IIT CS536: Science of Programming

Homework 3: Statements, Semantics, Errors and Hoare Triples

Prof. Stefan Muller
TAs: Chaoqi Ma, Zhenghao Zhao

Out: Wednesday, Feb. 9
Due: Monday, Feb. 21, 11:59pm CST

This assignment contains 7 written task(s) for a total of 65 points.

SOLUTIONS

Logistics

Submission Instructions

Please read and follow these instructions carefully.

- Submit your homework on Blackboard under the correct assignment by the deadline (or the extended deadline if taking late days).
- You may submit multiple times, but we will only look at your last submission. Make sure your last submission contains all necessary files.
- Email the instructor and TAs ASAP if
  - You submit before the deadline but then decide to take (more) late days.
  - You accidentally resubmit after the deadline, but did not intend to take late days.

  Otherwise, you do not need to let us know if you're using late days; we'll count them based on the date of your last submission.
- Submit your written answers in a single PDF or Word document. Typed answers are preferred (You can use any program as long as you can export a .pdf, .doc or .docx; LaTeX is especially good for typesetting logic and math, and well worth the time to learn it), but *legible* handwritten and scanned answers are acceptable as well.
- Your Blackboard submission should contain only the file with your written answers. Do not compress or put any files in folders.

Collaboration and Academic Honesty

Read the policy on the website and be sure you understand it.

1 Statement Syntax

Task 1.1 (Written, 8 points).

Write a program **using only the syntax of our language from class** that adds the elements of an array a and puts the sum in the variable x. Formally, if your program is s, we should have

$$\vDash [\ T\ ]\ s\ [\ x = a[0] + a[1] + \cdots + a[size(a) - 1]\ ]$$

$$\begin{array}{l} x := 0; \\ i := 0; \\ \mathsf{while}(i < size(a))\{ \\ \quad x := x + a[i]; \\ \quad i := i + 1 \\ \} \end{array}$$

2 Semantics

Task 2.1 (Written, 10 points).

Consider the following program, which we will refer to as s:

$$\begin{array}{l} \mathsf{while}(n > 1)\{ \\ \quad \mathsf{if}(even(n)) \\ \quad \mathsf{then}\{n := n/2\} \\ \quad \mathsf{else}\{n := 3 * n + 1\} \\ \} \end{array}$$

Assume that $even(n)$ returns true if n is even and false otherwise.

a) Show the steps of evaluation to evaluate s with the state $\sigma = \{n = 5\}$ until it reaches skip. You can define shorthands, e.g., let b be the body of the while loop, and use notations like $\rightarrow^2$ to skip boring steps. **Do not skip over any steps that perform state updates.** You don't need to show work for the evaluation of expressions (e.g., below we realize that $\sigma(n > 1) = T$ and $\sigma(even(n))$, but don't show that). The first couple steps are shown as an example.

$$\begin{array}{ll} & \langle s, \{n = 5\}\rangle \\ \rightarrow & \langle b; s, \{n = 5\}\rangle \\ \rightarrow & \langle n := 3 * n + 1; s, \{n = 5\}\rangle \\ \rightarrow & \ldots \end{array}$$

b) What is $M(s, \sigma)$? You don't need to show work.

a)

$$
\begin{array}{ll}
 & \langle s, \{n = 5\}\rangle \\
\to & \langle b; s, \{n = 5\}\rangle \\
\to & \langle n := 3 * n + 1; s, \{n = 5\}\rangle \\
\to & \langle s, \{n = 16\}\rangle \\
\to^2 & \langle n := n/2; s, \{n = 16\}\rangle \\
\to & \langle s, \{n = 8\rangle\} \\
\to^2 & \langle n := n/2; s, \{n = 8\}\rangle \\
\to & \langle s, \{n = 4\rangle\} \\
\to^2 & \langle n := n/2; s, \{n = 4\}\rangle \\
\to & \langle s, \{n = 2\rangle\} \\
\to^2 & \langle n := n/2; s, \{n = 2\}\rangle \\
\to & \langle s, \{n = 1\rangle\} \\
\to & \langle \mathsf{skip}, \{n = 1\}\rangle
\end{array}
$$

b) $\{\{n = 1\}\}$

Task 2.2 (Written, 12 points).

