Prof. Dr. Andreas Podelski
Matthias Heizmann

7.12.2011
Submission: 13.12.2011
at the beginning of the lecture

Tutorials for Program Verification
Exercise sheet 7

Exercise 1: Quantifier Elimination — 2+1 points

(a) Let $\phi \in \mathsf{Form}$ be a formula and t be a term that does not contain x. Prove that the formula $\exists x = t \wedge \phi$ is equivalent to the formula $\phi[t/x]$.

(b) State a formula that does not contain any quantifiers and is equivalent to the following formula.

$$\exists x''.\ \exists y''.\quad x'' \geq 0 \wedge y'' = 0 \wedge (x = x'' + 1 \vee x = x'' \wedge y = y'')$$

Exercise 2: Post-condition Function — 4 points

We say that post distributes over the connective $\odot$ wrt. the first argument if the following equation holds.

$$post(\phi_1 \odot \phi_2, \rho) = post(\phi_1, \rho) \odot post(\phi_2, \rho)$$

We say that post distributes over the connective $\odot$ wrt. the second argument if the following equation holds.

$$post(\phi, \rho_1 \odot \rho_2) = post(\phi, \rho_1) \odot post(\phi, \rho_2)$$

- Determine for $\odot \in \{\wedge, \vee, \rightarrow\}$ if *post* distributes over $\odot$ wrt. the first argument or wrt. the second argument.
- Does *post* distribute over negation wrt. the first argument or wrt. the second argument?

Give a proof for each positive answer, give a counterexample for each negative answer.

Exercise 3: Reachability Analysis 1+2 points

Consider again the program from Exercise 2 of the fifth exercise sheet.

$$
\begin{array}{rl}
0: & x := i; \\
1: & y := j; \\
2: & \textbf{while } x \neq 0 \textbf{ do } \{ \\
3: & \quad x := x - 1 \\
4: & \quad y := y - 1 \\
5: & \} \\
6: & assert(i = j \rightarrow y = 0)
\end{array}
$$

(a) State a formal definition of this program in the notation that was introduced in the lecture on Monday 28th November, where a program is given as a tuple

$$P = (V, pc, \varphi_{init}, R, \varphi_{err}).$$

(b) Compute the set of reachable states.

Exercise 4: Pre-condition Function 1 point

Let V be a tuple of program variables. Let ϕ be a set of states (i.e., ϕ is a formula whose free variables are in V). Let ρ be a binary relation over program states (i.e., ρ is a formula whose free variables are in $V \cup V'$).

In the lecture the formula $post(\phi, \rho)$ was defined as image of the set ϕ under the relation ρ. Define a function wp such that the formula $wp(\phi, \rho)$ denotes the preimage of the set ϕ under the relation ρ.