Exercise 1: Havoc
We define the transition relation for the guarded command $\text{havoc } x$ 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 $wp(\varphi \land x = 0, \rho_{\text{havoc}(x)}) \equiv false$ for any formula $\varphi$.

(b) Let $\varphi_{x=0}$ be a formula that contains $x = 0$ as a subformula.
Show that $wp(\varphi_{x=0}, \rho_{\text{havoc}(x)}) \equiv false$ 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
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: Inductive invariants
Consider the following program from the lecture

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

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

- $\rho_1 = (\text{move}(\ell_1, \ell_2) \land y \geq z \land \text{skip}(x, y, z))$
- $\rho_2 = (\text{move}(\ell_2, \ell_2) \land x < y \land x' = x + 1 \land \text{skip}(y, z))$
- $\rho_3 = (\text{move}(\ell_2, \ell_3) \land x \geq y \land \text{skip}(x, y, z))$
- $\rho_4 = (\text{move}(\ell_3, \ell_4) \land x \geq z \land \text{skip}(x, y, z))$
- $\rho_5 = (\text{move}(\ell_3, \ell_5) \land x < z \land \text{skip}(x, y, z))$
(a) Is the complement of $\varphi_{err}$ an inductive invariant? If not, give a counterexample.

(b) What is the weakest\footnote{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.} 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.