

# Automatsko rezonovanje – beleške sa predavanja

## Uvod

Milan Banković (na osnovu slajdova Filipa Marića)

\*Matematički fakultet,  
Univerzitet u Beogradu

Prolećni semestar 2024/25.

# Pregled

- 1 O automatskom rezonovanju
- 2 O kursu automatskog rezonovanja

# O rezonovanju uopšte

## Šta je rezonovanje?

Rezonovanje (rasuđivanje, zaključivanje) je izvođenje **zaključaka** na osnovu datih **pretpostavki**, korišćenjem adekvatnih **argumenata**

- **argument**: pravilo logičkog rasuđivanja
- **pretpostavke**: činjenice za koje pretpostavljamo da važe
- **zaključak**: činjenica koju izvodimo odgovarajućim argumentom

## Napomena

Nauka koja se bavi proučavanjem ispravnog rezonovanja naziva se logika

## Primeri rezonovanja

Svi ljudi su smrtni.

Sokrat je čovek.

Dakle, Sokrat je smrtnan.

Svi  $X$  su  $Y$ .

$a$  je  $X$ .

Dakle,  $a$  je  $Y$

Svi prosti brojevi su parni.

7 je prost broj.

Dakle, 7 je paran.

Sva tri argumenta se smatraju logički ispravnim, bez obzira što su u trećem primeru neki iskazi netačni (pri uobičajenom tumačenju korišćenih termina).

Svi Atinjani su Grci.

Sokrat je Atinjanin.

Dakle, Sokrat je smrtnan.

Ovaj argument nije logički ispravan, bez obzira što je izvedeni iskaz tačan (pri uobičajenom tumačenju korišćenih termina).

# Formalno rezonovanje

## Formalno rezonovanje

Formalno rezonovanje podrazumeva:

- Precizno definisan **jezik** kojim se formulišu tvrđenja (pretpostavke i zaključci)
- Formalno zadat sistem **pravila** kojim se opisuju argumenti koje je dozvoljeno koristiti prilikom zaključivanja

Formalno izvođenje nekog zaključka iz datih pretpostavki konačnim nizom primena pravila naziva se **dokaz**.

## Šta ovo znači?

- Formalno rezonovanje podrazumeva simbolički jezik koji ima striktno definisanu sintaksu i semantiku
- Izvođenje zaključaka (tj. konstrukcija dokaza) se svodi na mehaničku manipulaciju simbolima prema strogo definisanim pravilima
- Ovakav pristup (ako se striktno sprovodi) onemogućava izvođenje pogrešnih zaključaka
- Formalno rezonovanje je karakteristično za oblasti u kojima je neophodna besprekorna tačnost izvedenih zaključaka, poput **matematike**

## Matematička logika

**Matematička logika** je nauka koja se bavi formalizacijom matematičkog rasuđivanja

# Automatsko rezonovanje

## Automatsko rezonovanje

**Automatsko rezonovanje** je nauka koja se bavi automatizacijom formalnog rezonovanja

## Drugim rečima...

- Sistemi formalnog rasuđivanja uključuju pravila koja omogućavaju konstrukciju dokaza, ali ne definišu **postupak** koji opisuje redosled i način primene pravila u cilju dokazivanja konkretnog, unapred zadatog tvrđenja
- Automatsko rezonovanje podrazumeva razvoj **procedura za automatsku konstrukciju dokaza** nekog tvrđenja, ili utvrđivanja da li takav dokaz postoji
- Takođe, automatsko rezonovanje može podrazumevati razvoj **procedura za automatsku proveru ispravnosti postojećih dokaza** u nekom formalnom sistemu (npr. koje je konstruisao čovek)

