Additional exercises

Exercise 1

Prove soundness of the partial correctness rule for conditionals by proving that if $\models \{P \wedge B\}\ C_1\ \{Q\}$ and $\models \{P \wedge \neg B\}\ C_2\ \{Q\}$ then $\models \{P\}$ **if** B **then** C_1 **else** C_2 $\{Q\}$.

Exercise 2

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 3

Show that the alternative assignment axiom, $\vdash \{P\}\ V := E\ \{P[E/V]\}$, is unsound by providing a P, V and E such that $\neg(\models \{P\}\ V := E\ \{P[E/V]\})$.

Exercise 4

Prove that the following backwards-reasoning sequenced assignment rule is derivable from the normal proof rules of Hoare logic:

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

Exercise 5

Propose a loop invariant for proving the following partial correctness triple:

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

Exercise 6

Prove soundness of the separation logic assignment rule by proving that

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

Exercise 7

Propose a loop invariant for proving the following partial correctness triple in Separation logic:

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