynomy s přirozenými koeficienty. Dle Tvrzení 1.2.3 platí:

$$\underline{\mathbb{N}} \models \varphi \text{ právě když } Q \vdash \varphi$$

Označme jako ψ_Q konjunkci (generálních uzávěrů) všech axiomů Q. Zřejmě $Q \vdash \varphi$, právě když $\psi_Q \vdash \varphi$, což platí právě když $\vdash \psi_Q \to \varphi$. Dle Věty o úplnosti je to ale ekvivalentní $\models \psi_Q \to \varphi$. Dostáváme tedy následující ekvivalenci:

$$\underline{\mathbb{N}} \models \varphi \text{ právě když } \vdash \psi_Q \to \varphi$$

ovlivnily matematiku 20., i 21. století. Některé zůstávají nevyřešeny, např. Riemannova hypotéza, viz Wikipedia.

[16] Tzv. Lagrangeova věta o čtyřech čtvercích.

To znamená, že pokud existoval algoritmus rozhodující logickou platnost, mohli bychom rozhodovat i existenci přirozeného řešení rovnice $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$, neboli Hilbertův desátý problém by byl rozhodnutelný.[17] Což by byl spor. $\square$

1.4 Gödelovy věty

Na závěr přednášky představíme slavné Gödelovy věty o neúplnosti, jejichž pochopení by mělo být samozřejmou součástí vzdělání každého informatika. Pokusíme se vysvětlit i princip důkazů, ale vynecháme veškeré technické detaily.

1.4.1 První věta o neúplnosti

Nejprve vyslovíme Gödelovu *První větu o neúplnosti*, a vysvětlíme smysl jejích předpokladů.

Věta 1.4.1 (První věta o neúplnosti). *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence, která je pravdivá v $\underline{\mathbb{N}}$, ale není dokazatelná v T.*

Velmi neformálně řečeno, tato věta říká, že vlastnosti aritmetiky přirozených čísel nelze 'rozumně', efektivně popsat (v logice 1. řádu), každý takový popis je nutně 'neúplný'.

Je důležité si uvědomit, že mluvíme o *pravdivosti* ve standardním modelu aritmetiky, tj. ve struktuře $\underline{\mathbb{N}}$, zatímco *dokazatelnost* je v teorii T. (Z Věty o úplnosti samozřejmě plyne, že každá sentence *pravdivá v T* je v T i dokazatelná.)

Bezespornost je nutným předpokladem, neboť ve sporné teorii je dokazatelná každá sentence. Připomeňme, že rekurzivní axiomatizovanost můžeme chápat jako 'efektivní zadání' axiomů (pomocí algoritmu), bez této vlastnosti by taková teorie nebyla užitečná. Požadavek aby teorie byla extenzí Robinsonovy aritmetiky chápejte jako předpoklad, že má alespoň 'základní aritmetickou sílu', že v ní lze určitým způsobem 'mluvit' o přirozených číslech. Existují různé varianty tohoto předpokladu, s jinými teoriemi než je Robinsonova aritmetika, a není například nutné, aby šlo přímo o extenzi, stačí, když je v teorii Robinsonova aritmetika v jistém smyslu 'definovatelná'. Ale teorie, ve které 'nelze zakódovat přirozená čísla' (a zde je důležité, že můžeme mluvit nejen o sčítání, ale i o násobení), je 'příliš slabá'.

Je dobré si uvědomit, že speciálně platí i následující tvrzení 'o nekompletnosti':

Důsledek 1.4.2. *Splňuje-li teorie T předpoklady První věty o neúplnosti a je-li navíc $\underline{\mathbb{N}}$ modelem teorie T, potom T není kompletní.*

Důkaz. Předpokládejme pro spor, že T je kompletní. Vezměme sentenci φ, která je pravdivá v $\underline{\mathbb{N}}$ ale není dokazatelná v T. Díky kompletnosti víme, že $T \vdash \neg\varphi$, potom ale Věta o korektnosti říká, že $T \models \neg\varphi$, tedy φ je lživá v $\underline{\mathbb{N}}$, což je spor. $\square$

Zajímavé je nejen samotné tvrzení První věty o neúplnosti, ale také její důkaz: Gödel v něm přišel se zcela novou, na svou dobu převratnou důkazovou technikou. Sentence sestrojená v důkazu formalizuje tvrzení *"Nejsem dokazatelná v T"*, důkaz je založen na následujících dvou principech, které níže poněkud neformálně popíšeme:

[17] Ukazujeme, že existuje *redukce* "těžkého" problému (Hilbertova desátého) na náš problém, tedy i náš problém je "těžký".

