Automatsko rezonovanje – beleške sa predavanja Teorije prvog reda i SMT

Milan Banković

*Matematički fakultet,
Univerzitet u Beogradu

Proletnji semestar 2018.

Pregled

Višesortna logika prvog reda

Motivacija

- Uobičajena definicija logike prvog reda podrazumeva jedinstven domen (univerzum) iz koga se uzimaju vrednosti kojima se interpretiraju svi termovi
- Dakle, svi izrazi su ili termovi ili formule, pri čemu se svi termovi interpretiraju elementima iz tog jedinstvenog domena, dok se formule interpretiraju kao tačne ili netačne
- Ovakva definicija onemogućava razlikovanje tipova
- U mnogim primenama, poželjno je razlikovati tipove (npr. ako semantiku nekog programa opisujemo u okviru logike prvog reda, želimo da razlikujemo npr. izraze tipa `int` od izraza tipa `double`).
- Dakle, poželjno je termove razlikovati po sortama, pri čemu za svaku sortu termova postoji poseban domen iz koga se uzimaju vrednosti
- Ovakav logički okvir se naziva višesortna logika prvog reda

Sintaksa

Signatura $\Sigma = (\mathcal{S}, \mathcal{F}, r)$

- Skup sorti $\mathcal{S}$ (među kojima je i `Bool`)
- Skup funkcijskih simbola $\mathcal{F}$ (među kojima su i $\top$, $\bot$, $\wedge$, $\vee$, $\neg$ ...)
- Funkcija ranga $r : \mathcal{F} \longrightarrow \mathcal{S}^* \times \mathcal{S}$
- $r(f) = [s_1, \ldots, s_n] \longrightarrow s$ ($s_1, \ldots, s_n$ su sorte argumenata, a s je povratna sorta)
- $r(a) = [\,] \longrightarrow s$ (a je simbol konstante sorte s)
- Za svaku sortu $s \in \mathcal{S}$, skup promenljivih V^s

Izrazi

- Svaki izraz e ima svoju sortu s
- Simbol konstante a ranga $[\,] \longrightarrow s$ je izraz sorte s
- Promenljiva $x \in V^s$ je izraz sorte s
- Ako je t_i izraz sorte s_i $(i = 1, \ldots, n)$ i $r(f) = [s_1, \ldots, s_n] \longrightarrow s$, tada je $f(t_1, \ldots, t_n)$ izraz sorte s
- Izraze sorte `Bool` zovemo formulama, a ostale izraze termovima
- Iskazni simboli imaju uobičajene rangove: $r(\bot) = r(\top) = [\,] \longrightarrow \texttt{Bool}$, $r(\neg) = [\texttt{Bool}] \longrightarrow \texttt{Bool}$, $r(\wedge) = [\texttt{Bool}, \texttt{Bool}] \longrightarrow \texttt{Bool}$, ...
- Simbol jednakosti: $r(=_s) = [s, s] \longrightarrow \texttt{Bool}$ za svaku sortu $s \in \mathcal{S}$
- Promenljive se u formulama mogu kvantifikovati: $(\forall x : \sigma).F$ ili $(\exists x : \sigma).F$, gde je x promenljiva sorte σ, a F je formula

Semantika

Σ-struktura $\mathcal{L} = (\mathcal{D}, \_^{\mathcal{L}})$

- $\mathcal{D} = \{D^s \mid s \in \mathcal{S}\}$: skup domena (za svaku sortu s po jedan)
- $D^{\texttt{Bool}} = \{0, 1\}$: domen sorte `Bool` je uvek $\{0, 1\}$
- $a^{\mathcal{L}} \in D^s$ $(r(a) = [\,] \longrightarrow s)$: konstanta sorte s uzima vrednost iz D^s
- $f^{\mathcal{L}} : D^{s_1} \times \ldots \times D^{s_n} \longrightarrow D^s$ $(r(f) = [s_1, \ldots, s_n] \longrightarrow s)$
- Uobičajeno značenje iskaznih simbola: $\bot^{\mathcal{L}} = 0$, $\top^{\mathcal{L}} = 1$, $\neg^{\mathcal{L}}(x) = 1$ akko je $x = 0$, $\wedge^{\mathcal{L}}(x, y) = 1$ akko $x = 1$ i $y = 1$, ...
- $=_s^{\mathcal{L}}$ $(x, y) = 1$ akko su x i y isti element skupa D^s

