Model Checking, SS2011: Exercise Sheet 5

May 17, 2011

Note. Let us denote (integer) linear arithmetic formulas by F, φ_A and φ_B.

Exercise 5.1. Prove or refute each of the following propositions.

$$(\exists x'.\mathrm{F} \wedge x = x') \equiv \exists x'.\mathrm{F}[x'/x] \tag{1}$$

$$(\exists x'.\mathrm{F} \wedge x = x') \equiv \exists x'.\mathrm{F}[x/x'] \tag{2}$$

Exercise 5.2. Give an interpolant for each pair of formulas.

1. $\varphi_A := (x \geq z \wedge z > y + 1)$, $\varphi_B := (x + 1 \leq y)$
2. $\varphi_A := (x - y = 0 \wedge y + y \geq 1)$, $\varphi_B := (x \leq 0)$
3. $\varphi_A := (x = 1 \vee x > 0 \wedge z > 1)$, $\varphi_B := (x > 1)$
4. $\varphi_A := (z + 2 \leq x \wedge x + 1 \leq y - 3)$, $\varphi_B := (y > 0 \vee z > 0)$
5. $\varphi_A := (z + 2 \leq x \wedge x + 1 \leq y - 3 \wedge z + 2 \geq 4)$, $\varphi_B := (y > 8 \vee z < 0)$

Exercise 5.3. Let the programs given in exercises 3.3 and 3.4 be $P_{3.3}$ and $P_{3.4}$. Execute the Abstract Rechability (AR) algorithm on those programs. Use the function *more* as abstraction function, and the sets of predicates $\mathit{Preds}_{3.3} = \{pc = l_{init}, x \leq y, \perp, x \leq y + 1, x > y\}$ and $\mathit{Preds}_{3.4} = \{pc = l_1, \perp, x - 1 \geq y, pc = l_{exit}, pc = l_{err}\}$ for $P_{3.3}$ and $P_{3.4}$.

Exercise 5.4. Consider the following source code fragment.

```
assume(y <= z);
while(x > y) x--;
assert(x <= z);
```

A corresponding program for the fragment is $P = (X,\ pc,\ T,\ \varphi_{init},\ \varphi_{err})$ where

- $X = \{x, y, z\}$
- $T = \{\rho_1, \ldots, \rho_5\}$

- $\varphi_{init} = (pc = l_1)$
- $\varphi_{err} = (pc = l_5)$
- $\rho_1 = (pc = l_1 \wedge pc' = l_2 \wedge y \leq z \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_2 = (pc = l_2 \wedge pc' = l_2 \wedge x > y \wedge x' = x - 1 \wedge y' = y \wedge z' = z)$
- $\rho_3 = (pc = l_2 \wedge pc' = l_3 \wedge x \leq y \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_4 = (pc = l_3 \wedge pc' = l_4 \wedge x \leq z \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_5 = (pc = l_3 \wedge pc' = l_5 \wedge x > z \wedge x' = x \wedge y' = y \wedge z' = z)$

Give a set of predicates for the abstraction function *more* such that the AR algorithm gives a set formulas *AbstReach* such that

$$\neg \exists x, y, z, pc. (\bigvee \mathit{AbstReach}) \wedge \varphi_{err}$$

Exercise 5.5. Draw the reachability tree denoted by the output of AR in exercise 5.4.