

Opis sistema

Opis problema

U okviru kursa „Konstrukcija Kompilatora“ je napravljen projekat koji podrazumeva skup transformacija koje mogu da se primene na odgovarajuće delove koda, ali tako da se semantika samom programu ne promeni tj. program mora i dalje da vrati isti rezultat. Prime transformacije je zamena *while* petlje sa *for* petljom, odmotavanje petlje itd.

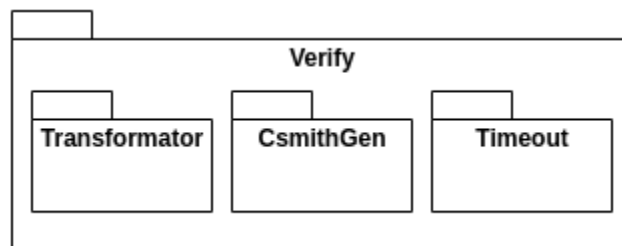
U okviru kursa „Verifikacija softvera“ je napravljena nadogradnja projekta sa ciljem da se podigne pouzdanost transformacija. Takođe je obogaćen skup mogućih transformacija. Za povećanje pouzdanosti se koristi tehnika metamorfnog testiranja, gde se generiše veliki broj nasumičnih programa na koje se primenjuju transformacije i testira se da li imaju identičan rezultat (i da li se novodobijeni kod prevodi).

Opis arhitekture sistema

Pregled tehnologija:

- Transformacije su pisane u C++-u uz korišćenje *Clang* biblioteke.
- Za generisanje nasumičnih C programa se koristi CSmith. Generisani programi se postprocesiraju i verifikuju kroz Python.
- Metamorfno testiranje (proces koji objedinjuje sve delove) se vrši kroz Python.

Pogled kompozicije



Pogled kompozicije visokog nivoa apstrakcije

Timeout

Python modul koji omogućava pokretanje sporednih procesa sa postavljenim tajmerom koji prekida proces kada istekne vreme. Funkcije su specijalizovane za rešavanje problema zombi procesa na Linux operativnom sistemu prilikom planiranog ili neplaniranog naglog prekidanja programa. Ovaj modul je nezavisno testiran i upotrebljiv u sličnim situacijama.

CsmithGen

Python modul koji služi za generisanje programa korišćenjem CSmith alata (okvir za alat). Clang biblioteka ne podržava rad sa tipovima u programima koji su generisani, zbog čega se ti tipovi u postprocesiranju zamenjuju sa tipovi sa kojim može da radi. Takođe, svi programi koji se generišu se završavaju u konačnom vremenu tj. nijedan program nema beskonačnu petlju. Provera da li program sigurno nema beskonačnu petlju se vrši korišćenjem **Timeout** modula.

Transformator

Transformator klasa apstrahuje cmake build za biblioteku za transformacije i primenu tih transformacija nad generisanim C Programima. Omogućava različite izbore načina primene transformacija (fleksibilna klasa) i proveru da li semantika programa ostaje ista nakon primenjene sekvence transformacija. Smatra se da je program promenio semantiku ako važi jedno od:

- Transformisan program daje drugačiji rezultat od inicijalnog.
- Transformisan program se ne prevodi.
- Transformisan program ima grešku pri izvršavanju.
- Transformisan program ima beskonačnu petlju (tačnije, izvršava se mnogo dugo u odnosu na inicijalni program).

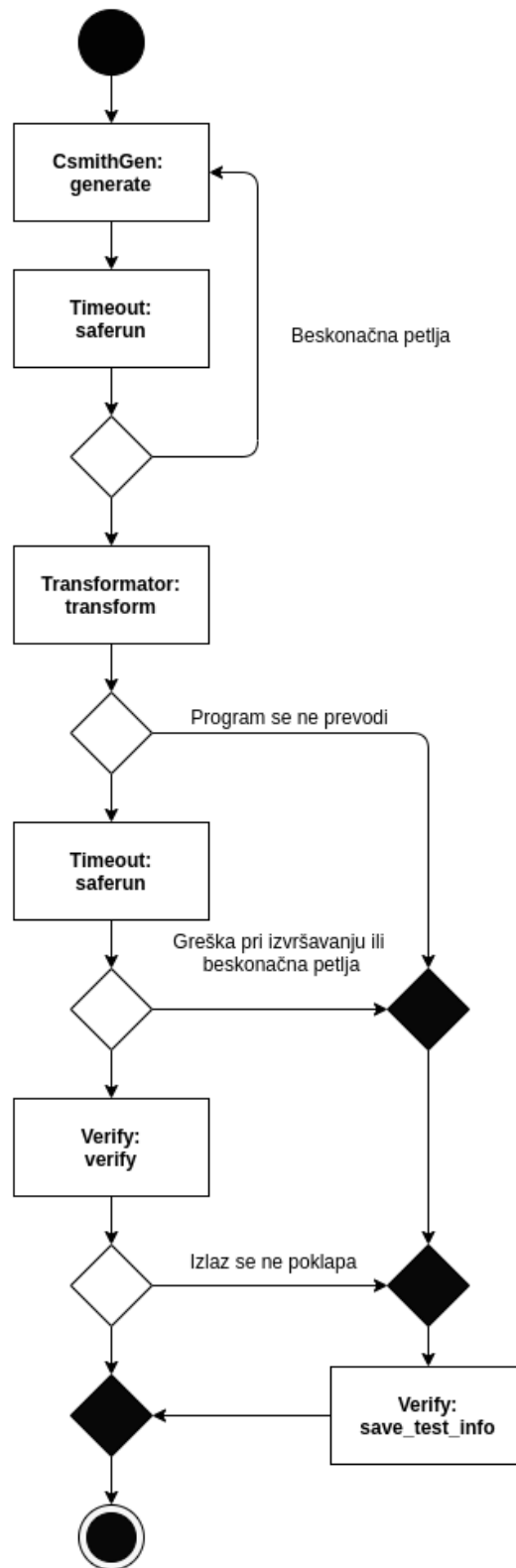
Verify

Modul koji objedinjuje proces generisanje programa, transformaciju programa i verifikaciju transformisanih programa korišćenjem CsmithGen i Transformator.

Pregled zavisnosti

	Timeout	CsmithGen	Transformator	Verify
Timeout				
CsmithGen				
Transformator				
Verify				

Pogled aktivnosti



Svaka iteracija podrazumeva generisanje C programa preko `csmith` alata. Alat generise nasumični C kod (koji ne mora da se završava). Izlaz iz ovog programa je suma koji je izračunata nizom nekih nasumičnih operacija. Ukoliko se kod sigurno uspešno završava (ovo se proverava prevođenjem i pokretanjem), onda se izvršava niz transformacija nad kodom. Nakon toga se transformisani C kod prevodi i pokreće opet. Ukoliko se kod uspešno prevodi i daje identičan izlaz, onda se smatra da je test prošao. U suprotnom je test pao i čuva se u odgovarajućem direktorijumu direktorijumu.