University of Tartu *Fall 2014*
Department of Computer Science *Vesal Vojdani*

Formal Methods in Software Engineering

`Exercise sheet 1`

Exercise 1: *Weakest Pre-Condition* *3 Points*

Compute $\mathsf{WP}\,[\![P]\!]\,(x = 2 \cdot y)$ for the following program P:

$$y = z + z\ ;$$
$$x = y \cdot y$$

Exercise 2: *Loop Invariant* *4 Points*

Show that the Hoare triplet $(\!|\, true \,|\!)\ P\ (\!|\, x = y \,|\!)$ is satisfied under partial correctness, where the program P is now defined as follows:

$$\begin{array}{l} a = x\ ; \\ y = 0\ ; \\ \mathsf{while}\ a \neq 0\ \mathsf{do}\ \{ \\ \qquad y = y + 1\ ; \\ \qquad a = a - 1 \\ \} \end{array}$$

Hint: First, ask yourself what remains the same when you take one from a and give it to y. Then, think what this value was like at the start of the program.

Exercise 3: *Two rules for conditionals* *3 Points*

Consider the two rules for conditionals:

$$\frac{(\!|\, \phi \wedge e \,|\!)\ C_1\ (\!|\, \psi \,|\!) \qquad (\!|\, \phi \wedge \neg e \,|\!)\ C_2\ (\!|\, \psi \,|\!)}{(\!|\, \phi \,|\!)\ \mathsf{if}\ e\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ (\!|\, \psi \,|\!)} \qquad \frac{(\!|\, \phi_1 \,|\!)\ C_1\ (\!|\, \psi \,|\!) \qquad (\!|\, \phi_2 \,|\!)\ C_2\ (\!|\, \psi \,|\!)}{(\!|\, \phi' \,|\!)\ \mathsf{if}\ e\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ (\!|\, \psi \,|\!)}$$

where $\phi' = (e \to \phi_1) \wedge (\neg e \to \phi_2)$. Show that adding the latter rule does not allow us to prove anything that we could not prove before. (You get 2 points if you can just state what exactly needs to be shown and 1 point for doing it.)