Interpretacija

- Valuacija $v : V^s \longrightarrow D^s$ (za svako $s \in \mathcal{S}$)
- $x \in V^s$: $I_v^{\mathcal{L}}(x) = v(x)$
- $r(a) = [\,] \longrightarrow s$: $I_v^{\mathcal{L}}(a) = a^{\mathcal{L}}$
- $r(f) = [s_1, \ldots, s_n] \longrightarrow s$: $I_v^{\mathcal{L}}(f(t_1, \ldots, t_n)) = f^{\mathcal{L}}(I_v^{\mathcal{L}}(t_1), \ldots, I_v^{\mathcal{L}}(t_n))$
- $I_v^{\mathcal{L}}((\forall x : \sigma).F) = 1$ akko $I_{v'}^{\mathcal{L}}(F) = 1$ za svako v' $(v'(y) = v(y)$ za $y \neq x)$
- $I_v^{\mathcal{L}}((\exists x : \sigma).F) = 1$ akko $I_{v'}^{\mathcal{L}}(F) = 1$ za neko v' $(v'(y) = v(y)$ za $y \neq x)$
- Interpretacija zatvorenih formula (rečenica) ne zavisi od v $(I_v^{\mathcal{L}}(F) = I^{\mathcal{L}}(F))$

Semantika – nastavak

Osnovne semantičke pojmove definišemo na uobičajen način

- $\mathcal{L} \models F$: zatvorena formula F je tačna u Σ-strukturi $\mathcal{L}$ ($I^{\mathcal{L}}(F) = 1$)
- Zadovoljiva formula: postoji Σ-struktura $\mathcal{L}$ takva da je $\mathcal{L} \models F$
- $\models F$: valjana formula (tačna u svim Σ-strukturama)
- $\Delta \models F$: logička posledica (tačna kad god su tačne sve formule iz Δ)
- $F_1 \equiv F_2$: logička ekvivalencija ($F_1 \models F_2$ i $F_2 \models F_1$)
- $F \models \bot$: nezadovoljiva (negacija $\neg F$ je valjana formula)

Napomene

Napomene

- Višesortna logika tretira sve simbole na uniforman način
- Sorta `Bool` je samo jedna od sorti (fiksiranog značenja)
- Predikatski simboli su prosto funkcijski simboli koji vraćaju `Bool`
- Iskazni simboli $\top$, $\bot$, $\neg$, $\wedge$, $\vee$, ... su samo funkcijski simboli nad `Bool` sortom i sa fiksiranim značenjem

Izražajnost

- Višesortna logika prvog reda nema veću izražajnost od uobičajene logike prvog reda bez sorti
- Za svaku Σ-strukturu $\mathcal{L}$ (u smislu višesortne logike) smo u standardnoj logici prvog reda mogli uzeti strukturu čiji je univerzum unija domena svih sorti iz $\mathcal{L}$
- Postojanje više sorti se sada može simulirati dodatnim unarnim predikatskim simbolima p^s koji se interpretiraju kao odgovarajući podskupovi univerzuma koji odgovaraju domenima pojedinih sorti $s \in \mathcal{L}$

