Automatsko rezonovanje
Verifikacija Hardvera svođenjem na SAT
Miloš Nikolić 1097/2021

Da bismo hardverski sistem sveli na problem iskazne logike potrebno je da određeni tranzicioni sistem prevedemo na jezik iskazne logike koji će dalje biti prosleđen SAT rešavaču.
Tranzicioni sistemi:

U ovom primeru želeo bih da ilustrujem kako se prevodi jedan trocifreni binarni brojač na problem SAT.

Tranzicioni sistem ima 9 stanja: (S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8)

Relacija prelaska je definisana sa: R(S0,S1), R(S1,S2), R(S2,S3), R(S3,S4), R(S4, S5), R(S5, S6), R(S6, S7), R(S7,S8)

inkrementiranjem brojaca (0,0,0)→(0,0,1), (0,0,1)→(0,1,0), (0,1,0)→(0,1,1), (0,1,1)→(1,0,0),(1,0,0)→(1,0,1), (1,0,1)→(1,1,0), (1,1,0)→(1,1,1)

Invarijantnost je I(S0,S8)

Prevođenje na SAT

naš problem se može iskazati sledećom formulom:

R(S0,S1) ∧ R(S1,S2) ∧ … ∧ R(S7,S8) => I(S0,S8)

Negiramo našu formulu I tražimo da nam SAT rešavac prijavi UNSAT, odnosno da je naša formula nezadovoljiva, to je dokaz da je početna formula tautologija I da je naš hardver ispravan.

Negiranjem početne formule i eliminacijom implikacije dobijamo sledeću formulu:

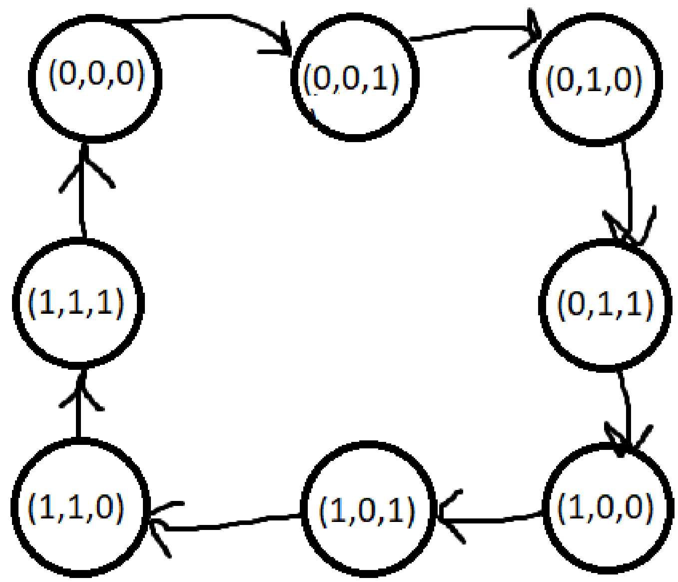
R(S0,S1) ∧ … ∧ R(S7,S8) ∧ ¬I(S0, S8)

Napomena: Da postoji neki pocetni uslov njega bismo dodali na pocetak konjunkcije kao I_0.

Opis stanja

Suštinski problem jeste kako opisati našu relaciju prelaska I invarijantnost pomoću iskazne logike

Relacija prelaska, je data na slici



Relacija prelaska

Svaki prelazak je opisan sa tri iskazna slova (p,q,r) tako da nasa relacija glasi

$$R(S_i, S_{i+1}) \Leftrightarrow (p_i, q_i, r_i) \rightarrow (p_{i+1}, q_{i+1}, r_{i+1})$$

Tablica prelaska

P_i	Q_i	R_i	P_{i+1}	Q_{i+1}	R_{i+1}
0	0	0	0	0	1
0	0	1	0	1	0
0	1	0	0	1	1
0	1	1	1	0	0
1	0	0	1	0	1
1	0	1	1	1	0
1	1	0	1	1	1
1	1	1	0	0	0

Neke zakonitosti je lako videti npr R_i <=> $\neg R_{i+1}$, a neke su teže uočljive,

Q_{i+1} <=> $Q_i \sim R_i$

(gde ~ predstavlja ekskluzivnu disjunkciju)

P_{i+1} <=> $P_i \sim (Q_i \& R_i)$

Sada je problem pronaći konjunktivnu normalnu formu (CNF)

Invarijantnost,
I(Si, Sj) je logički ekvivalentno sa

(Pi <=> Pj) & (Qi <=>Qj) & (Ri <=>Rj)

pošto je nama potrebna negacija invarijantnosti

¬I(Si, Sj) je logički ekvivalentno sa
¬(Pi <=> Pj) ∨ ¬(Si <=>Sj) ∨ ¬(Ri <=> Rj)

u konjunktivnoj normalnoj formi ova formula je ekvivalentna sa:

(Pi ∨ Pj ∨ Qi ∨ Qj ∨ Ri ∨ Rj) ∧ (Pi ∨ Pj ∨ Qi ∨ Qj ∨ ¬Ri ∨ ¬Rj) ∧ (Pi ∨ Pj ∨ ¬Qi ∨ ¬Qj ∨ Ri ∨ Rj) ∧ (Pi ∨ Pj ∨ ¬Qi ∨ ¬Qj ∨ ¬Ri ∨ ¬Rj) ∧ (¬Pi ∨ ¬Pj ∨ Qi ∨ Qj ∨ Ri ∨ Rj) ∧ (¬Pi ∨ ¬Pj ∨ Qi ∨ Qj ∨ ¬Ri ∨ ¬Rj) ∧ (¬Pi ∨ ¬Pj ∨ ¬Qi ∨ ¬Qj ∨ Ri ∨ Rj) ∧ (¬Pi ∨ ¬Pj ∨ ¬Qi ∨ ¬Qj ∨ ¬Ri ∨ ¬Rj)

R_i <=> $\neg R_{i+1}$

u konjunktivnoj normalnoj formi ova formula je logički ekvivalentna sa

(Ri ∨ ¬Rj) ∧ (¬Ri ∨ Rj)

Q_{i+1} <=> $Q_i \sim R_i$
u konjunktivnoj normalnoj formi ova formula je logički ekvivalentna sa

(¬Qi+1 ∨ Qi ∨ Ri) ∧ (¬Qi+1 ∨ ¬Qi ∨ ¬Ri) ∧ (Qi+1 ∨ Qi ∨ ¬Ri) ∧ (Qi+1 ∨ ¬Qi ∨ Ri)

Pi+1 <=> Pi ~(Qi & Ri)
u konjunktivnoj normalnoj formi ova formula je ekvivaletna formuli

(Pi+1 ∨ ¬Pi ∨ Qi) ∧ (Pi+1 ∨ ¬Pi ∨ Ri) ∧ (Pi+1 ∨ Pi ∨ ¬Qi ∨ ¬Ri) ∧ (¬Pi+1 ∨ Pi ∨ Qi) ∧ (¬Pi+1 ∨ Pi ∨ Ri) ∧ (¬Pi+1 ∨ ¬Pi ∨ ¬Qi ∨ ¬Ri)

Sada imamo ceo iskaz u konjunktivnoj normalnoj formi I možemo ga proslediti programu koji će na osnovu ulaza generisati izlaz u DIMACS formi, koja je neophodna za ulaz u SAT rešavač.

Tehnički detalji

prevodjenje programa: g++ 1.cpp

pokretanje programa: ./a.out | minisat