

# Verifikovana efikasna provera dokaza nezadovoljivosti za SAT

Filip Marić

\*Matematički fakultet,  
Univerzitet u Beogradu

Seminar grupe za automatsko rezonovanje, ARGO,  
24. 11. 2010.

# SAT rešavači

- Procedure odlučivanja za **problem iskazne zadovoljivosti**.
- Ogroman **progres** u prethodne dve decenije.
- SAT rešavači dovoljno moćni za mnoge **praktične primene**:
  - Verifikacija softvera i hardvera.
  - Rešavanje kombinatornih problema.
  - Rešavanje optimizacionih problema.
  - ...

# Problem pouzdanosti

- Kritične oblasti primene (npr. verifikacija softvera i hardvera).
- Pouzdanost neophodna.
- Dva pristupa:
  - 1 Verifikacija SAT rešavača;
  - 2 Generisanje i provera sertifikata za svaku pojedinačnu formulu.

# Verifikacija SAT rešavača

Formalizacija i verifikacija samih SAT rešavača.

## Prednosti:

- Nema potrebe za zasebnim razmatranjem svake instance.
- Doprinosi boljem razumevanju rada rešavača.

## Nedostaci:

- Izuzetno kompleksan zadatak.
- Veliki broj implementacionih trikova otežava problem.
- Potrebno je prilagoditi formalizaciju pri svakoj promeni SAT algoritama.

# Provera sertifikata

Za svaku instancu, rešavač uz SAT/UNSAT odgovor generiše i **sertifikat** koji se proverava nezavisnim alatima.

- **Modeli** za zadovoljive formule - trivijalno i generisanje i provera.
- **Dokazi** za nezadovoljive formule - problematično i generisanje i provera.

# Provera sertifikata

## Prednosti:

- Lakše je realizovati od verifikacije samih rešavača.
- Nisu potrebne prevelike izmene u slučaju promene SAT algoritama.

## Nedostaci:

- Zahteva modifikaciju samih rešavača.
- Zahteva dodatno vreme za generisanje i proveru dokaza.
- Zahteva dodatan prostor za skladištenje dokaza (meri se u GB za industrijske instance).

# Vrste dokaza nezadovoljivosti

- ① **Rezolucioni dokazi** (Zhang et al., Chaff)
  - RES, RPT (Van Gelder)
- ② **Klauzalni dokazi** (Godberg i Novikov, Berkmin)
  - RUP (Van Gelder)

# Rezolucioni dokazi

Niz koraka rezolucije kojima se od početnih klauza izvodi prazna klauza.

## Prednosti:

- Trivijalna provera.

## Nedostaci:

- Nije jednostavno modifikovati SAT rešavače da ih generišu.
- Izrazito su glomazni (nekoliko GB) — ne mogu uvek da stanu u memoriju prilikom provere!
- Vreme provere je nezanemarljivo.



# Klauzalni dokazi

Niz klauza koje se uče tokom rada sat rešavača.

## Prednosti:

- Jednostavno je modifikovati SAT rešavače da ih generišu.
- Često su znatno manji nego u slučaju rezolucionih dokaza.

## Nedostaci:

- Komplikovana provera — zbog efikasnosti se moraju koristiti sofisticirani algoritmi i strukture podataka.
- Ako je softver koji ih proverava kompleksan, kako se možemo u njega pouzdati?
- Iz prethodnog razloga, ovi dokazi su odbačeni u SAT zajednici.

# Korišćenje klauzalnih dokaza

- RUP2RES — Van Gelder 2008.
- Klauzalni dokazi se prevode u rezolucione i onda proveravaju.
- Samo prevođenje ne mora da bude pouzdano jer se RES dokaz nezavisno proverava.

## Prednosti:

- Nema potrebe za komplikovanim modifikacijama SAT rešavača potrebnim za generisanje rezolucionih dokaza.

## Nedostaci:

- Vreme prevođenja iz RUP u RES je nezanemarljivo.
- Nakon prevođenja, rezolucioni dokazi ostaju izrazito glomazni.
- Vreme provere je nezanemarljivo.

# Trenutni rad

- Proveravači klauzalnih dokaza **koriste strukture podataka i algoritme korišćene u SAT rešavačima** (npr. *two-watch literal scheme*).
- **Formalizacija i verifikacija ovih struktura i algoritama je već urađena** u okviru sistema Isabelle/HOL (Marić, doktorska disertacija).
- Iskoristiti raniji rad za izgradnju **formalizovanog i verifikovanog proverача dokaza** za klauzalne dokaze.

# Problemi koje je bilo potrebno prevazići

Kako postići željeni stepen **efikasnosti**?

- Efikasnost zahteva korišćenje imperativnih struktura podataka.
- Isabelle/HOL je čisto funkcionalni jezik.
- **Imperative/HOL** paket daje ovu mogućnost.
- Nakon formalizacije u Imperative/HOL, moguće je automatski ekstrahovati izvršni SML ili Haskell kôd koji koristi imperativne strukture i postiže traženu efikasnost.

# Demo

Rad SAT rešavača i formati dokaza.

# Trivijalna rezolucija

Niz  $C_1, C_2, \dots, C$  je *trivijalna rezolucija* klauze  $C$  iz formule  $F$  akko je svaka klauza  $C_i$ :

- 1 inicijalna klauza ( $C_i \in F$ ) ili
- 2 rezolventa  $C_{i-1}$  i neke inicijalne klauze  $c$  ( $c \in F$ ),  
pri čemu se svaka varijabla rezolvira najviše jednom.

## Teorema

*Ukoliko je  $C_1, C_2, \dots, C$ , trivijalna  $C \notin F$  onda  $C_1, C_2, \dots, \overline{C}$  jediničnom propagacijom daje nezadovoljivost.*

# Trivijalna rezolucija

*Dokaz:* Pretpostavimo u  $C_1, C_2, \dots, C$  sve inicijalne klauze prethode rezolventama. Neka je  $M$  valuacija  $\bar{C}$ . Dokaz ide indukcijom po broju rezolventi.

Neka je  $C = C_k \oplus c$ , za neko  $c \in F$ . Neka je  $C_k = A \vee \neg x$  i  $c = B \vee x$ . Važi da je  $C = A \vee B$ . Pošto važi  $M \models C$ , važi i  $M \models A$  i  $M \models B$ .

- 1 U slučaju da je  $C$  jedina rezolventa, tada je  $C_k \in F$ . Zato važi  $M \vdash_{up_F} x$  i  $M \vdash_{up_F} \neg x$ , te  $M \vdash_{up_F} \perp$ .
- 2 U slučaju da ima više rezolventi, tada važi  $C_k \notin F$ . Tada se za  $C_k$  može primeniti induktivna hipoteza i važi da  $M, x \vdash_{up_f} \perp$ . Pošto zbog  $c \in F$  važi  $M \vdash_{up_f} x$ , važi i  $M \vdash_{up_f} \perp$ .