Prof. Dr. Andreas Podelski
Dr. Matthias Heizmann

Preference deadline: June 14, 2017
Discussion: June 18, 2018

Tutorial for Program Verification
Exercise Sheet 7

Exercise 1: Weakest precondition 2 Points

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 we defined the formula $post(\phi, \rho)$ as the image of the set ϕ under the relation ρ.

(a) Define a function wp such that the formula $wp(\phi, \rho)$ denotes the largest set of states ψ such that $post(\psi, \rho)$ is a subset of ϕ.

(b) Compute $wp(\phi_i, \rho_i)$ for the following pairs.

$$\phi_1 \equiv y \geq 7 \qquad \rho_1 \equiv x < y \land x' = x \land y' = y$$
$$\phi_2 \equiv y = 7 \land x = 23 \qquad \rho_2 \equiv x' = x + y + 3 \land y' = y$$
$$\phi_3 \equiv y \geq 7 \land x = 23 \qquad \rho_3 \equiv y' = y$$

Note that this exercise is very similar to Exercise 5 on Sheet 6, which was not yet discussed in the exercise group. In contrast to the old exercise, the formula ϕ_2 in part (b) is $y = 7 \land x = 23$ instead of $y \geq 7$.

Exercise 2: Reachable states 2 Points

Compute the set of reachable states for the program below.

$$P = (V, pc, \varphi_{init}, \mathcal{R}, \varphi_{err})$$
$$V = (pc, x, y, i, j)$$
$$\mathcal{L} = \{\ell_0, \ell_1, \ell_2, \ell_3, \ell_4, \ell_6, \ell_{\mathrm{ex}}, \ell_{\mathrm{err}}\}$$
$$\varphi_{init} \equiv pc = \ell_0 \land i = 2 \land j = 2$$
$$\varphi_{err} \equiv pc = \ell_{\mathrm{err}}$$
$$\mathcal{R} = \{\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7, \rho_8\}$$
$$\rho_1 \equiv move(\ell_0, \ell_1) \land x' = i \land skip(i, y, j)$$
$$\rho_2 \equiv move(\ell_1, \ell_2) \land y' = j \land skip(x, i, j)$$
$$\rho_3 \equiv move(\ell_2, \ell_3) \land x \neq 0 \land skip(x, i, y, j)$$
$$\rho_4 \equiv move(\ell_2, \ell_6) \land x = 0 \land skip(x, i, y, j)$$
$$\rho_5 \equiv move(\ell_3, \ell_4) \land x' = x - 1 \land skip(i, y, j)$$
$$\rho_6 \equiv move(\ell_4, \ell_2) \land y' = y - 1 \land skip(x, i, j)$$
$$\rho_7 \equiv move(\ell_6, \ell_{\mathrm{ex}}) \land (i = j \to y = 0) \land skip(x, i, y, j)$$
$$\rho_8 \equiv move(\ell_6, \ell_{\mathrm{err}}) \land \neg(i = j \to y = 0) \land skip(x, i, y, j)$$