Model Checking is Static Analysis

Fuyuan Zhang <fuzh@imm.dtu.dk> Piotr Filipiuk <pifi@imm.dtu.dk>
Language Based Technology, DTU Informatics

Model Checking

mu-calculus

ACTL

CTL

Formula in ALPF

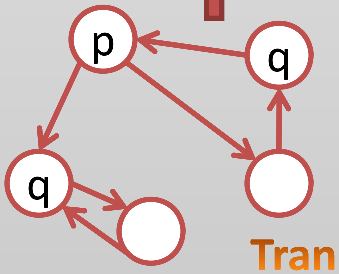
$$AF(p \vee q)$$

$$[\forall s:[\forall s':\neg T(s,s') \vee R_{AF(p\vee q)}(s')] \Rightarrow R_{AF(p\vee q)}(s)]$$

$$[\forall s: R_{(p\vee q)}(s) \Rightarrow R_{AF(p\vee q)}(s)]$$

$$[\forall s: P_q(s) \Rightarrow R_q(s)]$$

$$[\forall s: P_p(s) \Rightarrow R_p(s)]$$



Transition systems

- Transition systems and temporal logic formulas are encoded in ALFP.
- Transition relations and labeling information are defined in the initial model.
- For each subformula of the given temporal logic formula, we create a relation approximating the set of states that satisfy the subformula.
- The constraints of these relations are specified by ALFP formulas and matches the semantics of temporal logic

- Starting from the initial model, Succinct Solver calculates the least model of ALFP constraints
- The existence of least model is guaranteed by Moore Family property of ALFP formulas
- In the case of Model Checking, the least model equals the solution of model checking

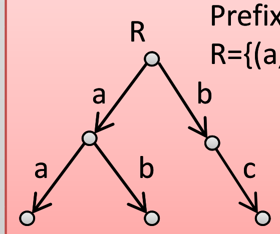
…

BDD based solver

Differential solver

Prefix trees:

R={(a,b),(a,a),(b,c)}



The least model for ALFP constraints

Static Analysis

π-calculus

λ -calculus

WHILE language

Reaching Definitions:

init(1) & flow(1,2) & … &
gen(1,x,1) & gen(4,y,4) &… &
kill(1,x,?) & kill(1,x,1) & … &
<RD specification>

WHILE programs

```
[x:=1]^1;
while [x<10]^2 do
      [x:=x+1]^3;
[y:=x+2]^4;
```

- Control Flow Graph and transfer functions are encoded in ALFP.
- The Reaching Definitions constraints are specified by ALFP clauses.
- We create a relation that for each program point approximates the possible place where a given variable may have been last assigned at (e.g. rd(2,x,1) means that at label 2 variable x, was last assigned at label 1).