Gödelovy věty o neúplnosti

Eva Ondráčková

Tato přednáška volně navazuje na předchozí Úvod do výrokové a predikátové logiky a bude se zabývat Gödelovými větami o neúplnosti. To jsou slavná tvrzení, která ve své době zcela změnila tvář matematiky. Naším cílem bude seznámit se s jejich zněním a důkazem, pochopit hlouběji, co vlastně tvrdí a jaký je jejich význam v logice a matematice. A možná se tak i váš pohled na tyto disciplíny trochu změní ...

Enumerovatelnost a rozhodnutelnost

Definice. (Enumerovatelnost a rozhodnutelnost) *Nechť $\mathcal{F}$ je množina formulí nějakého jazyka L, T je teorie s jazykem L.*

• *Říkáme, že $\mathcal{F}$ je enumerovatelná, existuje-li algoritmická procedura, která generuje všechny prvky množiny $\mathcal{F}$.*

• *Říkáme, že teorie T je rozhodnutelná, jestliže existuje algoritmická procedura, která pro libovolnou formuli A jazyka L dovoluje rozhodnout, zda A je či není větou teorie T. V opačném případě říkáme, že T je nerozhodnutelná.*

Můžete si rozmyslet (a na přednášce si o tom povíme), jaký je mezi těmito dvěma pojmy vztah, jestli třeba jeden neplyne z druhého ...
V definici jsme použili slovní spojení „algoritmická procedura“. Pod tím si pravděpodobně každý představí něco maličko jiného, bylo by tedy užitečné si tento pojem nějak formalizovat. Zavedeme si proto pojem rekurzivní funkce. Rekurzivními funkcemi se zabývá teorie vyčíslitelnosti a my do ní příliš fušovat nebudeme, postačí nám intuitivní představa, o čem je řeč. Uvedeme si přesné znění definice, ale spíše pro zajímavost; na přednášce si povíme o tom, jak jinak (a jednodušeji) lze na rekurzivní funkce nahlížet.

Definice. (Základní funkce) *Základními funkcemi nazveme funkce:*

• $o(x) \simeq 0$ *(nulová funkce)*

• $s(x) \simeq x + 1$ *(funkce následníka)*

• $\mathcal{I}_n^j(x_1, \ldots, x_n) \simeq x_j$, *kde* $1 \leq j \leq n$ *(funkce vydělení j-té složky)*

Symbolem $\simeq$ rozumíme, že pravá strana má smysl právě tehdy, když má smysl levá, a pak se rovnají.

Definice. (Operátory)

• *operátor substituce:* $\mathcal{S}_n^m(f, g_1, \ldots, g_m) = h$, *kde* h *je funkce taková, že*

$$h(x_1, \ldots, x_n) \simeq f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).$$

• *operátor primitivní rekurze, „for-cyklus“:* $\mathcal{R}_n(f, g) = h$, *kde*

$$h(0, x_2, \ldots, x_n) \simeq f(x_2, \ldots, x_n),$$
$$h(y+1, x_2, \ldots, x_n) \simeq g(y, h(y, x_2, \ldots, x_n), x_2, \ldots, x_n).$$

• *operátor minimalizace, „while-cyklus“:* $\mathcal{M}_n(f) = h$, *kde* $n \geq 1$ *a* $h(x_1, \ldots, x_n) \simeq z$ *pro* z *takové, že*

$$(\forall j)_{j<z}\ f(x_1, \ldots, x_n, j) \text{ je definovaná a různá od } 0,$$
$$f(x_1, \ldots, x_n, z) \text{ je definovaná a rovná } 0.$$

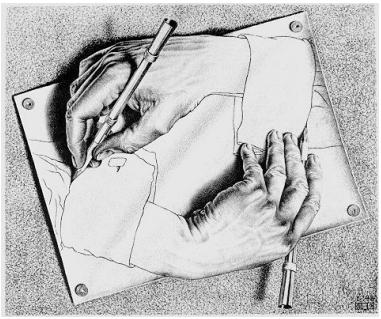
Definice. (Rekurzivní funkce) *Funkci nazveme primitivně rekurzivní (částečně rekurzivní), jestliže ji lze odvodit ze základních funkcí pomocí konečně mnoha použití operátorů* $\mathcal{S}_n^m$, $\mathcal{R}_n$ *(a* $\mathcal{M}_n$*). Částečně rekurzivní funkce definované všude nazveme rekurzivní.*

Definice.

