Učešće na letnjoj školi ,,SAT SMT @ MIT”

Filip Marić

Matematički fakultet,
Univerzitet u Beogradu

ARGO Seminar, jun 2011.

- Od 12. do 17. juna 2011.
- Na univerzitetu MIT (Massachusetts Institute of Technology)

- 250 učesnika
- Slajdovi javno dostupni na:
  `http://people.csail.mit.edu/vganesh/summerschool/`

Ciljevi škole

- Da bude mesto za razmenu ideja između različitih ljudi koji razvijaju i koriste SAT/SMT rešavače
- Da poveže korisnike SAT/SMT rešavača sa ljudima koji rešavače razvijaju
- Da poveže ljude koji teorijski i praktično razmatraju SAT/SMT
- Da poveže ljude koji istražuju ne-CDCL pristupe (e.g., pristupe inspirisane fizikom) sa ljudima koji koji koriste CDCL pristup
- Da ohrabri diskusije o rešavačima na više jezgara, programskim jezicima zasnovanim na rešavačima i o empirijskoj kompleksnosti

Prikaz stanja oblasti

- Škola je prikazala ono što je trenutno stanje oblasti (*state-of-the-art*) SAT/SMT tehnologija.
- Škola je bila namenjena istraživačima koji imaju neko ranije iskustvo u oblasti SAT/SMT.
- Za razliku od konferencija gde ljudi obično prikazuju ono što su radili u prethodnih najviše godinu dana, ovde su ljudi prikazivali ono što su radili u prethodnih nekoliko godina.

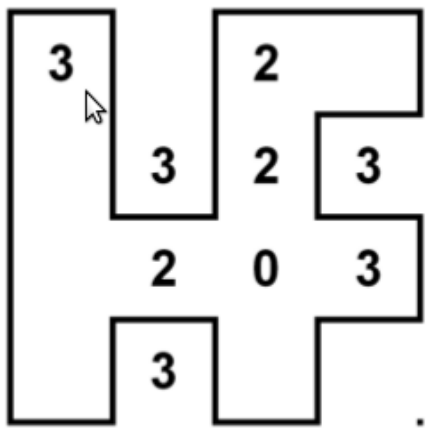
Kateogorije predavanja

1. Fundamentalni aspekti SAT/SMT rešavača
2. Opis konkretnih SAT/SMT rešavača sa naglaskom na njihovim primenama
3. Opis alata koji koriste SAT/SMT rešavače

Niklas Een

Introduction to Satisfiability Solving with Practical Applications

- Autor je tvorac čuvenog MiniSAT rešavača.
- Prezantacija je u sat vremena nabrojala i ukratko opisala skoro sve tehnike koje se koriste u okviru implementacije modernih SAT rešavača.
- Prikazana primena SAT rešavača za rešavanje raznih igrica (puzzles). Npr. SlitherLink



Albert Oliveras

SMT Theory and DPLL(T)

- Prezentacija je opisala istoriju SMT rešavača od kraja 1990-tih do danas
- Vredni i lenji pristup
- DPLL(T) shema
- Nelson-Oppen-ova shema sa kombinovanje procedura

Ed Clarke

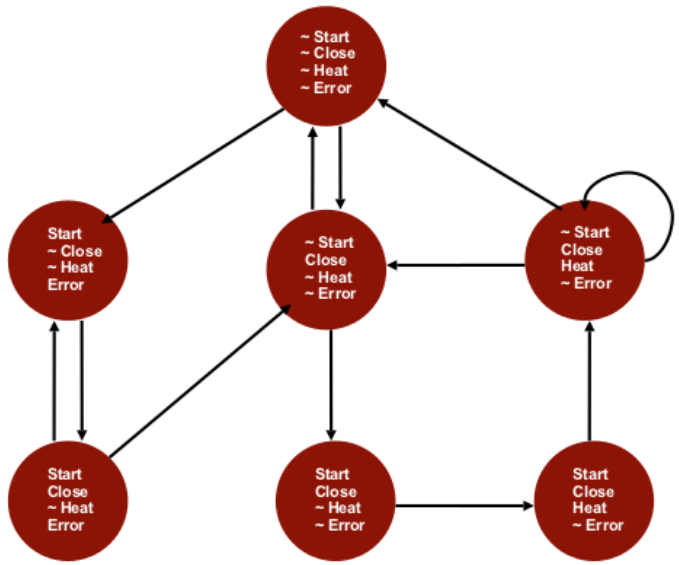
SAT Solvers for Formal Verification

- Autor je dobitnik Tjuringove nagrade 2007. za izum tehnike *model checking*.
- Dva dela prezentacije:
  1. Bounded model checking (BMC) korišćenjem SAT
  2. BMC za hibridne sisteme (kombinovanje sa numeričkim metodama)

- Sistemi se modeluju automatima (Kripke strukturama), a svojstva se zadaju LTL formulama. Npr. , mikrotalasna pećnica:

▸ The Microwave Oven Example:

$$\mathbf{AG}(start \rightarrow (\neg heat\ \mathbf{U}\ close))$$



- Automati i LTL formule se zatim kodiraju u SAT i proveravaju SAT rešavačima.