# Matematička logika i automatsko rezonovanje

## Pronalaženje i opravdavanje dokaza

- Matematička logika se uglavnom bavi **opravdavanjem** ispravnosti matematičkih argumenata i dokaza, dok se načini njihovog **pronalaženja** uglavnom zanemaruju i prepuštaju *intuiciji, iskustvu, ili sreći*.
- Postupci korišćeni da bi se došlo do samih dokaza često se ne prikazuju, već se prikazuje samo ono što čitaoca treba da uveri da je navedeni iskaz tačan
  - npr. dokazi u analizi koji počinju sa *neka je  $\delta < \frac{2\epsilon}{3}$*  (pitamo se „otkud baš  $\frac{2\epsilon}{3}$ ?”)
- Takođe, dokazi prikazani u knjigama su često nedovoljno precizni (predstavljaju samo „skice” dokaza, ne pokrivaju sve slučajeve i sl.)
  - ovo ostavlja mogućnost greške (ljudi su skloni previdima)
  - ljudima je veoma teško da te greške uoče u iole komplikovanijim dokazima
  - npr. štampani dokaz *Velike Fermaove teoreme* (Endrju Vajls, 1995.) je imao 129 strana
- Automatsko rezonovanje teži da proširi prethodni pogled karakterističan za matematičku logiku i da naglasak stavi na precizan **opis postupaka pronalaženja dokaza**, kao i na mogućnost **automatskog proveravanja dokaza**

# Oblasti automatskog rezonovanja

## Automatsko dokazivanje teorema

Automatsko dokazivanje teorema podrazumeva automatsku konstrukciju dokaza ili ispitivanje da li dokaz postoji, bez njegove konstrukcije.

- **problem odlučivanja**: da li dato tvrđenje važi ili ne pod datim pretpostavkama?
  - problem **verodostojnosti** dobijenog odgovora: implementacija procedure odlučivanja može sadržati greške, s obzirom da je u pitanju kompleksan softver, pa mu ne možemo apsolutno verovati
- **problem dokazivanja**: eksplicitna konstrukcija dokaza u datom formalnom sistemu, ako dokaz postoji
  - implementacije procedura dokazivanja nazivamo **dokazivačima** (engl. **prover**)
  - u slučaju jednostavnijih tvrđenja, dokaz može biti **čitljiv i čoveku**
  - u svakom slučaju, dokaz treba da bude **mašinski proveriv** (vidi sledeći slajd)

## Napomena

Teoreme koje dokazujemo na moraju biti isključivo **matematičke** – kasnije ćemo videti gde se sve automatsko dokazivanje teorema može primenjivati u praksi



# Oblasti automatskog rezonovanja

## Automatsko proveravanje dokaza

Automatsko proveravanje dokaza (utvrđivanje ispravnosti dokaza, engl. **proof checking**, **proof certification**) podrazumeva mašinsku proveru postojećeg dokaza koji je opisan u nekom unapred definisanom formalnom jeziku.

- Dokaz može biti konstruisan „ručno”, ili može biti rezultat rada nekog dokazivača teorema
- Provera ispravnosti dokaza je obično znatno jednostavniji posao od pronalaženja dokaza – zbog toga su procedure za proveru ispravnosti dokaza obično drastično jednostavnije i lakše im je verovati
- Implementacije procedura za proveru dokaza nazivamo **proveravačima** (engl. **proof checkers**)

# Oblasti automatskog rezonovanja

## Interaktivno dokazivanje teorema

Interaktivno dokazivanje teorema podrazumeva upotrebu tzv. **pomoćnika u dokazivanju** (engl. **proof assistant**):