• *Říkáme, že množina* $A \subseteq \mathbb{N}$ *je rekurzivní, je-li její charakteristická funkce rekurzivní.*

• *Říkáme, že množina* $A \subseteq \mathbb{N}$ *je rekurzivně spočetná, je-li definičním oborem nějaké částečně rekurzivní funkce.*

Aritmetizovatelnost a reprezentovatelnost



Ukážeme si, že formální systém lze tzv. *aritmetizovat*, tedy že jeho termy, formule, posloupnosti formulí a důkazy můžeme pomocí rekurzivních funkcí kódovat přirozenými čísly a tím vlastně onen formální systém celý vnořit do aritmetiky. A naopak, rekurzivní funkce v aritmetice můžeme *reprezentovat* zpět ve formálním systému, neboli převést aritmetické rovnosti na dokazatelnost určitých formulí a tak zase do onoho formálního systému vnořit celou aritmetiku. Tím dojdeme k pozoruhodným závěrům, umožníme například formulím, aby hovořily o jiných formulích, případně samy o sobě. Odtud

už získáme kýžené výsledky: neúplnost, nerozhodnutelnost, nedefinovatelnost pravdy atd.

Kódování formálního systému

Uvedeme si zde několik kroků kódování, začneme posloupnostmi: položíme

$$\langle\rangle = 1 \text{ (kód prázdné posloupnosti)},$$
$$\langle n_0, n_1, \ldots, n_k\rangle = p_0^{n_0+1} \cdot p_1^{n_1+1} \cdots p_k^{n_k+1},$$

kde $k \geq 0$ a p_i je i-té prvočíslo.

Jazyk aritmetiky je jazyk se speciálními symboly 0, S, $+$, $\cdot$ a $\leq$. Nejprve přiřadíme každému symbolu speciální číslo, které použijeme pro kódování. O proměnných budeme předpokládat, že se jmenují pouze x_i pro $i \in \mathbb{N}$. Přiřadíme jim sudá čísla, speciálním symbolům lichá čísla a logickým symbolům dosud nepoužitá lichá čísla:

$$\sigma(x_i) = 2i \text{ pro všechna } i \in \mathbb{N},$$
$$\sigma(0) = 1,\ \sigma(S) = 3,\ \sigma(+) = 5,\ \sigma(\cdot) = 7,\ \sigma(\leq) = 9,$$
$$\sigma(\neg) = 11,\ \sigma(\rightarrow) = 13,\ \sigma(\forall) = 15,\ \sigma(=) = 17.$$

Nyní přistoupíme ke kódování termů a formulí. Nechť x_i je proměnná, r a s jsou termy, pak budeme přiřazovat číslo $\sharp$ takto:

$$\sharp x_i = \langle\sigma(x_i)\rangle = \langle 2i\rangle \qquad \sharp 0 = \langle 1\rangle$$
$$\sharp Sr = \langle\sigma(S), \sharp r\rangle \qquad \sharp(r+s) = \langle\sigma(+), \sharp r, \sharp s\rangle$$
$$\sharp(r \cdot s) = \langle\sigma(\cdot), \sharp r, \sharp s\rangle$$

Analogický postup použijeme pro formule. Jsou-li B a C formule, pak

$$\sharp(r = s) = \langle\sigma(=), \sharp r, \sharp s\rangle \qquad \sharp(r \leq s) = \langle\sigma(\leq), \sharp r, \sharp s\rangle$$
$$\sharp\neg B = \langle\sigma(\neg), \sharp B\rangle \qquad \sharp(B \rightarrow C) = \langle\sigma(\rightarrow), \sharp B, \sharp C\rangle$$
$$\sharp(\forall x_i)B = \langle\sigma(\forall), \langle 2i\rangle, \sharp B\rangle$$

Reprezentovatelnost

Definice. *Nechť T je teorie prvního řádu s jazykem aritmetiky L. Potom namísto $A_{x_1,\ldots,x_k}[n_1, \ldots, n_k]$ budeme pro jednoduchost psát $A(n_1, \ldots, n_k)$.*

• *Říkáme, že k-ární relace $R \subseteq \mathbb{N}^k$ je reprezentovatelná v teorii T, jestliže existuje formule A v jazyce L s volnými proměnnými x_1, x_2, … , x_k taková, že pro libovolná n_1, n_2, … , $n_k \in \mathbb{N}$ platí*

$$R(n_1, n_2, \ldots, n_k) \Rightarrow T \vdash A(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k}),$$
$$\neg R(n_1, n_2, \ldots, n_k) \Rightarrow T \vdash \neg A(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k}).$$

Říkáme, že formule A reprezentuje relaci R v teorii T.

• *Říkáme, že k-ární funkce f je reprezentovatelná v teorii T, jestliže existuje formule A v jazyce L s volnými proměnnými x_1, x_2, … , x_k, y taková, že pro libovolná n_1,*

$n_2, \ldots, n_k \in \mathbb{N}$ *platí*

$$T \vdash A(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k}, y) \leftrightarrow y = \overline{f(n_1, n_2, \ldots, n_k)}.$$

Říkáme, že formule A reprezentuje funkci f v teorii T.

