Prof. Dr. Andreas Podelski
Dr. Matthias Heizmann
Christian Schilling

Preference deadline: June 18, 2017
Discussion: June 20, 2017

Tutorial for Program Verification
Exercise Sheet 7

Exercise 1: Havoc 1 Point

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

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

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

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

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

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) $\varphi = \mathit{wp}(\psi, \rho) \iff \mathit{post}(\varphi, \rho) = \psi$

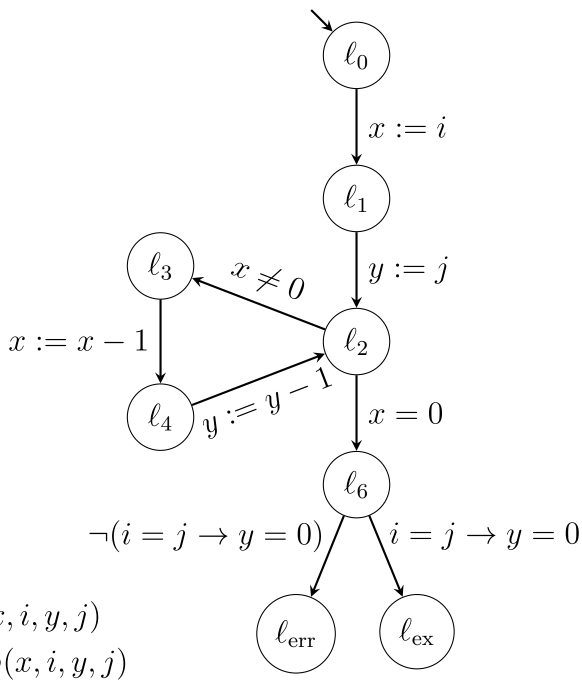
(b) $\varphi \subseteq \mathit{wp}(\psi, \rho) \iff \mathit{post}(\varphi, \rho) \subseteq \psi$

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

Exercise 3: Reachable states 2 Points

Compute the set of reachable states for the program below. Note that we changed φ_{init}.

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



Exercise 4: 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.

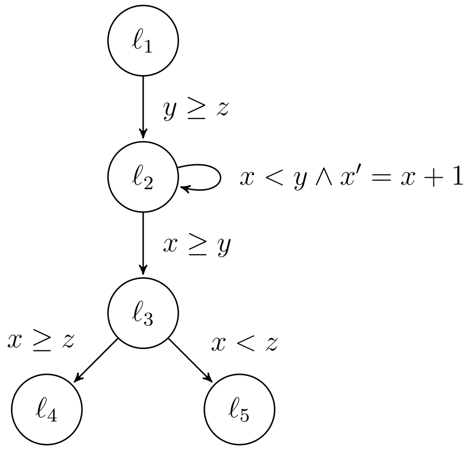
$\rho_1 = (move(\ell_1, \ell_2) \wedge y \geq z \wedge skip(x, y, z))$

$\rho_2 = (move(\ell_2, \ell_2) \wedge x + 1 \leq y \wedge x' = x + 1 \wedge skip(y, z))$

$\rho_3 = (move(\ell_2, \ell_3) \wedge x \geq y \wedge skip(x, y, z))$

$\rho_4 = (move(\ell_3, \ell_4) \wedge x \geq z \wedge skip(x, y, z))$

$\rho_5 = (move(\ell_3, \ell_5) \wedge x + 1 \leq z \wedge skip(x, y, z))$



(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.