SMT tutorijal

Milan Banković
milan@matf.bg.ac.rs

Matematički fakultet

ARGO Seminar, April 2010.

Outline

Outline

Outline

Outline

Outline

Logika prvog reda

Jezik i semantika

- Logički simboli: $\top$, $\bot$, $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$, prebrojiv skup varijabli V
- Nelogički simboli: signatura $\Sigma = (\Phi, \Pi, ar)$. Funkcijski simboli arnosti nula nazivaju se konstante.
- Termovi, atomičke formule, literali, klauze, slobodne i vezane promenljive, zatvorene formule (rečenice)...
- Model: $\mathcal{M} = (D, \mathcal{I}^{\Sigma})$ određuje interpretacije funkcijskih i predikatskih simbola.
- Interpretacija termova i formula: $I(t) \in D$, $I(F) \in \{0, 1\}$
- Formula F je zadovoljiva ako postoji model u kome je tačna, a valjana ako je tačna u svim modelima.
- Logika prvog reda je neodlučiva.

Teorije prvog reda

Deduktivna definicija

- Teorija $\mathcal{T}$ je definisana rekurzivnim skupom aksioma $\mathcal{A}$
- Rečenica A je teorema teorije $\mathcal{T}$ ako pripada deduktivnom zatvorenju $DC(\mathcal{A})$
- Ako je $\mathcal{A}$ skup aksioma teorije $\mathcal{T}$, pisaćemo $\mathcal{A} = Ax(\mathcal{T})$

Semantička definicija

- Teorija $\mathcal{T}$ je definisana skupom modela
- Rečenica A je valjana u teoriji $\mathcal{T}$ ako je tačna u svim njenim modelima

Zadovoljivost u teoriji (SMT)

Definicija

- Formula A je zadovoljiva u teoriji $\mathcal{T}$ (ili $\mathcal{T}$-zadovoljiva) ako je formula $\mathrm{Ax}(\mathcal{T}) \wedge A$ zadovoljiva u logici prvog reda.
- Problem ispitivanja zadovoljivosti u teoriji se naziva SMT problem (engl. Satisfiability Modulo Theory)
- SMT problem je u opštem slučaju neodlučiv
- Postoje odlučive teorije kao i odlučivi fragmenti neodlučivih teorija
- Procedure odlučivanja za (odlučive) SMT probleme zovu se SMT rešavači (solveri)

Zadovoljivost u teoriji (SMT)

Kvantifikatori i SMT

- Egzistencijalni kvantifikatori: skolemizacija
- Univerzalni kvantifikatori: problem ??
- Postoje teorije koje dopuštaju eliminaciju kvantifikatora
- Uglavnom razmatramo SMT probleme za bazne formule (bez kvantifikatora). Ovo umanjuje opštost ali je u praksi često dovoljno za izražavanje problema od interesa

Zadovoljivost u teoriji (SMT)

Primene SMT-a

- Verifikacija softvera i hardvera
- Problemi raspoređivanja
- Optimizacioni problemi

Outline

Prazna jednakosna teorija (EUF)

Definicija

- Signature svih teorija koje proučavamo sadrže binarni predikatski simbol $=$ (jednakost) koji se interpretira kao refleksivna, simetrična i tranzitivna relacija kongruentna sa svim funkcijama i relacijama kojima se interpretiraju ostali simboli u signaturi. Ovakve teorije zovu se jednakosne teorije.
- Signatura prazne jednakosne teorije (Equality with Uninterpreted Functions) osim jednakosti sadrži još i proizvoljan skup funkcijskih simbola čije interpretacije nisu fiksirane ni na koji način osim što moraju biti saglasne sa aksiomama jednakosti (ovo su jedine aksiome teorije)
- Fragment EUF-a bez kvantifikatora je odlučiv. Procedure odlučivanja su obično zasnovane na kongruentnim zatvorenjima

Realna aritmetika (RA)

Definicija

- Signatura: $0, 1, +, \cdot, -, =, \leq$
- Aksiome: Aksiome jednakosti + uobičajene aksiome polja realnih brojeva
- Teorija je odlučiva
- Njen fragment je linearna realna aritmetika (LRA) koja je odlučiva u 2-eksponencijalnom vremenu. Fragment LRA bez kvantifikatora odlučiv je u polinomijalnom vremenu