- *aritmetizace syntaxe*, tedy zakódování sentencí a jejich dokazatelnosti do přirozených čísel,
- *self-reference*, tedy schopnost sentence 'mluvit sama o sobě' (o svém kódu).

Aritmetizace dokazatelnosti

Konečné syntaktické objekty, jako jsou termy, formule, konečná tabla, a tedy i tablo důkazy, lze zakódovat do přirozených čísel. Konkrétní způsob jak to provést jako technický detail přeskočíme.[18] Stačí nám, že jsme schopni efektivně provést zakódování, a také poté kód přečíst (dekódovat).

Označme kód formule φ jako $\ulcorner\varphi\urcorner$, podobně pro jiné syntaktické objekty. Numerál odpovídající kódu φ, tedy $\ulcorner\varphi\urcorner$-tý numerál, budeme značit $\underline{\varphi}$. Pro danou teorii T definujme následující binární relaci na množině všech přirozených čísel:

$$(n, m) \in \mathrm{Proof}_T \quad \text{právě když} \quad n = \ulcorner\varphi\urcorner \text{ a } m = \ulcorner\tau\urcorner, \text{ kde } \tau \text{ je tablo důkaz sentence } \varphi \text{ z } T$$

Máme-li efektivní přístup k axiomům, umíme také efektivně zkontrolovat zda τ je opravdu důkazem φ, tedy platí:

Pozorování 1.4.3. *Je-li T rekurzivně axiomatizovaná, je relace* $\mathrm{Proof}_T \subseteq \mathbb{N}^2$ *rekurzivní.*

Klíčovou, ale velmi technickou částí důkazu První věty je následující tvrzení, které ponecháme bez důkazu.

Tvrzení 1.4.4. *Je-li T navíc extenzí Robinsonovy aritmetiky Q, potom existuje formule $Prf_T(x, y)$ v jazyce aritmetiky, která* reprezentuje *relaci* Proof_T*, tj. pro každá $n, m \in \mathbb{N}$ platí:*

- *Je-li $(n, m) \in \mathrm{Proof}_T$, potom $Q \vdash Prf(\underline{n}, \underline{m})$,*
- *jinak $Q \vdash \neg Prf(\underline{n}, \underline{m})$.*

Formule $Prf(x, y)$ tedy vyjadřuje *"y je důkaz x v T"*.[19] Potom můžeme vyjádřit, že *"x je dokazatelná v T"*, a to formulí $(\exists y)Prf(x, y)$. Lze dokázat následující, opět velmi technický důsledek:

Důsledek 1.4.5. *Pokud $T \vdash \varphi$, potom platí $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\varphi}, y)$ a také $T \vdash (\exists y)Prf_T(\underline{\varphi}, y)$.*

Umíme tedy vyjádřit, že daná sentence je, nebo také není, dokazatelná. Jak ale může sentence říci sama o sobě, že není dokazatelná? K tomu použijeme *princip self-reference.*

Self-reference

Abychom ilustrovali princip self-reference, pro názornost si místo logické sentence představme větu v češtině, a místo vlastnosti 'být dokazatelný' tvrzení o počtu písmen. Podívejme se na následující větu:

```
Tato věta má 22 znaků.
```

[18] Představte si jakýkoliv rozumný způsob, jak daný objekt zapsat do souboru. Soubor v binárním kódu je posloupnost 0 a 1. Připíšeme na začátek jedničku, abychom nezačínali nulou, a máme binární zápis přirozeného čísla.

[19] Přesněji, tablo jehož kódem je y je důkazem sentence jejíž kódem je y.

