

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**.

Solution Hints

- (a) Using operational semantics, we can prove a counterexample:

$$\frac{\frac{\{x \mapsto -5\}(5) \Rightarrow 5 \quad \{x \mapsto -5\}(x) \Rightarrow -5}{\{x \mapsto -5\}(5-x) \Rightarrow 10}}{\{x \mapsto -5\}(z := 5-x) \Rightarrow \{x \mapsto -5, z \mapsto 10\}}$$

This last state clearly does not satisfy $\{z \leq 11 \wedge x \geq -3\}$

- (b) For $\{x \geq -5\} z := 5 - x ; x := x + 2 \{z \leq 11 \wedge x \geq -3\}$, we again use operational semantics (expression evaluation not shown) to prove a counterexample:

$$\frac{\frac{\{x \mapsto 20\}(5-x) \Rightarrow -15}{\{x \mapsto 20\}(z := 5-x) \Rightarrow \{x \mapsto 20, z \mapsto -15\}} \quad \frac{\{x \mapsto 20, z \mapsto -15\}(z+2) \Rightarrow -13}{\{x \mapsto 20, z \mapsto -15\}(x := x+z) \Rightarrow \{x \mapsto -13, z \mapsto -15\}}}{\{x \mapsto 20\}(z := 5-x ; x := z+2) \Rightarrow \{x \mapsto -13, z \mapsto -15\}}$$

Although $\{x \mapsto 20\}$ satisfies the precondition $\{x \geq -5\}$, the final state $\{x \mapsto -13, z \mapsto -15\}$ does not

satisfy the postcondition $\{z \leq 11 \wedge x \geq -3\}$.

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) $\{z = \text{abs}(x)\} \text{if } x \geq 0 \text{ then } z := -z \text{ fi } \{xz = -x^2\}$
- (g) $\{z = 0\} \text{if } x = 0 \text{ then } w := \text{True} \text{ else } z := 1/x \text{ fi } \{\neg w \rightarrow xz = 1\}$

Solution Hints

- (a)
$$\frac{x \geq -5 \Rightarrow x \geq -6 \Leftrightarrow 5 - x \leq 11 \quad \{5 - x \leq 11\} z := 5 - x \{z \leq 11\}}{\{x \geq -5\} z := 5 - x \{z \leq 11\}}$$
- (b)
$$\frac{x \geq -5 \Rightarrow 5 - x \leq 11 \wedge x \geq -7 \quad \{5 - x \leq 11 \wedge x \geq -7\} z := 5 - x \{z \leq 11 \wedge x \geq -7\}}{\{x \geq -5\} z := 5 - x \{z \leq 11 \wedge x \geq -7\}}$$

(c) Using operational semantics, we can prove a counterexample:

$$\frac{\frac{\{x \mapsto -5\}(5) \Rightarrow 5 \quad \{x \mapsto -5\}(x) \Rightarrow -5}{\{x \mapsto -5\}(5 - x) \Rightarrow 10}}{\{x \mapsto -5\}(z := 5 - x) \Rightarrow \{x \mapsto -5, z \mapsto 10\}}$$

This last state clearly does not satisfy $\{z \leq 11 \wedge x \geq -3\}$

- (d) $\{x \geq -5\} z := 5 - x ; x := x + 2 \{z \leq 11 \wedge x \geq -3\}$
 \Leftarrow \langle sequence rule \rangle
 $\{x \geq -5\} z := 5 - x \{z \leq 11 \wedge x + 2 \geq -3\}$
 $\wedge \{z \leq 11 \wedge x + 2 \geq -3\} x := x + 2 \{z \leq 11 \wedge x \geq -3\}$
 \Leftarrow \langle left consequence, assignment \rangle
 $(x \geq -5 \Rightarrow (5 - x \leq 11 \wedge x + 2 \geq -3))$
 $\wedge \{5 - x \leq 11 \wedge x + 2 \geq -3\} z := 5 - x \{z \leq 11 \wedge x + 2 \geq -3\}$
 $\wedge \text{True}$
 \Leftarrow \langle logic and arithmetic, assignment \rangle
 $(x \geq -5 \Rightarrow x \geq -6) \wedge (x \geq -5 \Rightarrow x \geq -5) \wedge \text{True}$
 \Leftarrow \langle arithmetic \rangle
True

- (e) For $\{x \geq -5\} z := 5 - x ; x := x + z \{z \leq 11 \wedge x = 2\}$, we again use operational semantics (expression evaluation not shown) to prove a counterexample:

$$\frac{\frac{\{x \mapsto 0\}(5 - x) \Rightarrow 5}{\{x \mapsto 0\}(z := 5 - x) \Rightarrow \{x \mapsto 0, z \mapsto 5\}} \quad \frac{\{x \mapsto 0, z \mapsto 5\}(x + z) \Rightarrow 5}{\{x \mapsto 0, z \mapsto 5\}(x := x + z) \Rightarrow \{x \mapsto 5, z \mapsto 5\}}}{\{x \mapsto 0\}(z := 5 - x ; x := x + z) \Rightarrow \{x \mapsto 5, z \mapsto 5\}}$$

Although $\{x \mapsto 0\}$ satisfies the precondition $\{x \geq -5\}$, the final state $\{x \mapsto 5, z \mapsto 5\}$ does not satisfy the postcondition $\{z \leq 11 \wedge x = 2\}$.

