

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

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 .

Solution: (a)-3 (b)-6 (c)-1 (d)-4 (e)-3

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%]
$$\frac{\{P\} c \{Q_1\} \quad \{P\} c \{Q_2\}}{\{P\} c \{Q_1 \wedge Q_2\}}$$
- (b) [5%]
$$\frac{\{P\} c \{Q_1\} \quad \{P\} c \{Q_2\}}{\{P\} c \{Q_1 \vee Q_2\}}$$
- (c) [5%]
$$\frac{\{P_1\} c \{Q\} \quad \{P_2\} c \{Q\}}{\{P_1 \wedge P_2\} c \{Q\}}$$
- (d) [5%]
$$\frac{\{P_1\} c \{Q\} \quad \{P_2\} c \{Q\}}{\{P_1 \vee P_2\} c \{Q\}}$$
- (e) [10%]
$$\frac{\{P\} c \{Q\}}{\{P \wedge R\} c \{Q \wedge R\}}$$
- (f) [10%]
$$\frac{\{P\} c \{Q\}}{\{P \wedge R\} c \{Q \vee R\}}$$

Solution: (a)-T (b)-T (c)-T (d)-T (e)-F (f)-T .

Rule (e) becomes sound if we require that program variables in R are not modified by c .

Exercise 3 (Cyclic Hoare Calculus)

35%

In this exercise, we exploit the equivalence between programs

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

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 $c \in \text{Cmd}$. The new proof system replaces the **while**-rule by the following two new rules:

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

and

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

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.

Solution: We show the result by structural induction over the corresponding proof tree. Since only the while rule has been changed, it suffices to consider the while statement. Assume we can prove $\{A\} \text{ while } (b) \text{ do } \{c\} \{A \wedge \neg b\}$ in the original Hoare calculus. By definition, this implies the validity of $\{A \wedge b\} c \{A\}$.

We now construct a cyclic proof of $\{A\} \text{ while } (b) \text{ do } \{c\} \{A \wedge \neg b\}$.

$$\begin{array}{c} \text{I.H.} \\ \frac{\frac{\{A \wedge b\} c \{A\} \quad \{A\} \text{ while } (b) \text{ do } \{c\} \{A\} \quad (j)}{\{A \wedge b\} c; \text{while } (b) \text{ do } \{c\} \{A\}} \quad \frac{\models (A \wedge \neg b \Rightarrow A) \quad \{A\} \text{ skip } \{A\}}{\{A \wedge \neg b\} \text{ skip } \{A\}} \\ \hline \{A\} \text{ if } (b) \text{ then } \{c; \text{while } (b) \text{ do } \{c\}\} \text{ else } \{\text{skip}\} \{A\} \\ \hline \{A\} \text{ while } (b) \text{ do } \{c\} \{A\} \quad (i) \quad \models (A \wedge \neg b \Rightarrow A) \\ \hline \{A\} \text{ while } (b) \text{ do } \{c\} \{A \wedge \neg b\} \end{array}$$

Hence, the statement is correct.

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

Solution: Let P be the partial correctness property $\{x = 0\} x := 1 \{x = 2\}$. We show that $\{x = 0\} x := 1; x := 0; x := 1 \{x = 2\}$ can be derived in the cyclic Hoare calculus

which is obviously not a valid partial correctness property.

$$\begin{array}{c}
 \overline{\{0 = 0\} x := 0 \{x = 0\}} \\
 \frac{\overline{P} \quad (3) \quad \overline{\{x = 2\} x := 0 \{x = 0\}} \quad (4)}{\overline{\{x = 0\} x := 1; x := 0 \{x = 0\}} \quad (1)} \quad \overline{P} \quad (2) \\
 \hline
 \overline{\{x = 0\} x := 1; x := 0; x := 1 \{x = 2\}} \quad (0)
 \end{array}$$

Note that the (cycle) rule is applied in a loop: In (3) the existence of (2) is exploited and vice versa.

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

Solution: This is wrong by Theorem 10.3 of the lecture.