Celobrojna aritmetika (IA)

Definicija

- Signatura: $0, 1, +, \cdot, -, =, \leq$
- Teorija je zadata semantički (skup svih rečenica koje su tačne u uobičajenoj strukturi celih brojeva)
- Teorija je neodlučiva
- Njen fragment je linearna celobrojna aritmetika (LIA) koja je odlučiva u 2-eksponencijalnom vremenu. Fragment LIA bez kvantifikatora odlučiv je i NP-kompletan

Teorija nizova

Definicija

- Signatura: $=$, funkcijski simboli read, write
- Aksiome:
  - $(\forall a)(\forall i)(\forall v)(read(write(a, i, v), i) = v)$
  - $(\forall a)(\forall i)(\forall j)(\forall v)(\neg(i = j) \Rightarrow read(write(a, i, v), j) = read(a, j))$
- Teorija je neodlučiva, ali je njen fragment bez kvantifikatora odlučiv i NP-kompletan
- Primena: verifikacija softvera

Outline

SMT i SAT

SMT i SAT

- U oblasti SAT rešavača postignut je fantastičan napredak u prethodnim godinama
- Moderni SMT rešavači se zato obično oslanjaju na SAT rešavače kako bi iskoristili njihove dobre osobine
- U praksi postoje dva pristupa – gramzivi i lenji pristup

Gramzivi pristup

Opis

- Formula se transformiše u ekvizadovoljivu iskaznu formulu koja se predaje SAT rešavaču
- Gube se informacije specifične za datu teoriju
- Dobijena iskazna formula može biti veoma velika

Lenji pristup

Opis

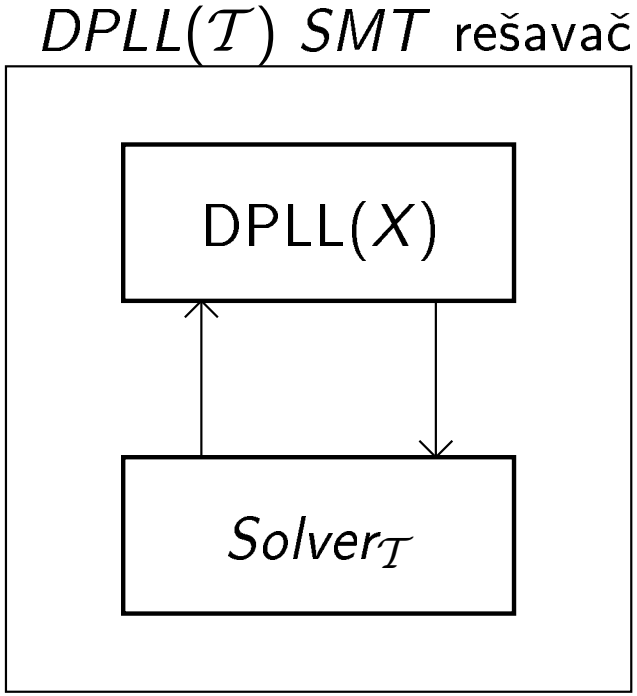
- Vrši se iskazna apstrakcija baznih atomičkih formula – iste se zamenjuju iskaznim promenljivama čime se dobija iskazna formula
- Data formula se predaje SAT rešavaču koji pronalazi iskazni model (ako postoji)
- Nađeni iskazni model (posmatran kao konjukcija literala) se predaje specifičnoj proceduri odlučivanja koja proverava njegovu zadovoljivost u datoj teoriji
- Omogućava korišćenje posebnih procedura odlučivanja koje su prilagođene teoriji, istovremeno koristeći dobre osobine SAT rešavača

DPLL($\mathcal{T}$)

Opis

- DPLL($\mathcal{T}$) je jedna od široko prihvaćenih arhitektura SMT rešavača zasnovanih na lenjom pristupu
- Autori: Robert Nieuwenhuis, Albert Oliveras (Technical University of Catalonia, Barcelona), Cesare Tinelli (University of Iowa)
- Implementacija grupe iz Barselone – BarcelogicTools
- Sastoji se iz DPLL-zasnovanog SAT rešavača (označenog sa DPLL(X)) i procedure odlučivanja za specifičnu teoriju od interesa (teorijski rešavač ili $\mathcal{T}$-rešavač, označen sa $Solver_{\mathcal{T}}$) koji ispituje zadovoljivost konjukcije literala u datoj teoriji