Cesare Tinelli

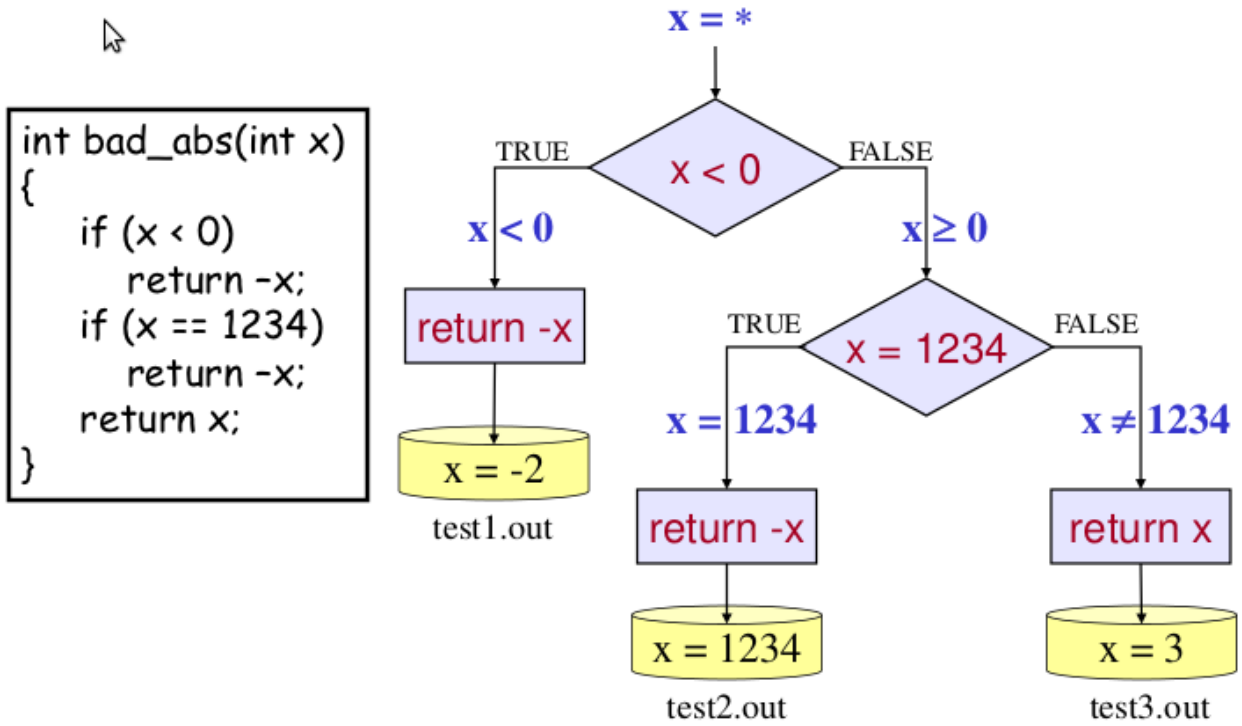
SMT-LIB Initiative

- Autor je jedan od inicijatora SMT-LIB inicijative.
- Opisan je SMT-LIB 2.0 standard.
- jSMTLIB: alat za korišćenje SMT-LIB iz Java/Eclipse okruženja
- Najave za budućnost:
  - format za dokaze
  - StarExec: mega execution service for logical systems (ne samo SMT)

Cristian Cadar

Constraint Solving Challenges in Dynamic Symbolic Execution

- Autor alata EXE i KLEE (Open Source)
- Alati na osnovu izvornog C koda generišu test ulaze kojima se postiže velika pokrivenost koda.



- Dinamičko simboličko izvršavanje (Dynamic SymEx).
- Opasne operacije (dereferenciranje NULL pokazivača, prekoračenje bafera, deljenje nulom i neispunjeni assert) se dodatno proveravaju.
- Koristi se teorija bitvektora i rešavač STP.
- Neke važne optimizacije:
  - Za nizove se koristi Abstraction/Refinement.
  - Nepotrebna ograničenja se ne dostavljaju rešavaču.
  - Keširanje upita i rezultata (slična ograničenja se javljaju na raznim granama).

