Dokazování v informatice

Ondřej Kunčar

Automated Reasoning Group
http://arg.mff.cuni.cz

ATP 2010, 3. října 2010

Přehled

- verifikace softwaru
  - často se nepoužívá plná síla dokazovače pro logiku prvního řádu
- verifikace obvodů
  - 1994 – Pentium FDIV bug
  - John Harrison
    - pracuje v Intelu
    - autor interaktivního dokazovače HOL Light
    - `http://www.cl.cam.ac.uk/~jrh13/`
- formalizace matematiky

Správnost důkazu

Správnost důkazu

Téměř nikdy není správnost důkazu dosažena formálními prostředky, ale spíše „sociálními prostředky“.

- Sociální prostředky
  - Neformální diskuse mezi matematiky.
  - Systém recenzního posuzování.
- Sociální prostředky mají několik problémů.

Mohou selhat – The Four Color Theorem

- 1879 – Alfred Kempe – vymyslel důkaz, který byl tehdy široce přijímán
- 1880 – Peter Guthrie Tait – další důkaz
- 1890 – Percy Heawood – Kempkeho důkaz je špatně
- 1891 – Julius Petersen – Taitův důkaz je taky špatně
- 1976 – Kenneth Appel a Wolfgang Haken – důkaz používající počítač
- 80. léta – pochybnosti o důkazu, řada vědců tvrdí, že našla chybu
- 1995 – Neil Robertson, Daniel P. Sanders, Paul Seymour, a Robin Thomas – revidovaný důkaz
- 2005 – Benjamin Werner a Georges Gonthier – formální důkaz v systému Coq

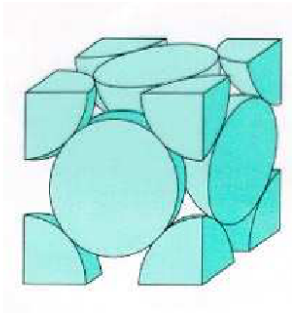
Nejsou si jisti – The Jordan Curve Theorem

- Camille Jordan – první důkaz
- následuje celá řada pochybností a námitek
- Oswald Veblen – většina se shoduje, že je to první úplný důkaz
- 2005 – Tom Hales – formální důkaz v systému HOL Light
- 2005 – Andrzej Trybulec a Yatsuka Nakamura – další formální důkaz v systému Mizar

Nejsou lidi

- velmi specializovaný důkaz – např. 5 lidí na světě je mu schopno porozumět
  - resp. má zájem
- důkaz je obrovský
  - Chudnovsky, Robertson, Seymour a Thomas – The Strong Perfect Graph Theorem – 150 stránek
  - Neil Robertson and Paul D. Seymour – The Graph Minor Theorem – 500 stránek
- nebo oboje
  - The Kepler conjecture
    - panel 12 recenzentů
    - po 4 letech jsou si jisti na 99 procent

The Kepler conjecture



- 1611 – formulováno Keplerem
- 1998 – Thomas Hales – důkaz s pomocí počítače
  - 250 stránek textu
  - 3GB dat (zdrojové kódy, data, výsledky)
- 2003 – Hales a jeho spolupracovníci zahajuji práci na formálním důkazu
- 2010 – Project FlysPecK – 65 procent hotovo v textové části

State of Art

1. The Irrationality of the Square Root of 2
2. Fundamental Theorem of Algebra
3. The Denumerability of the Rational Numbers
4. Pythagorean Theorem
5. Prime Number Theorem
6. Gödel's Incompleteness Theorem
7. Law of Quadratic Reciprocity
8. The Area of a Circle
9. Euler's Generalization of Fermat's Little Theorem

...

`http://www.cs.ru.nl/~freek/100/index.html`

Revoluce?

Správnost důkazu

Computer science změní práci matematiků.

- Freek Wiedijk: zhmotňování důkazů (odplatonizování)
- Matematici sami začnou psát své důkazy formálně
  - de facto zanikne sociální proces hodnocení
- Námitky:
  - matematici se neshodnou na jednom systému
  - je to příliš těžké
  - matematiky to nezajímá

Matematická wikipedia

- O čem přemýšlím
  - Wikipedia – univerzální encyklopedie
  - Myslím si: změnila přístup k informacím
  - Skeptici: nikdo nebude zadarmo psát encyklopedii
    - těžce se spletli
    - ve 240 jazycích
    - anglická má přes 3 miliony článků
- Formalizace matematiky
  - existuje, ale offline
  - Mizar - cca 50 tisíc vět
  - kdyby online: zopakuje se úspěch Wikipedie?
  - podaří se formalizovat celou matematiku?