Pregled

Dedukcija – podsećanje

Dedukcioni sistem

- Pravila izvođenja oblika: $\frac{P_1,\ldots,P_n}{Q}$
- Aksiome: tvrđenja koja se ne dokazuju
- Dokaz: izvođenje primenom pravila (u vidu niza ili stabla)
- $\Delta \vdash F$: F je dokaziva iz Δ (i aksioma)
- $\vdash F$: F je teorema, tj. dokaziva bez dodatnih pretpostavki (samo iz aksioma)
- Saglasnost: ako $\Delta \vdash F$, onda $\Delta \models F$
- Potpunost: ako $\Delta \models F$, onda $\Delta \vdash F$
- Potpuni i saglasni sistemi: Hilbertov sistem, prirodna dedukcija, račun sekvenata

Teorija prvog reda

Definicija teorije prvog reda

- Teorija $\mathcal{T}$ nad signaturom Σ zadata skupom aksioma $Ax(\mathcal{T})$ je skup svih formula F takvih da je $Ax(\mathcal{T}) \vdash F$
- Formule $F \in \mathcal{T}$ zovemo teoremama teorije $\mathcal{T}$ (u oznaci $\vdash_{\mathcal{T}} F$)
- Deduktivna posledica u teoriji (u oznaci $\Delta \vdash_{\mathcal{T}} F$): $Ax(\mathcal{T}) \cup \Delta \vdash F$
- Model teorije: struktura $\mathcal{L}$ u kojoj su sve formule iz $Ax(\mathcal{T})$ tačne
- Formula F je valjana u teoriji $\mathcal{T}$ ($\mathcal{T}$-valjana, u oznaci $\vDash_{\mathcal{T}} F$) ako je tačna u svim njenim modelima, tj. ako je $Ax(\mathcal{T}) \vDash F$
- Formula je zadovoljiva u teoriji $\mathcal{T}$ ($\mathcal{T}$-zadovoljiva) ako je tačna u bar jednom modelu teorije $\mathcal{T}$, tj. ako je $Ax(\mathcal{T}) \cup \{F\}$ zadovoljiv skup formula
- Logička posledica u teoriji (u oznaci $\Delta \vDash_{\mathcal{T}} F$): F je tačna u svim modelima teorije $\mathcal{T}$ u kojima su tačne sve formule iz Δ, tj. važi $Ax(\mathcal{T}) \cup \Delta \vDash F$

Teorija prvog reda

Veza između deduktivnih i semantičkih pojmova

Pod pretpostavkom da je deduktivni sistem koji razmatramo potpun i saglasan, važi:

- $\vdash_{\mathcal{T}} F$ akko $Ax(\mathcal{T}) \vdash F$ akko $Ax(\mathcal{T}) \models F$ akko $\models_{\mathcal{T}} F$
- $\Delta \vdash_{\mathcal{T}} F$ akko $Ax(\mathcal{T}) \cup \Delta \vdash F$ akko $Ax(\mathcal{T}) \cup \Delta \models F$ akko $\Delta \models_{\mathcal{T}} F$
- Rečenica F je $\mathcal{T}$-zadovoljiva akko nije $\models_{\mathcal{T}} \neg F$ tj. akko nije $\vdash_{\mathcal{T}} \neg F$

Teorija prvog reda

Osobine teorije prvog reda

- Za teoriju kažemo da je aksiomatska ako je zadata skupom aksioma $Ax(\mathcal{T})$ koji je rekurzivan (odlučiv)
- Za teoriju kažemo da je potpuna ako za svaku rečenicu A važi ili $\vdash_{\mathcal{T}} A$ ili $\vdash_{\mathcal{T}} \neg A$
- Za teoriju kažemo da je konzistentna ako ni za jednu rečenicu A ne važi istovremeno i $\vdash_{\mathcal{T}} A$ i $\vdash_{\mathcal{T}} \neg A$
- Za teoriju kažemo da je odlučiva ako postoji efektivan postupak koji za svaku rečenicu A u konačnom broju koraka ispituje da li je $\vdash_{\mathcal{T}} A$ ili ne

