Prof. Dr. Andreas Podelski
Dr. Matthias Heizmann

Preference deadline: June 21, 2017
Discussion: June 25, 2017

Tutorial for Program Verification
Exercise Sheet 8

Exercise 1: Havoc 1 Point

We define the transition relation for the guarded command **havoc** x as follows.

$$\rho_{\mathbf{havoc}(x)} :\equiv skip(V \setminus \{x\}) \equiv \bigwedge_{y \in V,\, y \neq x} y' = y.$$

(a) Show that $wp(\varphi \wedge x = 0, \rho_{\mathbf{havoc}(x)}) \equiv \mathit{false}$ for any formula φ.

(b) Let $\varphi_{x=0}$ be a formula that contains $x = 0$ as a subformula.
Show that $wp(\varphi_{x=0}, \rho_{\mathbf{havoc}(x)}) \equiv \mathit{false}$ does not hold in general.

Recall that $wp(\varphi, \rho) \equiv \forall V'.\, \rho \rightarrow \varphi[V'/V]$.

Exercise 2: Weakest precondition and strongest postcondition 1 Point

Let φ and ψ be arbitrary predicates and ρ be a transition relation.
Give a counterexample for each of the following statements if it does not hold.

(a) $\varphi = wp(\psi, \rho) \iff post(\varphi, \rho) = \psi$

(b) $\varphi \subseteq wp(\psi, \rho) \iff post(\varphi, \rho) \subseteq \psi$

(c) $\varphi \supseteq wp(\psi, \rho) \iff post(\varphi, \rho) \supseteq \psi$

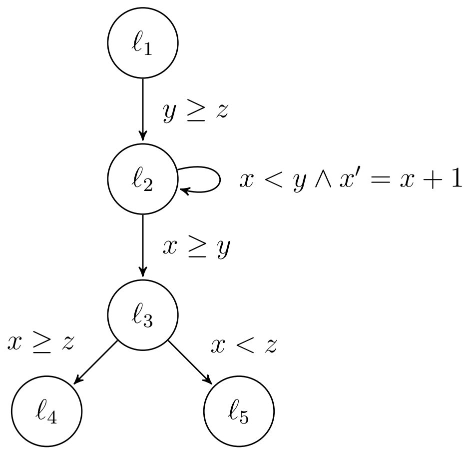
Exercise 3: Inductive invariants 2 Points

Consider the following program from the lecture

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

where the tuple of program variables V is (pc, x, y, z), the inital condition φ_{init} is $pc = \ell_1$, the error condition φ_{err} is $pc = \ell_5$, and the set of transition relations $\mathcal{R}$ contains the following transitions.

$$\rho_1 = (move(\ell_1, \ell_2) \wedge y \geq z \wedge skip(x, y, z))$$
$$\rho_2 = (move(\ell_2, \ell_2) \wedge x < y \wedge x' = x + 1 \wedge skip(y, z))$$
$$\rho_3 = (move(\ell_2, \ell_3) \wedge x \geq y \wedge skip(x, y, z))$$
$$\rho_4 = (move(\ell_3, \ell_4) \wedge x \geq z \wedge skip(x, y, z))$$
$$\rho_5 = (move(\ell_3, \ell_5) \wedge x < z \wedge skip(x, y, z))$$



(a) Is the complement of φ_{err} an inductive invariant? If not, give a counterexample.

(b) What is the weakest[1] inductive invariant that is contained in the complement of φ_{err} (i.e., disjoint from φ_{err})?

(c) Describe a (possibly non-terminating) algorithm to construct the weakest inductive invariant that is contained in the complement of φ_{err} (for any program that is safe).
Hint: Eliminate states that can reach an error state.

[1] A formula φ is weaker than a formula ψ if ψ implies φ. An inductive invariant φ is the weakest inductive invariant if φ is implied by all other inductive invariants.