Interaktivno dokazivanje teorema

Filip Marić

Matematički fakultet,
Univerzitet u Beogradu

16. oktobar 2015.

Pregled

Dokazi u matematici

- Matematika je deduktivna nauka
- Preko 2000 godina matematičari teže ka što preciznijim i striktnijim dokazima
- Dokaz matematičarima pruža:
  1. objašnjenje
  2. opravdanje

Greške u matematičkim dokazima

- Lecat, 1935: „Erreurs de math'ematiciens" – veoma bogata kolekcija grešaka koje su napravili čuveni matematičari pre 1900-te
- S obzirom na hiperprodukciju, veruje se da se kolekcija poput Lecatove za period posle 1900-te ne bi mogla napraviti

Greške u matematičkim dokazima

Neki čuveni primeri:

- Vejls i Tejlor su preko godinu dana ispravljali grešku koja je pronađena u prvoj verziji Vejlsovog dokaza velike Fermaove teoreme
- Mejson i Gorenštajn su 1980. objavili klasifikaciju konačnih grupa, međutim, pronađena praznina je popunjena tek 2001. godine i to dokazom od 1.221 strane koji su dali Ašbaher i Smit.
- Časopis „Anali Matematike" je imenovao 12 recenzenata koji analizirali dokaz Keplerove hipoteze koji su prijavili Hejls i Ferguson (dokaz je bio ispisan na 300 strana i sadržao je 40.000 linija programskog koda), da bi posle četiri pune godine izjavili da su „99% sigurni" da je dokaz ispravan

Istorijat formalnog dokazivanja teorema

- Pioniri formalnog dokazivanja teorema: Euklid, Lajbnic, Frege, Rasel i Vajthed, Burbakisti, Hilbert, ...
- Gedelove teoreme neodlučivosti
- Makarti, 1960-ih: „Provera matematičkih dokaza jedna je od najinteresantnijih i najkorisnijih primena automatskih računara”

Automatsko i interaktivno dokazivanje teorema

- Automatsko dokazivanje teorema podrazumeva da računar samostalno konstruiše dokaz teoreme
- Interaktivno dokazivanje podrazumeva da čovek zadaje kostur dokaza, a da računar proverava njegovu korektnost automatski dopunjavajući nedostajuće korake (koji mogu biti netrivijalni)

Istorijat interaktivnih dokazivača

- De Brujinov sistem AUTOMATH iz kasnih 1960-ih jedan je od prvih uspešnih interaktivnih dokazivača teorema — 1970-ih, u njemu su formalizovane Landauove „Osnove analize”
- Kroz istoriju se koristilo mnoštvo različitih sistema (LCF, NQHTM, HOL, Mizar, . . .)
- Danas su najkorišćeniji interaktivni dokazivači Coq, Isabelle/HOL, HOL Light, ACL2, PVS, Agda, Matita, Lean . . .

Logičke osnove

- Osnove interaktivnih dokazivača su obično rezultati iz polja matematičke logike
- Prirodna dedukcija
- λ-račun i teorija tipova
- Kari-Hauardov izomorfizam

Pouzdanost dokazivača

- Quis custodiet ipsos custodes?
- Jezgro sistema mora biti krajnje jednostavno
- Kompleksna i efikasne automatske komponente konstruišu dokaze, ali svi dokazi na kraju moraju biti provereni od strane krajnje jednostavnog jezgra (de Brujnov princip, LCF princip)

Pregled

Primer

DEMO

Pregled

Teorema o prostim brojevima

- Prime Number Theorem (PNT)
- Asimptotski zakon distribucije prostih brojeva
- Pretpostavili Ležandr, Gaus i Dirihle u drugoj polovini 18. veka
- Ako je $\pi(x)$ broj prostih brojeva manjih i jednakih broju x, tada

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \ln x} = 1$$

Teorema o prostim brojevima

- Čebišev napravio značajan napredak, ali glavni korak je napravio Riman koji povezao PNT sa nulama ζ-funkcije na osnovu čega su Adamar i de La Vale Puason našli dokaz.
- Hardi je verovao da dokaz zahteva kompleksnu analizu, ali su 1949. Erdoš i Selberg našli elementaran dokaz.

