Exercise 1: Havoc

We define the transition relation for the guarded command \texttt{havoc} \( x \) as follows.

\[ \rho_{\text{havoc}}(x) \equiv \text{skip}(V \setminus \{ x \}) \equiv \bigwedge_{y \in V, y \neq x} y' = y. \]

(a) Show that \( \text{wp}(\varphi \land x = 0, \rho_{\text{havoc}}(x)) \equiv \text{false} \) for any formula \( \varphi \).

(b) Let \( \varphi_{x=0} \) be a formula that contains \( x = 0 \) as a subformula.

Show that \( \text{wp}(\varphi_{x=0}, \rho_{\text{havoc}}(x)) \equiv \text{false} \) does not hold in general.

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

Exercise 2: Weakest precondition and strongest postcondition

Let \( \varphi \) and \( \psi \) be arbitrary predicates and \( \rho \) be a transition relation.

Give a counterexample for each of the following statements if it does not hold.

(a) \( \varphi = \text{wp}(\psi, \rho) \iff \text{post}(\varphi, \rho) = \psi \)

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

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

Exercise 3: Reachable states

Compute the set of reachable states for the program below. Note that we changed \( \varphi_{\text{init}} \).

\[
P = (V, pc, \varphi_{\text{init}}, \mathcal{R}, \varphi_{\text{err}})
\]

\[
V = (pc, x, y, i, j)
\]

\[
\mathcal{L} = \{ \ell_0, \ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6, \ell_{\text{ex}}, \ell_{\text{err}} \}
\]

\[
\varphi_{\text{init}} \equiv pc = \ell_0 \land i = 2 \land j = 2
\]

\[
\varphi_{\text{err}} \equiv pc = \ell_{\text{err}}
\]

\[
\mathcal{R} = \{ \rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7, \rho_8 \}
\]

\[
\rho_1 \equiv \text{move}(\ell_0, \ell_1) \land x' = i \land \text{skip}(i, y, j)
\]

\[
\rho_2 \equiv \text{move}(\ell_1, \ell_2) \land y' = j \land \text{skip}(x, i, j)
\]

\[
\rho_3 \equiv \text{move}(\ell_2, \ell_3) \land x \neq 0 \land \text{skip}(x, i, y, j)
\]

\[
\rho_4 \equiv \text{move}(\ell_2, \ell_6) \land x = 0 \land \text{skip}(x, i, y, j)
\]

\[
\rho_5 \equiv \text{move}(\ell_3, \ell_4) \land x' = x - 1 \land \text{skip}(i, y, j)
\]

\[
\rho_6 \equiv \text{move}(\ell_4, \ell_2) \land y' = y - 1 \land \text{skip}(x, i, j)
\]

\[
\rho_7 \equiv \text{move}(\ell_6, \ell_{\text{ex}}) \land (i = j \rightarrow y = 0) \land \text{skip}(x, i, y, j)
\]

\[
\rho_8 \equiv \text{move}(\ell_6, \ell_{\text{err}}) \land \neg(i = j \rightarrow y = 0) \land \text{skip}(x, i, y, j)
\]
Exercise 4: Inductive invariants

Consider the following program from the lecture

\[ P = (V, pc, \varphi_{init}, R, \varphi_{err}) \]

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

\begin{align*}
\rho_1 &= (move(\ell_1, \ell_2) \land y \geq z \land \text{skip}(x, y, z)) \\
\rho_2 &= (move(\ell_2, \ell_2) \land x + 1 \leq y \land x' = x + 1 \land \text{skip}(y, z)) \\
\rho_3 &= (move(\ell_2, \ell_3) \land x \geq y \land \text{skip}(x, y, z)) \\
\rho_4 &= (move(\ell_3, \ell_4) \land x \geq z \land \text{skip}(x, y, z)) \\
\rho_5 &= (move(\ell_3, \ell_5) \land x + 1 \leq z \land \text{skip}(x, y, z))
\end{align*}

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

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

(c) Describe a (possibly non-terminating) algorithm to construct the weakest inductive invariant that is contained in the complement of \( \varphi_{err} \) (for any program that is safe).

Hint: Eliminate states that can reach an error state.

\(^1\)A formula \( \varphi \) is weaker than a formula \( \psi \) if \( \psi \) implies \( \varphi \). An inductive invariant \( \varphi \) is the weakest inductive invariant if \( \varphi \) is implied by all other inductive invariants.