V přirozeném jazyce snadno vyjádříme self-referenci zájmenem 'Tato', z kontextu víme, že myslíme větu samou. Ve formálních systémech ale typicky nemáme self-referenci přímo k dispozici. *Přímou referenci* obvykle máme k dispozici, stačí umět 'mluvit' o posloupnostech symbolů, jako v následujícím příkladě:

```
Následující věta má 29 znaků. "Následující věta má 29 znaků."
```

Zde se ale není žádná self-reference. Pomůžeme si trikem, kterému budeme říkat 'zdvojení':

```
Následující věta zapsaná jednou a ještě jednou v uvozovkách má 149
znaků. "Následující věta zapsaná jednou a ještě jednou v uvozovkách
má 149 znaků."
```

Pomocí přímé reference a zdvojení tedy můžeme získat self-referenci.

Poznámka 1.4.6. Stejný princip lze použít k sestrojení programu v C, jehož výstupem je jeho vlastní kód (34 je ASCII kód uvozovek):[20]

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

1.4.2 Důkaz a důsledky

[TODO]

1.4.3 Druhá věta o neúplnosti

Druhá Gödelova věta o neúplnosti říká, neformálně řečeno, že efektivně daná, dostatečně bohatá teorie nemůže sama dokázat svou bezespornost. Bezespornost vyjádříme následující sentencí, kterou označíme jako Con_T:

$$\neg(\exists y)Prf_T(\underline{0 = 1}, y)$$

Všimněte si, že platí $\underline{\mathbb{N}} \models Con_T$, právě když $T \nvdash 0 = \underline{1}$. Neboli sentence Con_T opravdu vyjadřuje, že *"Teorie T je bezesporná"*.

Věta 1.4.7 (Druhá věta o neúplnosti)**.** *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Peanovy aritmetiky platí, že Con_T není dokazatelná v T.*

[TODO]

Věta o pevném bodě

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

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

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

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

[20] V Pythonu si vystačíme bez principu zdvojení: `print(open(__file__).read())`

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

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})} \tag{1.1}$$

- Za ψ vezměme sentenci $\varphi(d(\underline{\varphi(d(x))}))$. Stačí ověřit $T \vdash d(\underline{\varphi(d(x))}) = \underline{\psi}$.
- To plyne z (1.1) pro $\chi(x)$ tvaru $\varphi(d(x))$, neboť v tom případě

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

Nedefinovatelnost pravdy

Nedefinovatelnost pravdy

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

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

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

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

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

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

což v bezesporné teorii není možné. $\square$

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

1. věta o neúplnosti

Důkaz 1. věty o neúplnosti

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

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

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

$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y). \tag{1.2}$$

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

- Nejprve ukážeme, že ψ_T *není dokazatelná v T*. Kdyby $T \vdash \psi_T$, tj. ψ_T je lživá v $\underline{\mathbb{N}}$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy z (1.2) plyne $T \vdash \neg\psi_T$, což ale není možné, neboť T je bezesporná.

- Zbývá dokázat, že ψ_T je pravdivá v $\underline{\mathbb{N}}$. Kdyby ne, tj. $\underline{\mathbb{N}} \models \neg\psi_T$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy $T \vdash \psi_T$, což jsme již dokázali, že neplatí. □

Důsledky a zesílení 1. věty

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

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

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

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

Gödelovu 1. větu o neúplnosti lze následovně zesílit.

Věta (Rosser) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje nezávislá sentence. Tedy T je nekompletní.*
Poznámka Tedy předpoklad, že $\underline{\mathbb{N}} \models T$, je v prvním důsledku nadbytečný.

1.4.4 Druhá věta o neúplnosti

[TODO]

Gödelova 2. věta o neúplnosti

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

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

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

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

$$\text{“}\textit{Je-li } T \textit{ bezesporná, pak } \psi_T \textit{ není dokazatelná v } T.\text{”} \tag{1.3}$$

  Jinak vyjádřeno, platí $Con_T \rightarrow \psi_T$.

- Je-li T extenze Peanovy aritmetiky, důkaz tvrzení (1.3) lze formalizovat v rámci T. Tedy $T \vdash Con_T \rightarrow \psi_T$.

- Jelikož T je bezesporná dle předpokladu věty, podle (1.3) je $T \nvdash \psi_T$.

- Z předchozích dvou bodů vyplývá, že $T \nvdash Con_T$. $\square$

Poznámka Taková teorie T tedy neumí dokázat vlastní bezespornost.

1.4.5 Důsledky druhé věty

[TODO]

Důsledky 2. věty

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

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

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

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

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

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