# Exercises for Hoare Logic and Model Checking

2017/2018

**Exercise 1.** Provide a program $C$ such that the following partial correctness triple holds, or argue why such a $C$ cannot exist:

$$\{X = x \wedge Y = y \wedge x \neq y\}\ C\ \{x = y\}$$

**Exercise 2.** Show that the alternative assignment axiom

$$\overline{\{P\}\ V := E\ \{P[E/V]\}}$$

is unsound by providing $P$, $V$, and $E$ such that

$$\neg(\models \{P\}\ V := E\ \{P[E/V]\})$$

**Exercise 3.** Prove that the following backwards reasoning sequenced assignment rule is derivable from the normal proof rules of Hoare logic:

$$\frac{\{P\}\ C\ \{Q[E/V]\}}{\{P\}\ C; V := E\ \{Q\}}$$

**Exercise 4.** Propose a loop invariant for proving the following partial correctness triple:

$$\begin{array}{l} \{X = x \wedge Y = y \wedge Z = 0 \wedge A = 1 \wedge Y \geq 0\} \\ \textbf{while } A \leq Y \textbf{ do } (Z := Z + X; A := A + 1) \\ \{Z = x \times y\} \end{array}$$

**Exercise 5.** Prove soundness of the separation logic heap assignment rule by proving that

$$\models \{E_1 \mapsto t\}\ [E_1] := E_2\ \{E_1 \mapsto E_2\}$$

**Exercise 6.** Propose a loop invariant for proving the following partial correctness triple in separation logic:

$$\{(N \geq 0 \wedge X = 0) \wedge Y \mapsto 0\}$$
$$\textbf{while } X < N \textbf{ do } (A := [Y]; X := X + 1; [Y] := A + X)$$
$$\left\{Y \mapsto \sum_{i=1}^{N} i\right\}$$

**Exercise 7.** Propose a loop invariant for proving the following partial correctness triple in separation logic:

$$\{\mathit{list}(X, \alpha)\}$$
$$Y := \textbf{null};$$
$$\textbf{while } X \neq \textbf{null do}$$
$$(Z := [X + 1]; [X + 1] := Y; Y := X; X := Z)$$
$$\{\mathit{list}(Y, \mathit{rev}(\alpha))\}$$

where *rev* is mathematical list reversal, so that

$$\begin{aligned} \mathit{rev}([]) &= [] \\ \mathit{rev}([h]) &= [h] \\ \mathit{rev}(\alpha ++ \beta) &= \mathit{rev}(\beta) ++ \mathit{rev}(\alpha) \end{aligned}$$