



## 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.

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

- (a) Show that  $wp(\varphi \wedge x = 0, \rho_{\text{havoc}(x)}) \equiv \text{false}$  for any formula  $\varphi$ .
- (b) Let  $\varphi_{x=0}$  be a formula that contains  $x = 0$  as a subformula.  
 Show that  $wp(\varphi_{x=0}, \rho_{\text{havoc}(x)}) \equiv \text{false}$  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  $\varphi$  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.

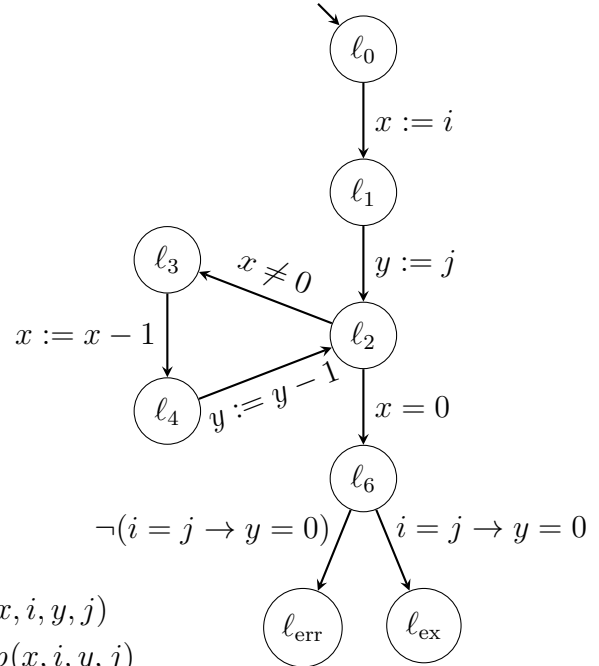
- (a)  $\varphi = wp(\psi, \rho) \iff post(\varphi, \rho) = \psi$
- (b)  $\varphi \subseteq wp(\psi, \rho) \iff post(\varphi, \rho) \subseteq \psi$
- (c)  $\varphi \supseteq wp(\psi, \rho) \iff post(\varphi, \rho) \supseteq \psi$

### Exercise 3: Reachable states

2 Points

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

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



### 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 initial condition  $\varphi_{init}$  is  $pc = \ell_1$ , the error condition  $\varphi_{err}$  is  $pc = \ell_5$ , and the set of transition relations  $\mathcal{R}$  contains the following transitions.

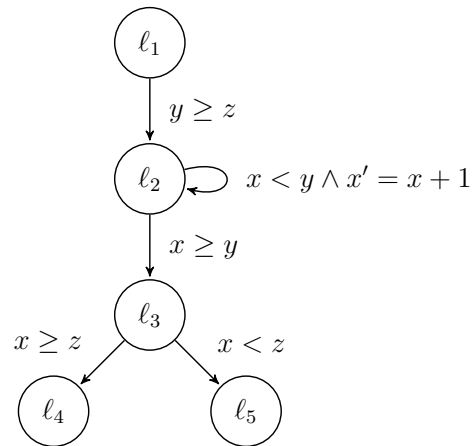
$$\rho_1 = (move(\ell_1, \ell_2) \wedge y \geq z \wedge skip(x, y, z))$$

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

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

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

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



- Is the complement of  $\varphi_{err}$  an inductive invariant? If not, give a counterexample.
- What is the weakest<sup>1</sup> inductive invariant that is contained in the complement of  $\varphi_{err}$  (i.e., disjoint from  $\varphi_{err}$ )?
- 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.

---

<sup>1</sup>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.