

Program Semantics; Hoare Triples

CS 536 Lecture 6, Mon Jan 30, 2012

A. Why

- The meaning of a program is that it transforms states.
- To specify a program's correctness, we need to know its precondition (what must be true before executing it) and its postcondition (what should be true after it).

B. Objectives

- At the end of this activity you should
- Be able to calculate the semantics of simple programs.
- Be able to recognize syntactically correct correctness triples.
- Be able to say whether a correctness triple is satisfied, given information about whether the current state satisfies the precondition, whether the statement terminates, and if it terminates in a state satisfying the postcondition.

C. Questions (with solutions)

Questions 1 – 3 are left over from Activity 5:

1. What is $M(\mathbf{if\ }x > 0\ \mathbf{then\ }x := x+1\ \mathbf{else\ }y := 2*x\ \mathbf{fi}, \sigma)$ if

a. $\sigma(x) = 8$?

b. $\sigma(x) = 0$?

(a) $M(\mathbf{if...fi}, \sigma) = M(x := x+1, \sigma) = \sigma[x \mapsto \sigma(x+1)] = \sigma[x \mapsto 9]$

(b) $M(\mathbf{if...fi}, \sigma) = M(y := 2*x, \sigma) = \sigma[y \mapsto \sigma(2*x)] = \sigma[y \mapsto 0]$

2. What is $M(\mathbf{if\ }x > 0\ \mathbf{then\ }x := x+1\ \mathbf{else\ }y := 2*x\ \mathbf{fi}, \sigma)$?

Either $M(x := x+1, \sigma)$ or $M(y := 2*x, \sigma)$ depending on whether $\sigma \models x > 0$ or not.

3. What is $M(\mathbf{if\ }x > 0\ \mathbf{then\ }x := x/z\ \mathbf{fi}, \sigma)$ if $\sigma(x) = -2$?

Since $\sigma \not\models x > 0$, we have $M(\mathbf{if...fi}, \sigma) = M(\mathbf{skip}, \sigma) = \sigma$

4. What is $M(W, \sigma)$ where $W \equiv \mathbf{while\ }x < 3\ \mathbf{do\ }x := x+1;\ y := y*x\ \mathbf{od}$ and $\sigma \models x = 4 \wedge y = 1$?

Since $\sigma \not\models x < 3$, $M(W, \sigma) = \sigma$.

5. What is $M(W, \sigma)$ for the same W but when $\sigma \models x = 1 \wedge y = 1$?

Let $\sigma = \tau_0$, $\tau_1 = M(S, \tau_0)$ where S is the loop body

so $\tau_1 = M(x := x+1; y := y*x, \tau_0) = \sigma[x \mapsto 2][y \mapsto 2]$.

Let $\tau_2 = M(x := x+1; y := y*x, \tau_1) = \sigma[x \mapsto 3][y \mapsto 6]$

Since τ_0 and τ_1 both $\models x < 3$ but $\tau_2 \not\models x < 3$, we get $M(W, \sigma) = \tau_2$.

6. What is $M(\text{while true do skip od}, \sigma)$?

It's undefined for all σ .

7. For a loop-free program (a program that doesn't include any loops), is there any difference between partial and total correctness?

No.

8. Say we're given $\sigma \models \{x > 0\} S \{y > x\}$ for all σ and we're given a state τ where $\tau(x) = -3$. Do we know what S will do if we run in τ ? Must it terminate? Diverge? Must $y > x$ afterwards? How about $y \leq x$?

No, no, no, no, and no.

9. For which σ does $\sigma \models \{x > 1\} y := x*x \{y > x\}$ hold? Is this triple valid?

For all states σ , so the triple is valid.

10. For which σ does $\sigma \models \{x > 0\} y := x*x \{y > x\}$ hold? Is this triple valid?

For states in which $x > 1$, but not for states where $x = 0$, so the triple is not valid.

11. In general, does $\sigma \models \{\text{false}\} S \{q\}$ hold? What about $\sigma \models \{p\} S \{\text{true}\}$?

Yes, both triples hold for all states (so neither triple says anything useful about programs).

Not mentioned in class: Under total correctness, the second triple is satisfied iff S terminates in σ , so it does say something useful.