Model Checking, SS2011: Exercise Sheet 3

May 13, 2011

Note. Let us denote (integer) linear arithmetic formulas by F and G.

Exercise 3.1. Consider the definiton of the *more* function.

$$\mathit{more}(\mathrm{F}) = \bigwedge\{\mathrm{G} \in \mathit{Predicates} \mid \mathrm{F} \models \mathrm{G}\}$$

Let $\mathit{Predicates} = \{x \geq 0, x+5 > y, z < x, y \geq x, z \leq y, z < y, y > x\}$. Compute the result of applying *more* to the following formulas.

1. $x = 1 \vee x > 0 \wedge z > 1$
2. $x + 3 > y + 4 \wedge z \geq 0$
3. $z + 2 \leq x \wedge x + 1 \leq y - 3$
4. $\exists z. x \leq z - 1 \wedge y \geq z + 1$
5. $x - 2 < y + 3 \wedge x + 1 \leq z \vee y \leq z - 1 \wedge x + 1 \leq y$

Exercise 3.2. Prove that the symbolic *post* operator distributes over disjunction, i.e. prove that the following proposition holds.

$$\mathit{post}(\rho, \mathrm{F} \vee \mathrm{G}) \equiv \mathit{post}(\rho, \mathrm{F}) \vee \mathit{post}(\rho, \mathrm{G})$$

Exercise 3.3. Consider the following source code fragment.

```
assume(x <= y);
while (x <= y) x++;
```

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

- $X = \{x, y\}$
- $T = \{\rho_0, \ldots, \rho_2\}$
- $\varphi_{init} = (pc = l_{init})$

- $\varphi_{err} = (pc = l_{err})$
- $\rho_0 = (pc = l_{init} \land pc' = l_1 \land x \leq y \land x' = x \land y' = y)$
- $\rho_1 = (pc = l_1 \land pc' = l_1 \land x \leq y \land x' = x + 1 \land y' = y)$
- $\rho_2 = (pc = l_1 \land pc' = l_{exit} \land x \geq y + 1 \land x' = x \land y' = y)$

Argue why the Forward-Symbolic-Reachability (FSR) algorithm does not terminate on P.

Exercise 3.4. Consider the following source code fragment.

```
while (x <= y) x++;
assert(x >= y + 1);
```

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

- $X = \{x, y\}$
- $T = \{\rho_1, \ldots, \rho_4\}$
- $\varphi_{init} = (pc = l_1)$
- $\varphi_{err} = (pc = l_{err})$
- $\rho_1 = (pc = l_1 \land pc' = l_1 \land x' = x + 1 \land y' = y)$
- $\rho_2 = (pc = l_1 \land pc' = l_2 \land x > y \land x' = x \land y' = y)$
- $\rho_3 = (pc = l_2 \land pc' = l_{exit} \land x \geq y + 1 \land x' = x \land y' = y)$
- $\rho_4 = (pc = l_2 \land pc' = l_{err} \land x < y + 1 \land x' = x \land y' = y)$

Does FSR terminate on P? In that case, is the assertion in the source code violated?