Definice. (Robinsonova aritmetika) *Robinsonova aritmetika Q je teorie prvního řádu s následujícími axiomy:*

Q1:	$S(x) \neq 0$	*Q5:*	$x + S(y) = S(x + y)$
Q2:	$S(x) = S(y) \rightarrow x = y$	*Q6:*	$x \cdot 0 = 0$
Q3:	$x \neq 0 \rightarrow \exists y\ (x = S(y))$	*Q7:*	$x \cdot S(y) = (x \cdot y) + x$
Q4:	$x + 0 = x$	*Q8:*	$x \leq y \leftrightarrow \exists z\ (z + x = y)$

Definice. (Peanova aritmetika) *Peanova aritmetika P je teorie prvního řádu s jazykem aritmetiky, má axiomy Q1, Q2, Q4 – Q8 a následující schéma indukce:*

$$A_x[0] \rightarrow \{\forall x(A \rightarrow A_x[S(x)]) \rightarrow \forall x A\}.$$

Definice. (Úplná aritmetika) *Úplná aritmetika $Th(\mathfrak{N})$ je teorie v jazyku aritmetiky, jejíž axiomy jsou všechny uzavřené formule pravdivé ve standardním modelu aritmetiky $\mathfrak{N}$, tedy*

$$Th(\mathfrak{N}) = \{A | A \text{ je uzavřená formule a } T \models A\}.$$

Je-li $T \subseteq Th(\mathfrak{N})$ teorie s jazykem aritmetiky a jsou-li všechny rekurzivní relace a všechny částečně rekurzivní funkce reprezentovatelné v T, píšeme Repr T.

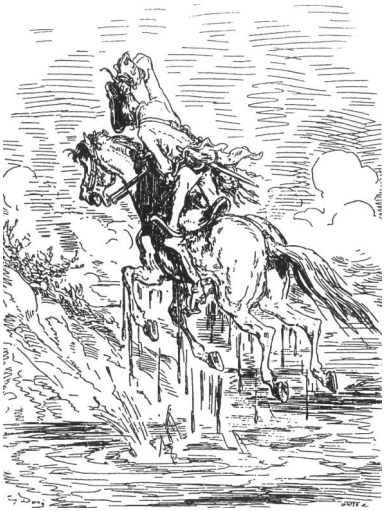
Věta. *Repr Q, Repr P, Repr $Th(\mathfrak{N})$.*

Lemma. (O diagonalizaci) *Nechť T je teorie taková, že platí Repr T. Pro každou formuli A s jednou volnou proměnnou existuje uzavřená formule D_A taková, že platí*

$$T \vdash D_A \leftrightarrow A_x[\overline{\sharp D_A}]$$

(D_A říká „mám vlastnost A“).

Věta. (A. Tarski, o nedefinovatelnosti pravdy v aritmetice)
(i) Nechť T je bezesporné rozšíření Q, pro které platí Repr T. Je-li množina $Th(T)$ všech pravdivých uzavřených formulí teorie T reprezentovatelná v T, pak existuje uzavřená formule D jazyka teorie T taková, že D ani $\neg D$ není prvkem množiny $Th(T)$.



(ii) $Th(T)$ *není reprezentovatelná v* $Th(T)$.

Definice. *Je-li* T *teorie s jazykem aritmetiky, definujeme množinu* Thm_T *kódů vět teorie* T *jako* $Thm_T = \{\sharp A | A$ *je formule a* $T \vdash A\}$. *Řekneme, že* T *je rozhodnutelná, právě když* Thm_T *je rekurzivní množina.*

Věta. (O nerozhodnutelnosti aritmetiky, Church, 1936) *Je-li* T *bezesporné rozšíření Robinsonovy aritmetiky* Q, *potom* T *je nerozhodnutelná teorie.*

Věta. (O neúplnosti aritmetiky, Gödel, Rosser) *Je-li* T *rekursivně axiomatizované rozšíření Robinsonovy aritmetiky, pak* T *není úplná teorie.*

Věta. (Druhá věta o neúplnosti, Gödel, 1931) *Nechť* T *je bezesporné, rekurzivně axiomatizovatelné rozšíření Peanovy aritmetiky. Pak* $T \nvdash \neg Thm_T(\overline{\sharp(0 = 1)})$.

A co to všechno vůbec znamená?

První Gödelova věta říká, že máme-li libovolný formální systém tak silný, že obsahuje základní aritmetiku, pak nutně obsahuje tvrzení, která v něm nelze dokázat ani vyvrátit. Mohou tak existovat pravdy, ke kterým nelze zkonstruovat důkaz (a naopak nepravdy, pro něž neexistuje důkaz jejich negace). Druhá věta tvrdí zase to, že uvnitř dostatečně silné teorie nelze dokázat bezespornost jí samé. Populárně řečeno: prostředky matematiky nemůžeme dokázat konzistenci matematiky.

Literatura

- *Petr Štěpánek: Meze formální metody, v elektronické podobě k dispozici na* `http://ktiml.mff.cuni.cz/downloads/Meze_ps.zip`.
- *Douglas R. Hofstadter: Gödel, Escher, Bach: an Eternal Golden Braid, Basic Books, Inc., 1979.*
- *John D. Barrow: Pí na nebesích (O počítání, myšlení a bytí), Edice Kolumbus, Mladá fronta 1992.*