Teorija prvog reda

Mogu se dokazati sledeće važne činjenice

- Teorija je konzistentna akko ima model
- Za svaku konzistentnu teoriju koja ima bar jedan beskonačan model postoje modeli koji su neizomorfni (posledica Skolem-Lovenhajmove teoreme)
- Drugim rečima, u logici prvog reda se ne može formulisati konzistentna teorija koja ima tačno jedan model (do na izomorfizam). Za to su nam potrebne moćnije logike (poput logike drugog reda)
- Teorija je potpuna akko su joj svi modeli međusobno elementarno ekvivalentni (tj. za svaku rečenicu F važi da je F tačna u jednom modelu akko je tačna u drugom i obratno)
- Potpuna teorija je odlučiva akko je aksiomatska
- Problem ispitivanja $\mathcal{T}$-zadovoljivosti formule F je odlučiv akko je teorija odlučiva u smislu prethodne definicije

Pregled

SMT problem i SMT rešavači

SMT problem

- SMT problem (engl. Satisfiability Modulo Theory) za teoriju $\mathcal{T}$ je problem ispitivanja $\mathcal{T}$-zadovoljivosti date formule F
- Odlučivost SMT problema zavisi od izbora teorije $\mathcal{T}$
- Za pojedine teorije, SMT problem je odlučiv samo za neke fragmente (formule određenog oblika)

SMT rešavači

- Softverski alati koji implementiraju procedure odlučivanja (za odlučive SMT probleme) zovu se SMT rešavači
- Relativno nova tehnologija (početak 21. veka)
- SAT tehnologija + procedure odlučivanja (lenji pristup)
- Primene: verifikacija softvera i hardvera, problemi zadovoljavanja ograničenja

Kvantifikatori i SMT

Kvantifikatori

- Egzistencijalni kvantifikatori: skolemizacija
- Univerzalne kvantifikatore nije uvek moguće ukloniti
- Neke teorije dopuštaju eliminaciju kvantifikatora
- Istanciranje kvantifikatora je jedna od tehnika za tretman univerzalnih kvantifikatora
- SMT problem za bazne formule – najčešći slučaj

Pregled

EUF teorija

EUF teorija

- Equality with Uninterpreted Functions
- Nema drugih predikatskih simbola osim jednakosti (svi atomi su oblika $u = v$)
- Signatura može saržati proizvoljan broj sorti i funkcijskih simbola koji se mogu potpuno slobodno interpretirati (neinterpretirani simboli i sorte)
- Modeli teorije su svi (normalni) modeli (prazan skup aksioma)
- SMT problem za ovu teoriju je neodlučiv
- SMT problem za bazni fragment ove teorije (u oznaci QF_UF) je odlučiv
- Zadovoljivost konjunkcije baznih literala ove teorije je odlučiv u polinomijalnom vremenu (procedure zasnovane na kongruentnim zatvorenjima, poput Nelson-Openove procedure)

Realna aritmetika

Realna aritmetika

- Signatura: sorta `Real`, simboli $0, 1, +, \cdot, -, /, \leq$
- Aksiome: realna zatvorena polja
- Standardni model: struktura realnih brojeva $\mathbb{R}$
- Teorija je odlučiva (eliminacijom kvantifikatora)
- Bazni linearni fragment (u oznaci QF_LRA)
- Problem ispitivanja zadovoljivosti konjunkcije linearnih baznih literala je odlučiv u polinomijalnom vremenu
- Neke od procedura odlučivanja (eksponencijalne složenosti) su Furije-Mockinova procedura (zasnovana na eliminaciji kvantifikatora) i Simpleks procedura

Celobrojna aritmetika

Celobrojna aritmetika

- Signatura: sorta `Int`, simboli $0, 1, +, \cdot, -, \leq$
- Aksiome: Peanove aksiome (prvog reda)
- Standardni model: struktura celih brojeva $\mathbb{Z}$
- Teorija je neodlučiva
- Njen linearni fragment (Presburgerova aritmetika) je odlučiv
- Bazni linearni fragment (QF_LIA)
- Problem ispitivanja zadovoljivosti konjunkcije linearnih baznih literala je odlučiv i NP-kompletan

