

Design and Selection of Programming Languages

4 November 2005

Exercise 8.1 — Using Operational Semantics to Prove Incorrectness

The following Hoare triples do not hold.

For each of these Hoare triples, present a derivation in the operational semantics that proves a counterexample to the statement.

- (a) $\{x \geq -5\} z := 5 - x \{z \leq 11 \wedge x \geq -3\}$
- (b) $\{x \geq -5\} z := 5 - x ; x := z + 2 \{z \leq 11 \wedge x \geq -3\}$

“Proving a counterexample” for the Hoare triple

$$\{pre\}Prog\{post\}$$

means to derive an assertion

$$\sigma_1(Prog) \Rightarrow \sigma_2$$

involving

- a state σ_1 for which *pre* **holds**, and
- a state σ_2 for which *post* **does not hold**.

Exercise 8.2 — Partial Correctness

For each of the following Hoare triples, determine whether it holds; if yes, prove it using the rules of axiomatic semantics, and if no, prove a counter-example using the rules of operational semantics (**you may abbreviate each expression evaluation into a single step**).

- (a) $\{x \geq -5\} z := 5 - x \{z \leq 11\}$
- (b) $\{x \geq -5\} z := 5 - x \{z \leq 11 \wedge x \geq -7\}$
- (c) $\{x \geq -5\} z := 5 - x \{z \leq 11 \wedge x \geq -3\}$
- (d) $\{x \geq -5\} z := 5 - x ; x := x + 2 \{z \leq 11 \wedge x \geq -3\}$
- (e) $\{x \geq -5\} z := 5 - x ; x := x + z \{z \leq 11 \wedge x = 2\}$
- (f) $\{z = abs(x)\} \text{ if } x \geq 0 \text{ then } z := -z \text{ fi } \{xz = -x^2\}$
- (g) $\{z = 0\} \text{ if } x = 0 \text{ then } w := \text{True} \text{ else } z := 1/x \text{ fi } \{\neg w \rightarrow xz = 1\}$

Exercise 8.3 — Partial Correctness Proof — 50% of Midterm 4, 2003

Consider the following program in a language providing a Java-like printing statement:

```
s := 1 ;  
r := 0 ;  
while s ≤ n do  
    r := r + 1 ;  
    s := s + 2 * r + 1 ;  
    println(r + " " + s)  
od
```

- (a) What is the output of this program for $n = 30$?
- (b) Give an equation relating the values of r and s in each **println** statement.
- (c) For this program **without the println** statement, **prove partial correctness** with respect to the **precondition** $\{ n \geq 0 \}$ and the **postcondition** $\{ r^2 \leq n \wedge n < (r + 1)^2 \}$.

Hint: Use the equation from (b) as part of the invariant!