- (f) Here a rule for “if ... then ... fi” is needed — this was not provided in the lecture, but is easy to produce:

$$\frac{\{P \wedge b\}S_1\{Q\} \quad P \wedge \neg b \Rightarrow Q}{\{P\}\text{if } b \text{ then } S_1 \text{ fi}\{Q\}}$$

- $\{z = \text{abs}(x)\} \text{if } x \geq 0 \text{ then } z := -z \text{ fi } \{xz = -x^2\}$
 \Leftarrow \langle one-sided conditional $\rangle \{z = \text{abs}(x) \wedge x \geq 0\} z := -z \{xz = -x^2\}$
 $\wedge (z = \text{abs}(x) \wedge x < 0 \Rightarrow xz = -x^2)$
 \Leftarrow \langle left consequence, arithmetic \rangle
 $(z = \text{abs}(x) \wedge x \geq 0 \Rightarrow x \cdot (-z) = -x^2) \wedge \{x \cdot (-z) = -x^2\} z := -z \{xz = -x^2\}$
 $\wedge (z = -x \Rightarrow xz = -x^2)$
 \Leftarrow \langle arithmetic, assignment, arithmetic \rangle
 $(z = x \Rightarrow x \cdot (-z) = -x^2) \wedge \text{True} \wedge \text{True}$
 \Leftarrow \langle arithmetic \rangle
True

(g) $\{z = 0\}$ **if** $x = 0$ **then** $w := \text{True}$ **else** $z := 1/x$ **fi** $\{\neg w \rightarrow xz = 1\}$
 \Leftarrow \langle conditional \rangle
 $\{z = 0 \wedge x = 0\} w := \text{True} \{\neg w \rightarrow xz = 1\} \wedge \{z = 0 \wedge x \neq 0\} z := 1/x \{\neg w \rightarrow xz = 1\}$
 \Leftarrow \langle left consequence, left consequence \rangle
 $(z = 0 \wedge x = 0 \Rightarrow (\neg \text{True} \rightarrow xz = 1))$
 $\wedge \{\neg \text{True} \rightarrow xz = 1\} w := \text{True} \{\neg w \rightarrow xz = 1\}$
 $\wedge (z = 0 \wedge x \neq 0 \Rightarrow (\neg w \rightarrow x \cdot (1/x) = 1))$
 $\wedge \{\neg w \rightarrow x \cdot (1/x) = 1\} z := 1/x \{\neg w \rightarrow xz = 1\}$
 \Leftarrow \langle logic, assignment, logic, assignment \rangle
 $(z = 0 \wedge x = 0 \Rightarrow (\text{False} \rightarrow xz = 1)) \wedge \text{True} \wedge (x \neq 0 \Rightarrow x \cdot (1/x) = 1) \wedge \text{True}$
 \Leftarrow \langle *ex falso quodlibet*, arithmetic \rangle
 $(z = 0 \wedge x = 0 \Rightarrow \text{True}) \wedge \text{True}$
 \Leftarrow \langle logic \rangle
True

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!

Solution Hints

1 4
2 9
3 16
4 25
5 36

— (b): $s = (r + 1)^2$

$\{n \geq 0\} P \{r^2 \leq n \wedge n < (r + 1)^2\}$

$\Leftarrow \langle (\text{right consequence}) \rangle$
 $\{n \geq 0\} P \{r^2 \leq n \wedge s = (r+1)^2 \wedge n < s\}$
 $\wedge (r^2 \leq n \wedge s = (r+1)^2 \wedge n < s \Rightarrow r^2 \leq n \wedge n < (r+1)^2)$

$\Leftarrow \langle (\text{sequence, logic}) \rangle$
 $\{n \geq 0\} (s, r) := (1, 0) \{r^2 \leq n \wedge s = (r+1)^2\}$
 $\wedge \{r^2 \leq n \wedge s = (r+1)^2\} \text{ while } s \leq n \text{ do } B \text{ od } \{r^2 \leq n \wedge s = (r+1)^2 \wedge n < s\}$
 $\wedge \text{True}$

$\Leftarrow \langle (\text{left consequence, while}) \rangle$
 $(n \geq 0 \Rightarrow 0^2 \leq n \wedge 1 = (0+1)^2)$
 $\wedge \{0^2 \leq n \wedge 1 = (0+1)^2\} (s, r) := (1, 0) \{r^2 \leq n \wedge s = (r+1)^2\}$
 $\wedge \{r^2 \leq n \wedge s = (r+1)^2 \wedge s \leq n\} r := r+1; s := s+2*r+1 \{r^2 \leq n \wedge s = (r+1)^2\}$

$\Leftarrow \langle (\text{logic, assignment, sequence}) \rangle$
 $\text{True} \wedge \text{True}$
 $\wedge \{r^2 \leq n \wedge s = (r+1)^2 \wedge s \leq n\} r := r+1 \{r^2 \leq n \wedge s+2*r+1 = (r+1)^2\}$
 $\wedge \{r^2 \leq n \wedge s+2*r+1 = (r+1)^2\} s := s+2*r+1 \{r^2 \leq n \wedge s = (r+1)^2\}$

$\Leftarrow \langle (\text{left consequence, assignment}) \rangle$
 $(r^2 \leq n \wedge s = (r+1)^2 \wedge s \leq n \Rightarrow (r+1)^2 \leq n \wedge s+2*(r+1)+1 = ((r+1)+1)^2)$
 $\wedge \{(r+1)^2 \leq n \wedge s+2*(r+1)+1 = ((r+1)+1)^2\} r := r+1 \{r^2 \leq n \wedge s+2*r+1 = (r+1)^2\}$
 $\wedge \text{True}$

$\Leftarrow \langle (\text{arithmetic, assignment}) \rangle$
 $(r^2 \leq n \wedge s = (r+1)^2 \wedge s \leq n \Rightarrow (r+1)^2 \leq n \wedge s+2*(r+1)+1 = (r+1)^2 + 2*(r+1)*1 + 1^2)$
 $\wedge \text{True}$

$\Leftarrow \langle (\text{logic, arithmetic}) \rangle$
 True