Teorija nizova

Teorija nizova

- Signatura: sorte `Index`, `Value` i `Array`, simboli
  - $select : [\texttt{Array}, \texttt{Index}] \longrightarrow \texttt{Value}$
  - $store : [\texttt{Array}, \texttt{Index}, \texttt{Value}] \longrightarrow \texttt{Array}$
- Aksiome:
  - $(\forall x)(\forall y)(\forall z)(select(store(x, y, z), y) = z)$
  - $(\forall x)(\forall y_1)(\forall y_2)(\forall z)(y_1 \neq y_2 \Rightarrow select(store(x, y_1, z), y_2) = select(x, y_2))$
  - $(\forall x_1)(\forall x_2)((\forall y)(select(x_1, y) = select(x_2, y)) \Rightarrow x_1 = x_2)$
- Teorija je neodlučiva u opštem slučaju
- Bazni fragment teorije (QF_AX) je odlučiv
- Problem ispitivanja zadovoljivosti konjunkcije baznih literala je NP-kompletan

Teorija bitvektora

Teorija bitvektora

- Signatura: sorte $\texttt{BitVec}_n$ ($n \in \mathbb{N}$), simboli:
  - $bvnot_n, bvneg_n : [\texttt{BitVec}_n] \longrightarrow \texttt{BitVec}_n$
  - $bvadd_n, bvshl_n, \ldots : [\texttt{BitVec}_n, \texttt{BitVec}_n] \longrightarrow \texttt{BitVec}_n$
  - $bvult_n, bvslt_n, \ldots : [\texttt{BitVec}_n, \texttt{BitVec}_n] \longrightarrow \texttt{Bool}$
- Standardni model: hardverska aritmetika
- Teorija je odlučiva
- Bazni fragment QF_BV
- Problem ispitivanja zadovoljivosti konjunkcije baznih literala je NP-kompletan

Pregled

Lenji pristup

Lenji pristup

- Iskazna apstrakcija: atomi prvog reda se zamenjuju iskaznim slovima
- SAT rešavač ispituje zadovoljivost dobijene iskazne formule
- Zadovoljavajuća iskazna valuacija određuje konjunkciju baznih literala
- Posebna procedura odlučivanja proverava zadovoljivost dobijene konjunkcije baznih literala u teoriji
- Rezultat: efikasnost pretrage SAT rešavača + procedure odlučivanja prilagođene teoriji
- ,,Lenja DNF transformacija”

DPLL($\mathcal{T}$)

DPLL($\mathcal{T}$) (Nievenhuis, Oliveras, Tineli (2006))

- Najčešće korišćena arhitektura zasnovana na lenjom pristupu
- DPLL zasnovan SAT rešavač + $\mathcal{T}$-rešavač
- SAT rešavač: inkrementalno konstruiše zadovoljavajuće iskazne valuacije
- $\mathcal{T}$-rešavač: ispituje zadovoljivost odgovarajuće konjunkcije literala prvog reda u teoriji $\mathcal{T}$ *u toku konstrukcije* zadovoljavajuće valuacije
- Mogućnost rezonovanja *unapred* u teoriji (teorijske propagacije)

DPLL($\mathcal{T}$)

DPLL(X) – sistem zasnovan na pravilima

- Implementira klasičan CDCL zasnovan SAT rešavač proširen dodatnim pravilima za rezonovanje u teoriji
- Stanje (F, M, C): F skup klauza, M je stek literala (parcijalna valuacija), C je konfliktni skup (ili no_cflt ako nema konflikta)
- Pravilo: definiše način promene stanja, kao i uslove pod kojima se može primeniti
- Grananje, jedinična propagacija, analiza konflikata i nehronološko vraćanje unazad
- Dodatno: teorijske propagacije i konflikti