DPLL($\mathcal{T}$)



Struktura

- SMT rešavač ima modularnu strukturu, komponente su jasno odvojene i komuniciraju preko precizno definisanog interfejsa.
- Ovakva arhitektura omogućava da se teorijski rešavač lako zameni rešavačem za neku drugu teoriju, bez ikakvih promena u SAT rešavaču.
- $DPLL(X) + Solver_{\mathcal{T}} = DPLL(\mathcal{T})$

DPLL(X)

DPLL(X) – prošireni DPLL

- DPLL(X) implementira nerekurzivnu adaptaciju DPLL procedure uobičajenu za moderne SAT rešavače
- Stanje (F, M, C): F je skup klauza čija se zadovoljivost ispituje, M je skup literala organizovan u vidu steka (parcijalni model), C je konfliktni skup (u slučaju da konflikt postoji)
- Pravilo: definiše način na koji se menja stanje i uslove pod kojim se može primeniti
- Inkrementalna izgradnja parcijalnog modela: `UnitPropagate` i `Decide` pravila
- Detekcija i analiza konflikata: `Conflict` i `Explain` pravila
- Učenje klauza: `Learn` pravilo
- Nehronološki backtracking: `Backjump` pravilo
- DPLL(X) proširuje skup pravila DPLL-a uvođenjem pravila za rezonovanje u okviru teorije (`TheoryPropagate`, `TheoryConflict`, `TheoryExplain`)

$Solver_{\mathcal{T}}$

Zahtevana funkcionalnost

- Ispituje da li je $M \vDash_{\mathcal{T}} \bot$ (detekcija konflikta). Svojstvo inkrementalnosti.
- Ako jeste $M \vDash_{\mathcal{T}} \bot$, tada pronalazi (što je moguće manji) skup $E \subset M$, takav da $E \vDash_{\mathcal{T}} \bot$ (objašnjenje konflikta)
- Ispituje da li postoji literal $l \notin M$ takav da $M \vDash_{\mathcal{T}} l$ (teorijska propagacija)
- Pronalazi (što je moguće manji) skup $E \subset M^{\prec l}$ takav da $E \vDash_{\mathcal{T}} l$ (objašnjenje propagacije)
- Biva obavešten od strane DPLL(X)-a o dodavanju novih literala u M, kao i o backtracking-u. Mora da omogući vraćanje u prethodno stanje prilikom backtracking-a.

Outline

Argo grupa i SMT

Prethodni rad

- ArgoSAT SAT solver – Filip Marić, Predrag Janičić
- ArgoLib SMT rešavač (nad ArgoSAT-om) – Filip Marić, Predrag Janičić (rešavači za teorije EUF i LRA)
- Rešavač za teoriju `alldifferent` – Milan Banković, Filip Marić

alldifferent rešavač

Opis

- Globalno ograničenje alldifferent$(x_1, \ldots, x_n)$ zahteva da varijable $x_1, \ldots, x_n$ (nad konačnim domenima) imaju međusobno različite vrednosti
- Ovo ograničenje je izraženo u okviru teorije prvog reda
- Implementiran je teorijski rešavač zasnovan na uparivanju u bipartitnim grafovima (Régin-ov algoritam)
- Procedura je proširena potpuno novim algoritmom za generisanje objašnjenja konflikata i propagacija. Algoritam je zasnovan na obilasku usmerenog grafa, i izvršava se u linearnom vremenu. Dokazana je korektnost algoritma
- Prototipska implementacija je integrisana sa ArgoSAT-om. Testirana je na Sudoku instancama dimenzije 5 (25 x 25) i postignuti su ohrabrujući rezultati

Budući rad – ArgoSMT

Opis

- DPLL($\mathcal{T}$)-zasnovan SMT rešavač, modularnog dizajna, otvorenog koda
- Kombinacija teorija (Nelson-Oppen vs. DTC)
- Paralelizacija (multi-threaded)
- Izjednačavanje iskaznog rezonovanja sa ostalim teorijama
- Paralelizacija SAT-a
- Implementacija procedura odlučivanja za najznačajnije teorije