Shai Ben David

Independence Results for the P vs. NP Question

- Za neke matematičke problemi koji dosta dugo nisu bili rešeni (npr. Euklidov V postulat, aksioma izbora, kontinuum hipoteza) se kasnije pokazalo da nisu ni mogli biti rešeni jer su u određenom smislu nezavisni.
- Autor je izložio rezultate nezavisnosti za problem $P \neq NP$ u odnosu na Peanovu aritmetiku.
- Pokazano je da ako je $P \neq NP$ nezavisno od Peanove aritmetike onda SAT ima ,,skoro” polinomijalne algoritme (DTIME $n^{\log n}$).

Vijay Ganesh

HAMPI: A Solver for String Theories

- Motivacija:

Primer

Pronaći nisku `s` dužine najviše 12 tako da je
`SELECT msg FROM messages WHERE topicid = s`
ispravan SQL upit koji sadrži podnisku `OR TRUE`.

- HAMPI koristi regularne izraze i kontekstno slobodne gramatike za opise sintakse dopuštenih niski.
- Nakon normalizacije, upit se svodi na teoriju bitvektora i rešava korišćenjem STP rešavača.

Leonardo De Moura, Nikolaj Bjorner

Modern SMT Solver Implementation

- Opisane različite tehnike i primene Z3 rešavača (u okviru Microsoft-a).
- Puno malih specifičnih procedura prilagođenih određenim specifičnim primenama (npr. različito naštimane procedure za aritmetiku).
- Naglasak i budući razvoj na nelinearnoj aritmetici i na teoriji kvantifikatora.
- Slajdovi nisu dostupni.

George Candea, Stefan Bucur

Parallel and Selective Symbolic Execution

- Cloud9 — masivno paralelno dinamičko simboličko izračunavanje (zasnovano na alatu KLEE). Paralelizacija omogućava da se sa nivoa jednostavnih aplikacija (npr. GNU coreutils) pređe na verifikaciju kompleksnih aplikacija (npr. apache).
- S^2E — platforma za izgradnju alata za analizu koji su ,,in vivo”. U obzir se ne uzima samo korisnički kôd već i sve biblioteke i operativni sistem. Mešavina simboličkog i konkretnog izvršavanja.
- DDT+ — Device Driver Tester
- RevNIC+ — Reverzno inženjerstvo drajvera
- PROF_s — Profajler performansi najgoreg slučaja

Karem Sakallah

CEGAR+SMT: Formal Verification of Control Logic in the Reveal System

- Potpuno automatska verifikacija kompleksnog hardvera.
- Pokazuje se ekvivalentnost neoptimizovanih i optimizovanih VERILOG specifikacija.
- CEGAR — Counter Example Guided Abstraction and Refinement.
- Ključna paradigma u mnogim primenama — naivni pristup dovodi do eksplozije broja stanja i ne skalira se dobro.

Mate Soos

CryptoMiniSat – A Rough Guide

- Pobednik SAT Race 2010.
- Rešavače deli na staru generaciju (MiniSat i slični) i novu generaciju (Lingeling i CryptoMiniSat).
- Kôd vođen mišlju ,,ideje doprinose više nego tehnički detalji”.
- Ne postoji faza pretprocesiranja — koraci koji su se primenjivali u pretprocesiranju se sada primenjuju tokom samog rešavanja.
- Puno novih heuristika i implementacionih detalja (struktura podataka) — autor nema jasnu sliku koje tehnike najviše doprinose efikasnosti.
- Autor traži saradnju zajednice u izradi ovog rešavača.
- Apstraktni opis bi dobro došao.

