Model Checking, SS2011: Exercise Sheet 4

May 16, 2011

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

Exercise 4.1. Prove that the symbolic *post* operator distributes over disjunction on its first parameter, i.e. prove that the following proposition holds.

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

Exercise 4.2. Execute the Abstract Rechability (AR) algorithm on the program program $P = (X,\ pc,\ T,\ \varphi_{init},\ \varphi_{err})$ where

- $X = \{x, y, z\}$
- $T = \{\rho_1, \ldots, \rho_5\}$
- $\varphi_{init} = (pc = l_1)$
- $\varphi_{err} = (pc = l_5)$
- $\rho_1 = (pc = l_1 \wedge pc' = l_2 \wedge y \geq z \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_2 = (pc = l_2 \wedge pc' = l_2 \wedge x < y \wedge x' = x + 1 \wedge y' = y \wedge z' = z)$
- $\rho_3 = (pc = l_2 \wedge pc' = l_3 \wedge x \geq y \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_4 = (pc = l_3 \wedge pc' = l_4 \wedge x \geq z \wedge x' = x \wedge y' = y \wedge z' = z)$
- $\rho_5 = (pc = l_3 \wedge pc' = l_5 \wedge x < z \wedge x' = x \wedge y' = y \wedge z' = z)$

Use the function *more* as abstraction function, and the set of predicates $Preds = \{pc = l_1, \ldots, pc = l_5, \bot, y \geq z, x \geq z\}$.

Exercise 4.3. (Optional) Use the output of AR in exercise 4.2 to show that the program P is correct, i.e. show that $\neg \exists x, y, z, pc. (\bigvee AbstReach) \wedge \varphi_{err}$.

Exercise 4.4. (Optional) Draw the reachability tree denoted by the output of AR in exercise 4.2.