Dve formalizacije

1. 2005. Avigad i drugi formalizuju elementaran dokaz u sistemu Isabelle/HOL
2. 2009. Harison formalizuje analitički dokaz u sistemu HOL Light
3. različite propratne biblioteke
   - Avigad: teorija prirodnih i celih brojeva sa naglaskom na proste brojeve i deljivost, fundamentalna teorema aritmetike, konačne sume i proizvodi, realni brojevi i svojstva logaritama, asimptotika i O-notacija, ...
   - Harison: realni brojevi uvedeni preko Košijevih nizova, analiza u $\mathbb{R}^n$, kompleksni brojevi $\mathbb{C}$ izgrađeni nad $\mathbb{R}^2$ (kompleksno diferenciranje, holomorfne i analitičke funkcije, Košijeva integralna formula za topološki jednostavne oblasti), definicija ζ-funkcije i osnovna svojstva, ...
4. Elementaran dokaz je oko 30.000 linija koda, a analitički oko 5.000 linija.

4-obojivost grafova

- Oko 1850. Gutri je pokušao da oboji mapu VB samo sa četiri boje i pretpostavio je da četiri boje dovoljno za svaku mapu
- De Morgan se zainteresovao za problem
- Mnoštvo nepotpunih i pogrešnih dokaza tokom više od 100 godina
- Birkhof pravi određen progres, ali postaje jasno da će za dokaz biti potrebna ogromna analiza slučajeva
- 1976. Apel i Haken „dokazuju" teoremu pišući program u asembleru za IBM 370 koji analizira više od 10.000 slučajeva
- Da li je takav dokaz matematički prihvatljiv?
- 1995. Robertson i ostali prave čistiju verziju tog dokaza (programe pišu u C-u i smanjuju broj slučajeva koje je potrebno razmatrati)

Formalni dokaz

- Gontije, 2005. u sistemu Coq.
- Precizno tvrđenje teoreme („svaka mapa se može obojiti sa četiri boje, tako da su susedne regije obojene različitim bojama" je očigledno veoma neprecizno)
- Iako se govori o topološkim objektima, dokaz je suštinski kombinatoran
- Osnovna struktura su hipermape (omogućavaju prepoznavanje uslova planarnosti pomoću Ojlerove, a ne Žordanove teoreme koja je sama po sebi izazov za formalizaciju)
- Dokaz zasnovan na refleksiji tj. na izračunavanju
- Oko 60.000 linija koda (oko 1.000 definicija i više od 2.5000 lema)

Fejt-Tompsonova teorema

- Značajan korak u klasifikaciji konačnih grupa (klasifikacija završena 2008. godine je izuzetno značajan rezultat u celokupnoj istoriji matematike)
- Svaka konačna grupa neparnog reda je rešiva (može se razložiti na seriju abelovskih faktora tj. postoji $\{1\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_k = G$, tdj. G_{j-1} normalna podgrupa grupe G_j i G_j/G_{j-1} je Abelova, za svako $j = 1, 2, \ldots, k$)
- Fejt i Tompson su ovo dokazali 1963. i dokaz zauzima celo izdanje časopisa (više od 250 strana)

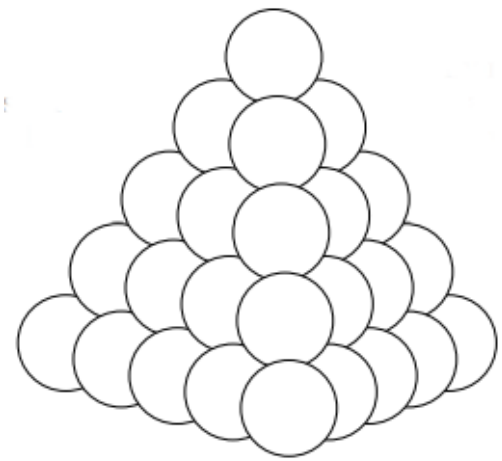
Formalizacija Fejt-Tompsonove teoreme

- Gontije i ostali (rad ima 15 autora) su 2012. objavili da su formalizovali Fejt-Tompsonov dokaz
- Sama formulacija teoreme (uključujući i sve potrebne definicije) zahteva manje od 100 linija koda
- Dokaz sadrži više od 150.000 linija koda (oko 4.000 definicija i 13.000 lema)

Formalizacija Fejt-Tompsonove teoreme

- Potrebno je bilo kombinovati mnoge matematičke tehnike i prilagoditi dokazivače tako da implicitno, iz konteksta zaključuju mnoge stvari
  - Na primer, „Ako su G i H grupe, f homomorfizam iz G u H i a i b su iz G, tada je $f(ab) = f(a)f(b)$.
  - G je grupa u stvari znači da je to skup sa operacijom, jediničnim i inverznim elementom
  - a je iz G u stvari znači da je a iz skupa nosača te grupe
  - ab je primena operacije grupe G, a $f(a)f(b)$ je primena operacije grupe H
- Matematičari ovakve nepreciznosti podrazumevaju, dok je za interaktivno dokazivanje teorema pravi izazov naučiti računare da tako zaključuju stvari iz konteksta