Funkcionalnost $\mathcal{T}$-rešavača

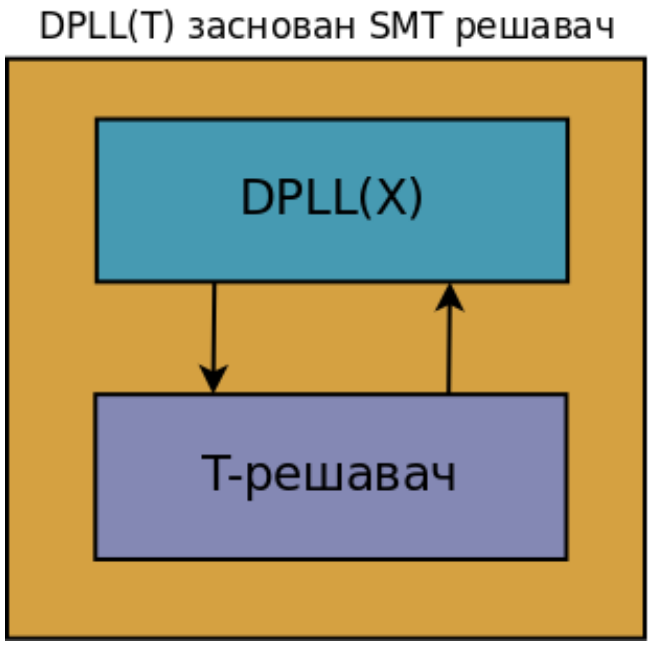
Obavezna funkcionalnost

- da može da utvrdi da li je konjunkcija literala na steku zadovoljiva u teoriji
- da može da konstruiše objašnjenje konflikta ($R \subset M$ takav da je $R \models_{\mathcal{T}} \bot$)

Poželjna funkcionalnost

- da može da vrši teorijske propagacije i generiše njihova objašnjenja ($R \subset M$ takav da je $R \models_{\mathcal{T}} l$, gde je l propagirani literal)
- inkrementalnost (mogućnost efikasne provere zadovoljivosti u slučaju dodavanja novih literala u konjunkciju bez pokretanja celog postupka iz početka)
- efikasna rekonstrukcija prethodnog stanja (za potrebe vraćanja unazad)

DPLL($\mathcal{T}$)



Struktura

- SMT rešavač ima modularnu strukturu, komponente su jasno odvojene i komuniciraju putem precizno definisanog interfejsa
- ovakva arhitektura omogućava da se $\mathcal{T}$-rešavač zameni $\mathcal{T}'$-rešavačem za neku drugu teoriju $\mathcal{T}'$ bez ikakvih promena na SAT rešavaču
- $DPLL(X) + \mathcal{T}$-rešavač $= DPLL(\mathcal{T})$

Primer interfejsa teorijskog rešavača

Interfejs procedure

- *newLevel*() – uspostavljanje novog nivoa odlučivanja
- *backtrack*(m) – vraćanje unazad na nivo m
- *assert*(l) – dodavanje literala l na stek
- *checkConflict*(E) – provera konflikta u teoriji
- *checkPropagate*(L) – detekcija teorijskih propagacija
- *explainLiteral*(l, E) – objašnjavanje propagiranog literala

Pregled

SMT-LIB

SMT-LIB

- Poznati SMT rešavači: Z3, Yices, CVC, MathSAT, OpenSMT, BarcelogicTools
- Cilj SMT-LIB inicijative: bolja koordinacija u razvoju i lakše poređenje SMT rešavača
- Standard SMT-LIB (tekuća verzija 2.6): ulazno-izlazni jezik, logički okvir, teorije
- Veliki skup instanci za testiranje i poređenje
- `http://smtlib.cs.uiowa.edu/`