Exercise Sheet 7: Axiomatic Semantics

Due date: June 9th. You can hand in your solutions at the start of the exercise class.

Exercise 1 (Interpretation of Hoare Triples) — 25%

Match each of the following Hoare triples

(a) [5%] $\{P\}\ c\ \{\mathsf{true}\}$
(b) [5%] $\{P\}\ c\ \{\Downarrow \mathsf{true}\}$
(c) [5%] $\{\mathsf{true}\}\ c\ \{\mathsf{false}\}$
(d) [5%] $\{\mathsf{true}\}\ c\ \{\Downarrow \mathsf{false}\}$
(e) [5%] $\{\mathsf{false}\}\ c\ \{\Downarrow Q\}$

with their corresponding interpretation from 1–6. (There may be more than one Hoare triple with the same interpretation in 1–6.) Assume that P and Q contain no logical variable.

1. Program c diverges for all initial states.
2. The program never finishes in a final state satisfying Q.
3. The triple does not say anything about program c; it is logically equivalent to true.
4. The triple is logically equivalent to false.
5. None of the above. Provide yourself the interpretation of the triple.
6. Program c always terminate whenever executed in an initial state that satisfies P.

Exercise 2 (Derived Rules) — 40%

Which of the following rules hold true? For rules that do not hold, provide a counterexample and propose side conditions that make the rule sound. (Rules that do hold require no further justification).

(a) [5%] $\dfrac{\{P\}\ c\ \{Q_1\} \qquad \{P\}\ c\ \{Q_2\}}{\{P\}\ c\ \{Q_1 \wedge Q_2\}}$

(b) [5%] $\dfrac{\{P\}\ c\ \{Q_1\} \qquad \{P\}\ c\ \{Q_2\}}{\{P\}\ c\ \{Q_1 \vee Q_2\}}$

(c) [5%] $\dfrac{\{P_1\}\ c\ \{Q\} \qquad \{P_2\}\ c\ \{Q\}}{\{P_1 \wedge P_2\}\ c\ \{Q\}}$

(d) [5%] $\dfrac{\{P_1\}\ c\ \{Q\} \qquad \{P_2\}\ c\ \{Q\}}{\{P_1 \vee P_2\}\ c\ \{Q\}}$

(e) [10%] $\dfrac{\{P\}\ c\ \{Q\}}{\{P \wedge R\}\ c\ \{Q \wedge R\}}$

(f) [10%] $\dfrac{\{P\}\ c\ \{Q\}}{\{P \wedge R\}\ c\ \{Q \vee R\}}$

Exercise 3 (Cyclic Hoare Calculus) **35%**

In this exercise, we exploit the equivalence between programs

$$\mathsf{while}\ (b)\ \mathsf{do}\ \{c\} \text{ and } \mathsf{if}\ (b)\ \mathsf{then}\ \{c; \mathsf{while}\ (b)\ \mathsf{do}\ \{c\}\}\ \mathsf{else}\ \{\mathsf{skip}\}$$

to define an alternative proof rule for while statements. For convenience, we equip every partial correctness property in a derivation tree with a unique index $i \in \mathbb{N}$ and denote the corresponding property by P_i. Moreover, let $P \equiv P'$ denote that two partial correctness properties P, P' are syntactically equivalent, i.e. $P = \{A\}c\{B\} = P'$ for some assertions A, B and $c \in \mathsf{Cmd}$. The new proof system replaces the while-rule by the following two new rules:

$$(\mathsf{while})\frac{\{A\}\ \mathsf{if}\ (b)\ \mathsf{then}\ \{c; \mathsf{while}\ (b)\ \mathsf{do}\ \{c\}\}\ \mathsf{else}\ \{\mathsf{skip}\}\ \{B\} \qquad (i')}{\{A\}\ \mathsf{while}\ (b)\ \mathsf{do}\ \{c\}\ \{B\} \qquad (i)} i \neq i' \text{ fresh}$$

and

$$(cycle)\frac{}{\{A\}\ c\ \{B\} \qquad (i)} \exists j \in \mathbb{N} : i \neq j \wedge P_j \equiv P_i.$$

The other rules are as presented in the lecture (except for the additional index). We call the resulting proof system the cyclic Hoare calculus.

Please state whether the following statements are correct. Explain your answer.

(a) [15%] Every partial correctness property P than can be proven in the original Hoare calculus, can also be proven using the cyclic Hoare calculus.

(b) [15%] The cyclic Hoare calculus is sound.

(c) [5%] The cyclic Hoare calculus is complete.