

Gödelova veta a súvislosti

Mišo Forišek

<misof@mfnotes.ksp.sk>
 Department of Computer Science
 Faculty of Mathematics, Physics, and Informatics
 Comenius University, Bratislava, Slovakia

Február 2008

1 Stručná história matiky

dávno praľudia, Čína, Mezopotámia, Egypt

-550 až 300 antické Grécko:

začiatky Táles a Pytagoras: objav iracionálnych čísel

-300 Euklides a jeho Základy (geometrie): axiómy, vety, dôkazy

-230 Eratostenovo sito

500 až 1500 Čína a Arabi:

rozvoj algebry, algoritmus, kryptoanalýza

1000 Al-Karaji: matematická indukcia

1200 až 1600 Európa sa zobúdzda:

1200 Fibonacci: arabské číslice

ešte v 1400 rímske číslice, neexistuje plus, rovná sa, ani x

1510: všeobecné riešenie kubickej rovnice

16. storočie: rozvoj trigonometrie

1600 a ďalej Európa sa rozbehla:

1637: Descartes: súradnicová sústava, analytická geometria

1654: Pascal a Fermat: kombinatorika a hlavne pravdepodobnosť

koniec 17. stor.: Newton a Leibniz nezávisle na sebe objavujú analýzu

Leibniz: myšlienka univerzálneho formalizmu a mechanického dokazovania

18. stor.: Euler zavádza pojem funkcie $f(x)$, mocninové rady, Eulerova fcia a dôkaz aj zovšeobecnenej Malej Fermatovej vety, základy teórie grafov (7 mostov v Kaliningrade)

„Lisez Euler, lisez Euler, c'est notre maître à tous“ – Laplace

1796: Gauss: modulárna aritmetika, základná veta algebry (korene polynómu)

1830: Lobačevskij a Bolyai: neeuklidovská geometria

koniec 19. stor.: Bolzanova a Cantorova teória množín, problémy s nekonečnom

2 Gottlob Frege

Begriffsschrift (1879): formalizácia logiky (axiomatickej predikátovej), kvantifikátory ako významný krok vpred oproti Aristotelovskej logike.

Jeden z hlavných cieľov: pri dôkaze sa nemusieť odvolávať na „je to intuitívne jasné“, mechanická kontrolovateľnosť.

Na základe logických základov potom formalizuje aritmetiku v Grundgesetze der Arithmetik (1893, druhý diel 1903).

Prúser: Tesne pred tým ako ide druhý diel do tlače prichádza list od Russella.

3 Bertrand Russell a jeho paradox

Russell ukazuje problém hneď v základoch, v axiomatizácii teórie množín.

Princíp v čom bol problém: ukazuje, že nie pre každú vlastnosť existuje množina s tou vlastnosťou.

Russellova formálna formulácia: „množina tých množín, ktoré neobsahujú samé seba“. Príklad takejto množiny: komplement množiny všetkých štvorcov.

Príbuzné formulácie v ľudskej reči: Paradox vojenského holiča, Grellingov-Nelsonov paradox heterologických slov.

4 Zermelo a Fraenkel

1908 Zermelov pokus, potom 1920 spolu s Fraenkelom a Skolemom vylepšená verzia – nová lepšia axiomatická teória množín.

(Novú várku problémov prináša Axióm výberu, ale o tom inokedy.)

(Boli aj iné riešenia, ako napr. typové teórie, ale táto je najvýznamnejšia.)

5 Hilbertove problémy

Rok 1900, International Congress of Mathematicians, David Hilbert uvádza zoznam 23 problémov, čím v podstate stanovuje program matematiky pre 20. storočie.

1. Hypotéza kontinua.
2. Dokázať korektnosť (bezospornosť) axióm aritmetiky.
3. Mám dva mnohosteny s rovnakým objemom, dá sa jeden rozrezať na konečne veľa kusov a preskladať na druhý? (nie)
8. Riemannova hypotéza.
10. Algoritmus na riešenie polynomických Diofantických rovníc.
13. Riešenie rovníc 7. stupňa pomocou funkcií dvoch premenných.

6 Hilbertov program

Po roku 1920 prichádza Hilbert s prirodzeným cieľom: nájsť dokázateľne korektnú formalizáciu matematiky. Podrobnejšie:

- Formálny jazyk na zápis tvrdení, formálne pravidlá na manipuláciu s nimi.
- Úplnosť: Všetko pravdivé musí byť dokázateľné.
- Korektnosť (bezospornosť): Nepravdivé sa nesmie dať dokázať.
(Dôkaz tejto vlastnosti by pokiaľ možno mal uvažovať len o konečných objektoch.)
- Konzervatívnosť: Každý výsledok o „reálnych objektoch“ by mal byť dokázateľný bez pomoci „ideálnych objektov“ (napr. nespočítateľných množín).
- Rozhodnuteľnosť: Algoritmus rozhodujúci pravdivosť tvrdenia.

Príklad: Dôležitosť bezospornosti – z jedného sporu už vyplýva čokoľvek.

Príklad: Konzervatívnosť: čo ide komplexnými číslami, ide aj v reálnych.

7 Gödelova veta

Základná myšlienka: chceme v danom formálnom systéme vyrobiť tvrdenie, ktoré bude hovoriť „som nedokázateľné“.

V korektnom formálnom systéme zdanlivo dostávame spor:

Ak by bolo nepravdivé, tak je dokázateľné. A ak je dokázateľné, tak je pravdivé. Spor.

Tým sme dokázali, že musí byť pravdivé. Ale potom je nedokázateľné. Spor?