Youssef Hamadi

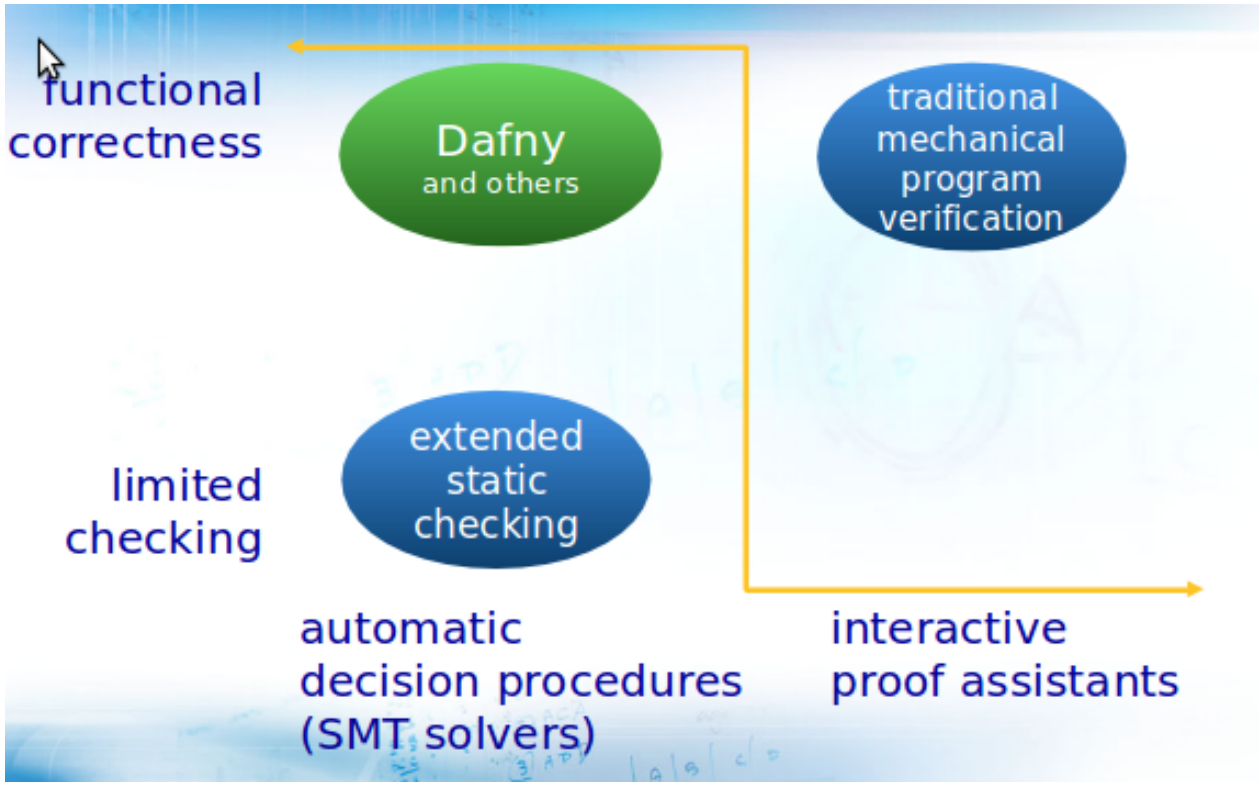
Approaches to Parallel SAT Solving

- Moderna paralelizacija se zasniva na principu ,,portfolio sa deljenjem klauza” (compete and cooperate).
- Rešavači koji ulaze u portfolio ne smeju da se previše razlikuju (kako bi mogli da uspešno sarađuju).
- Pregršt heuristika koje kontrolišu koliko i koje klauze treba deliti (ideje iz TCP congestion control)
- Deterministički Paralelni DPLL

Rustan Leino

Harnessing SMT power using the verification engine Boogie

- Alati dokazuju funkcionalnu korektnost:



- Dafny je novi jezik u kome korisnik zadaje implementaciju i uslove korektnosti.

Primer

```
method ISqrt(n: int) returns (r: int)
requires 0 <= n;
ensures r*r <= n  n < (r+1)*(r+1);
{ /* method body goes here. . . */ }
```

- Za petlje korisnik zadaje invarijante. Invarijante mogu da se navedu i za strukture podataka.
- Dafny specifikacije se prevode u Boogie i onda automatski dokazuju korišćenjem Z3 SMT rešavača.
- Dafny je veoma pogodan za primenu u nastavi.
- Kolike su mogućnosti ovakvih sistema u odnosu na klasičan (proof-assistant) pristup?

Bart Selman, Carla Gomes

Non-DPLL Approaches to Boolean SAT Solving

- Opisuje se Survey Propagation algoritam.
- Ovaj algoritam je u stanju da reši slučajni 3-SAT formule sa preko milion promenljivih oko tačke fazne tranzicije!
- Algoritam razvili fizičari.
- Zasniva se na proceni verovatnoća da neka promenljiva ima vrednost 1 ili 0 u nekom modelu (uz mnoštvo aproksimacija).

Joao Marques-Silva

MaxSAT for Optimization Problems

- Linearna optimizacija nad Bulovskim domenom:
  - Pseudo-Boolean Optimization (PBO)
  - Maximum Satisfiability (MaxSAT)
  - Weighted-Boolean Optimization (WBO)
- Primene:
  - Lokalizacija grešaka u C kodu
  - Debagovanje hardvera
  - Raspored
  - Kombinatorne aukcije