- U pitanju su okruženja u okviru kojih čovek „ručno” izvodi dokaz u nekom formalnom sistemu
  - računarski program koji je deo okruženja automatski proverava svaki korak dokaza
  - daje korisniku uvid u stanje dokaza (tj. koje je podciljeve još potrebno dokazati i pod kojim pretpostavkama).
- Većina interaktivnih dokazivača u sebi sadrže i razne automatske metode dokazivanja koje mogu automatski dokazati mnoga jednostavna tvrđenja
  - ovo pomaže korisniku da se fokusira na globalnu strukturu dokaza, a da jednostavne poslove prepusti automatskim dokazivačima koji su deo interaktivnog okruženja
  - zato se interaktivni dokazivači teorema često nazivaju **poluautomatski dokazivači**
- Interaktivni dokazivači omogućavaju da se formalno dokažu mnoga tvrđenja koja su trenutno (ili će uvek biti) van domašaja potpuno automatskih dokazivača
  - mnoge logičke teorije su **neodlučive**, tj. nije moguće konstruisati proceduru koja će za proizvoljno zadato tvrđenje odgovoriti na pitanje da li je dokazivo ili ne
  - kod neodlučivih teorija nema drugog načina nego da ručno pokušamo da kreiramo dokaz
  - i kod odlučivih teorija procedure odlučivanja su ponekad veoma složene i neefikasne, pa je tada jedini realni pristup upotreba interaktivnih dokazivača

# Primene automatskog rezonovanja

## Gde se primenjuje automatsko rezonovanje?

- Dokazivanje teorema u matematici
  - dokazivanje nedokazanih teorema i rešavanje otvorenih problema
  - formalizacija postojećeg matematičkog znanja
- Razvoj i primena **formalnih metoda**
  - u pitanju su metode za specifikaciju, modelovanje i verifikaciju formalnih sistema, poput hardvera, softvera i kriptografskih protokola
- Rešavanje različitih problema pretrage i optimizacije
  - u pitanju su problemi čija rešenja moraju zadovoljavati unapred zadate i precizno opisane uslove
  - u logičkom smislu, uslovi se predstavljaju logičkom **formulom**, a rešenja su **modeli** te formule
  - u toku pretrage primenjuje se logičko rezonovanje u cilju sužavanja prostora pretrage
  - implementacije procedura za rešavanje ovakvih problema nazivamo **rešavačima** (engl. **solver**)
  - problemi zadovoljavanja ograničenja, problemi planiranja, kombinatorni dizajn i sl.

# Pregled

- 1 O automatskom rezonovanju
- 2 O kursu automatskog rezonovanja

# Struktura kursa

## Nastavne teme

- Iskazna logika
  - SAT rešavači i primene
- Logika prvog reda
  - Rezolucijski dokazivači i primene
  - Interaktivni dokazivači
- Logika prvog reda sa jednakošću
  - Kongruentna zatvorenja
  - Sistemi za prezapisivanje
- Teorije prvog reda
  - Procedure odlučivanja
  - SMT rešavači i primene

## Vežbe

- Simboličko izračunavanje (transformacije formula, normalne forme)
- Implementacija metoda automatskog rezonovanja
- Primene gotovih alata

# Nastava

## Nastava

- Predavanja: 2 časa (Milan Banković)
  - <http://www.matf.bg.ac.rs/~milan/?content=ar>
- Vežbe: 3 časa (Ivan Drecun)
  - <http://www.matf.bg.ac.rs/~ivan.drecun/ar.html>

# Obaveze studenata

## Obaveze studenata

Vrsta aktivnosti	maksimum	prag
Testovi i domaći zadaci	20 (10 + 10)	0
Seminarski rad	20	1
Praktični ispit	30	12
Usmeni ispit	30	12 (+ svako pitanje 25%)
<b>Ukupno</b>	<b>100</b>	<b>51</b>

# Literatura

- 1 John Harrison, *Handbook of Practical Logic and Automated Reasoning*
- 2 Predrag Janičić, *Matematička logika u računarstvu*
- 3 Alan Robinson, Andrei Voronkov, eds. *Handbook of Automated Reasoning*
- 4 Franz Baader, Tobias Nipkow, *Term rewriting and all that*
- 5 Alan Bundy, *The Computer Modelling of Mathematical Reasoning*
- 6 Armin Biere, Marijn Heule, Hans van Maaren, Toby Walsh eds. *Handbook of satisfiability*