Spor je len zdanlivý, lebo my sme to nedokázali. My sme pravdivosť tvrdenia len zdôvodnili v metajazyku. Celú úvahu budeme musieť ešte raz zopakovať, a to priamo v danom formálnom systéme.

Ukážeme, že v každom dostatočne silnom systéme ide takéto „Gödelovo tvrdenie“ sformulovať, a predstavuje v ňom príklad tvrdenia, ktoré je intuitívne pravdivé, ale nedokázateľné.

7.1 Aritmetizácia syntaxe

Základnou myšlienkou, ktorou Gödel predbehol dobu, je aritmetizácia: očíslovanie výrokov, formúl aj dôkazov prirodzenými číslami.

Teda akonáhle máme systém schopný pracovať s číslami, vieme určite pracovať aj s tvrdeniami.

7.2 Požiadavky na teóriu

Možnosť interpretovať Peanovu aritmetiku (0, 1, +, × a indukcia).

Potreba ω -bezospornosti: Nesmie sa dať súčasne dokázať $(\exists x)F(x)$ aj všetky $\neg F(i)$.

(Rosser v 1936 ukázal, že stačí obyčajná bezospornosť – zostrojil tvrdenie „ak existuje môj dôkaz, tak existuje dôkaz mojej negácie, ktorý má od neho menšie číslo“.)

7.3 Konštrukcia Gödelovho tvrdenia

Majme teóriu T . Očíslujme si všetky formuly v nej, ktoré obsahujú jediná voľnú premennú x . Teda množina týchto formúl bude $\{\varphi_n(x) \mid n \in \mathbb{N}\}$. Rovnako majme množinu dôkazov $\{\Delta_n \mid n \in \mathbb{N}\}$. Obe tieto kódovania vieme spraviť efektívne, teda tak, že vieme prevádzať medzi číslom a formulou/dôkazom.

Príklad: $\varphi_{47}(x)$ môže byť tvrdenie „ x je prvočíslo“, Δ_9 môže byť dôkaz: „2 nedelí 7, 3 nedelí 7, ..., 6 nedelí 7, 7 je prvočíslo“.

Ďalej v teórii T vieme sformulovať predikát (funkciu vracajúcu true/false):

$$Dok(n, m, k) : \quad \text{je } \Delta_k \text{ dôkazom tvrdenia } \varphi_n(m)?$$

Príklad: $Dok(47, 7, 9)$ by vrátilo true, lebo Δ_9 je dôkaz $\varphi_{47}(x)$.

Tieto funkcie fungujú úplne mechanicky: Z n a m zostrojím funkciu, z k zostrojím dôkaz (postupnosť axióm a pravidiel odvodenia), zaradom čítam dôkaz a kontrolujem korektnosť krokov, na konci porovnam záver s dokazovaným tvrdením.

Zjavné: ak vieme dokázať $\varphi_n(m)$, tak vieme dokázať $(\exists z)Dok(n, m, z)$.

Menej zjavné: opačný smer. Na ten potrebujeme tú spomínanú ω -bezospornosť. Totiž ak bude naša teória moc divoká, tak to proste vyplývať nebude. (Príklad s 2 riadkami nekonečnej tabuľky.)

Uvažujme teraz formulu $Nedok(x) = \neg(\exists z)Dok(x, x, z)$, teda „tvrdenie $\varphi_x(x)$ nemá dôkaz“.

Toto tvrdenie je opäť formula s jednou voľnou premennou x , a teda má nejaké číslo g . Inými slovami, $\varphi_g(x) = Nedok(x)$.

A už sme doma: Všimnime si tvrdenie $\varphi_g(g)$. Toto je ono – hovorí „tvrdenie $\varphi_g(g)$ nemá dôkaz“.

7.4 Dôkaz

Nech je dokázateľné $\varphi_g(g)$. Potom zoberme dôkaz a nájdime jeho číslo d . Keď vieme d , vieme dokázať $Dok(g, g, d)$, a z toho vieme dokázať $(\exists z)Dok(g, g, z)$, čo je $\neg\varphi_g(g)$.

Naopak, nech je dokázateľné $\neg\varphi_g(g)$. To je tvrdenie $(\exists z)Dok(g, g, z)$. Pri ω -bezospornosti z toho vyplýva, že vieme dokázať aj niektoré z tvrdení $Dok(g, g, z)$, a teda aj tvrdenie $\varphi_g(g)$.

Stručný záver: Ak je teória bezosporná, tak je neúplná.

8 Ďalšie rany do hlavy

Druhá Gödelova veta: V rámci takejto teórie nevieme ani dokázať jej vlastnú bezospornosť.

Tarski: Nedá sa definovať, čo je pravda. Presnejšie, v bezospornej teórii nejde sformulovať predikát $Pravda(x, y)$, ktorý by bol pravdivý práve vtedy, keď je $\varphi_x(y)$ pravdivé.

Ešte bola nádej „odfiltrovať“ takéto škaredé tvrdenia a hrať sa len s tými dobrými, dokázateľnými.

Church 1936: Predikát $(\exists z)Dok(x, y, z)$ nie je rekurzívny.

Dôsledok: Vieme síce generovať dokázateľné tvrdenia, nevieme však o tvrdení mechanicky zistiť, či je dokázateľné.

Disclaimer. Tieto poznámky môžete voľne používať na ľubovoľné nekomerčné účely. Na akékoľvek komerčné využitie je potrebný súhlas autora. Ak v mojich poznámkach objavíte nejakú chybu, prípadne ich nejakým spôsobom viete doplniť, budem rád, ak mi dáte vedieť.

Pre potreby prípadného citovania má tento kus poznámok evidenčné číslo MF-0011.