

Razvijanje matematičkih veština kroz interaktivno dokazivanje teorema

Sana Stojanović Đurđević, Andrija Urošević, Filip Marić

Argo seminar
Automated Reasoning GrOup
Matematički fakultet, Beograd, 27. Maj, 2025.

Šta je dokaz?

- Izvođenje zaključka teoreme na osnovu skupa aksioma i pravila izvođenja
- Dokaz objašnjava zašto je teorema tačna, dok formalni dokaz radi istu stvar ali kroz mnogo više detalja (*Bezem, Hendriks*)
- Zavisí od konteksta u kom se koristi
 - Obrazovni sistem (tradicionalni dokazi - papir):
akcenat je na ideji, što kraći ali razumljivi dokazi
 - Formalni sistem (formalni dokazi - računar):
akcenat je na ispravnosti dokaza, nije dozvoljeno izostavljanje delova dokaza

Dokazivanje teorema uz pomoć računara

- Programi za automatsko dokazivanje
DA/NE odgovor na pitanje: Da li je dato tvrđenje teorema?
(koriste se za proveravanje ispravnosti tvrđenja)
- Programi za interaktivno dokazivanje
Detaljan odgovor na pitanje: Da li je dati dokaz datog tvrđenja ispravan?
(koriste se za proveravanje ispravnosti dokaza teoreme)
- Kombinacija prethodna dva pristupa

Prednosti i mane formalnog dokazivanja

- Da li je dokazivanje teorema zanimljivije uz pomoć računara? - DA!!!
- Da li je dokazivanje teorema lakše uz pomoć računara? - I DA I NE!!!
Zavisi od cilja koji želimo da postignemo.
- Prednosti
 - Dokazi su sigurno ispravni
 - Omogućava detaljniji uvid u skup pravila i aksioma koje se koriste u dokazu
 - Bolje razumevanja strukture dokaza
- Mane
 - Vremenski zahtevno, daleko od trivijalnog
 - Struktura formalnog dokaza nekada odstupa od originalnog dokaza iz knjige

Upotreba Isabelle-a u nastavi matematike i računarstva

- Dva načina kreiranja interaktivnih dokaza:
 - Skript dokazi (koriste *apply rule* naredbe)
 - Isar dokazi (koriste ključne reči bliske svakodnevnom rečniku: *proof*, *assume*, *show*)
- Bogat jezik, veoma blizak jeziku klasične matematike
- Sintaksa nalik funkcionalnim programskim jezicima
- Koristi se za formalizaciju bitnog matematičkog znanja
- Koristi se sve češće za formalnu verifikaciju softvera

Uvod u interaktivno dokazivanje teorema

- Relativno nov kurs na Matematičkom fakultetu:
 - (2018) IV godina smera Informatika
 - (2025) I godina master smera Informatika
- Pređeno gradivo:
 - Osnovi matematičke logike, skupovi, funkcije, brojevi
 - Osnovi programiranja, automatsko generisanje verifikovanog koda, liste, stabla, osnovi algoritama
- Detaljna dokumentacija na srpskom jeziku (Filip Marić, Sana Stojanović Đurđević, Andrija Urošević):
 - Materijali u Isabelle formatu, vežbanja, video snimci
 - Skripta u PDF formatu (oko 300 strana), podeljena po oblastima na individualne Isabelle fajlove

- Studenti sa smera Informatika (rano usmerenje ka industriji, malo matematičkih sadržaja, slabo predznanje iz logike)
- Uvođenje u oblast koristeći skup relativno jednostavnih primera (da bi se studenti brzo zainteresovali za oblast i posmatrali je kao vrstu programiranja)
- Kreiranje odgovarajućeg materijala
- Izborni kurs (broj studenata raste - 15, 30, 60)
- Studenti su od početka kursa usmereni da sami formulišu i dokazuju teoreme
- Konstruktivistički pristup nastavi približava studentima oblasti matematike i računarstva na nov i originalan način (efekat igranja igrice)

- Kreiranje skripte direktno u samom dokazivaču Isabelle (dodatni izazov za autore)
- Svako poglavlje je jedan Isabelle fajl koji se može nezavisno menjati i testirati
- <http://poincare.matf.bg.ac.rs/~sana//uidt/uidt.pdf>

- Formulisanje matematičkih tvrđenja - *u cilju učenja sintakse*
 - Tautologije
 - Silogizmi
 - Logički lavirinti
- Prirodna dedukcija - *u cilju učenja apply dokaza*
 - Logika prvog reda ($\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists$)
 - Intuicionistička i klasična logika
 - Pravila uvođenja i eliminacije veznika
 - Akcenat stavljen na postupene (korak po korak) dokaze i rad sa nebezbednim pravilima

- Dokazivanje elementarnih matematičkih tvrđenja - *u cilju učenja jezika Isar*
 - Uvođenje osnovnih šablona definisanih pravilima prirodne dedukcije
 - Relacije jednakosti skupova i podskup
- Dokazi sa osnovnim matematičkim pojmovima
 - Algebra skupova, korak po korak građenje dokaza
 - Osnovna svojstva funkcija (slika skupa funkcijom, inverzna slika)
 - Dokazi u matematičkoj logici
- Brojevi i matematička indukcija
 - Tip prirodnih brojeva, tip realnih brojeva
 - Matematička indukcija

- Definisanje novih tipova podataka i operatora nad tim tipovima
 - Građenje skupa prirodnih brojeva
 - Uvođenje tipa listi
 - Uvođenje algebarskog tipa binarnog drveta
- Verifikacija algoritama
 - Rekurzivne funkcije (stepenovanje, nzd, računanje vrednosti izraza)
 - Algoritmi sortiranja i binarna pretraga

- Formalizacija značajnog matematičkog znanja
- Veoma izazovan zadatak (prvih par godina većina studenata se posvetila olimpijadama - neočekivano)
- Kreiran je github repozitorijum (preko 60 problema formalizovanih sa rešenjima i preko 100 problema formalizovanih bez rešenja)
- Obrađene oblasti: teorija brojeva, algebra i kombinatorika. Geometrijski problemi nisu mogli da budu obrađeni.

- Formalizacija knjige: Euklidska i hiperbolička geometrija, *Zoran Lučić*
- Neophodna priprema projekta
 - Detaljna analiza knjige
 - Vremenski zahtevno
 - Neprekidno kontrolisanje projekta
- Oko 35 studenata je radilo na formalizaciji
 - Pojedinačni projekti su se sastojali od formulisanja određenog skupa aksioma i teorema, kao i dokazivanja tih teorema
 - Projekti su bili zavisni od prethodnih projekata
- Rezultati projekta:
 - Aksiome pripadnosti i njene posledice (kompletno formalizovano)
 - Aksiome rasporeda i njene posledice (formalizovano u velikoj meri; nastaju prvi problemi)
 - Aksiome podudarnosti i njene posledice (započeto; formulisano nekoliko teorema)

- Formalizacije 3 knjige: Perls of Functional Design, Abstract Algebra Theory and Applications, Topology Without Tears
- Studenti mogu da biraju knjigu
 - Veći izbor materijala za projekat
 - Međusobno nezavisni projekti
 - Lakša formulacija problema, dokazi različite težine
- U ovoj školskoj godini najviše njih je izabralo formalizaciju funkcionalnih algoritama

- Praktično savladavanje značajnih delova logike
- Upoznavanje značajnog matematičkog znanja
- Veće samopouzdanje u svoje programerske mogućnosti