Keplerova hipoteza



- 1611. Kepler je pretpostavio da je najgušće pakovanje jednakih sfera u prostoru „pakovanje đuladi”
- Popunjenost je $\pi/(3\sqrt{2})$ tj. oko 74%
- Mnogi matematičari su pokušavali ovo da dokažu (npr. Gaus).
- Feješ Tot je prvi predložio uspešnu strategiju – formulisati problem kao optimizacioni problem nad konačnim brojem promenljivih i upotrebiti računare da izvrše optimizaciju

Keplerova hipoteza — prvi dokaz

- 1998. Hejls je najavio prvi dokaz (izveden uz pomoć računarskih JAVA programa)
- Objavljen tek 2005. i to nakon što je tim od 12 recenzenata izjavio da su 99% sigurni da je sve u redu
- Hejls se nije mogao zadovoljiti time i pokrenuo je kolaborativni FlysPecK projekat (Formal Proof of Kepler) sa ciljem da se njegov dokaz formalno verifikuje

Formalan dokaz Keplerove hipoteze

- Kombinuje formalizaciju matematike (Euklidski prostor, diskretna geometrija, analitičke nejednakosti) i verifikaciju softvera (dokaze korektnosti programa koji izvode različite oblike optimizacije)
- Veliki tim istraživača sa nekoliko svetskih univerziteta (Hejls, Harison, Nipkov, . . .)
- Nekoliko različitih interaktivnih dokazivača – svaki pogodan za određene delove dokaza
- Sama provera dokaza (uključujući proces verifikovane optimizacije) traje nedelju dana na 32 procesora

Verifikovani C kompilator

- Korektnost softvera u velikoj meri zavisi od korektnosti kompilatora
- CompCert – verifikovani kompilator za veoma širok podskup jezika C
- Potpuno isprogramiran i verifikovan u sistemu CoQ
- Dobijeni C kod je veoma efikasan (implementirane i verifikovane mnoge kompleksne faze optimizacije)

Verifikovani OS

- Mikrojezgro – jedini deo OS koji radi u privilegovanom režimu i ima potpuni pristup hardveru
- Korektnost OS zavisi od korektnosti mikrojezgra
- seL4 – potpuno verifikovano mikrojezgro u sistemu Isabelle/HOL
- Mikrojezgro sadrži oko 8.700 linija C koda 8 oko 600 linija asemblerskog koda
- Dokazi korektnosti sadrže oko 450.000 linija koda
- seL4 se koristi trenutno u nekoliko sistema kod kojih je bezbednost izuzetno važna (npr. Boing ga koristi u svojim Little Bird helikopterima)

Pregled

Rezultati istraživača iz Srbije

- Sporadična istraživanja uglavnom nezavisnih istraživača
- Teorija dokaza, teorijske osnove interaktivnog dokazivanja, λ-račun (Došen, Petrić, Borisavljević, Gilezan, Lutovac, . . .)
- Interaktivno dokazivanje (Petar Maksimović, Predrag Janičić, Bojan Marinković, Vesna Marinković, Sana Stojanović-Đurđević, Danijela Simić, Mirko Spasić, . . .)

Rezultati istraživača iz Srbije

- Formalizacija SAT i SMT rešavača
- Formalizacije u vezi sa Franklovom hipotezom
- Formalizacije geometrijskog rezonovanja i geometrije kompleksne ravni
- Formalizacije šahovskih problema
- Formalizacije procesnog računa
- Formalizacije verovatnosnih logika
- Formalizacije mrežnih protokola
- ...

Pregled

Zaključci

- Oblast između matematike i računarstva
- Značajno polje istraživanja u poslednjih tridesetak, pa i više godina
- Trebaju nam široke biblioteke formalizovanog matematičkog znanja, bolja automatizacija procesa dokazivanja, bolja komunikacija između različitih sistema, mehanizmi efikasne pretrage postojećeg znanja, bolji načini da se izračunavanje inkorporira u dokazivanje, bolji korisnički interfejsi, itd.
- Ipak, napredak na ovom polju je evidentan i pitanje je vremena kada će formalno dokazane teoreme postati uobičajeni oblik matematičke delatnosti