For each of the following statements and states, give $M(s, \sigma)$. Use $\perp_d$ for divergence and $\perp_e$ for errors; don't use just $\perp$.

a) $s = \mathsf{while}\ n < 0\ \{n := n - 1\}$, $\sigma = \{n = -1\}$

b) $s = \mathsf{while}\ n > 0\ \{n := n - 1\}$, $\sigma = \{n = 3\}$

c) $s = \mathsf{while}\ n > 0\ \{n := n - 1\}$, $\sigma = \{n = -1\}$

d) $s = \mathsf{if}\ x > 0\ \mathsf{then}\ \{y := a[x]\}\ \mathsf{else}\ \{z := 0\}$, $\sigma = \{x = 1, a = [0, 3, 2, 1]\}$

e) $s = \mathsf{if}\ x > 0\ \mathsf{then}\ \{y := a[x]\}\ \mathsf{else}\ \{z := 0\}$, $\sigma = \{x = -1, a = [0, 3, 2, 1]\}$

f) $s = \mathsf{if}\ x > 0\ \mathsf{then}\ \{y := a[x]\}\ \mathsf{else}\ \{z := 0\}$, $\sigma = \{x = 5, a = [0, 3, 2, 1]\}$

a) $\{\perp_d\}$

b) $\{\{n = 0\}\}$

c) $\{\{n = -1\}\}$

d) $\{\{x = 1, a = [0, 3, 2, 1], y = 3\}\}$

e) $\{\{x = 1, a = [0, 3, 2, 1], z = 0\}\}$

f) $\{\perp_e\}$

3 Hoare triples

Task 3.1 (Written, 16 points).

Let $s = \textsf{while}\ i > 0\ \{x := x * i; i := i - 1\}$. For each of the following, is the triple satisfied or unsatisfied in the given state? Explain why in a sentence or two. Note that some of these are partial correctness triples and others are total correctness.

a) $\{i = 3, x = 1\} \vDash \{i > 0\}\ s\ \{i > 0\}$

b) $\{i = 3, x = 1\} \vDash \{i > 0\}\ s\ \{i \geq 0 \wedge x \geq 1\}$

c) $\{i = 3, x = 1\} \vDash [\ i > 0\ ]\ s\ [\ i \geq 0 \wedge x \geq 1\ ]$

d) $\{i = -1, x = 1\} \vDash \{i > 0\}\ s\ \{i \geq 0 \wedge x \geq 1\}$

e) $\{i = -1, x = 1\} \vDash [\ i > 0\ ]\ s\ [\ i \geq 0 \wedge x \geq 1\ ]$

f) $\{i = 3, x = 0\} \vDash \{i > 0\}\ s\ \{i \geq 0 \wedge x \geq 1\}$

g) $\{i = 3, x = 1\} \vDash \{i > 0\}\ s\ \{x = i!\}$

h) $\{i = 3, x = 1, k = 3\} \vDash \{i > 0 \wedge i = k\}\ s\ \{x = k!\}$

a) Unsatisfied. $i = 0$ in the final state.

b) Satisfied. $i = 0$ and $x = 6$ in the final state.

c) Satisfied. The program terminates in a state with $i = 0$ and $x = 6$.

d) Satisfied. The precondition is false.

e) Satisfied. The precondition is false.

f) Unsatisfied. $x = 0$ in the final state.

g) Unsatisfied. In the final state, $i = 0$ and $x = 6$.

h) Satisfied. In the final state, $k = 3$ and $x = 6 = 3!$.

Task 3.2 (Written, 12 points).

For each of the following triples, say if it's valid (satisfied in all states) or not. If not, fix the precondition, postcondition or statement to make the triple valid. Don't make your change trivial (that is, don't make the precondition a contradiction, the postcondition a tautology or the statement something that always errors or diverges).

a) $\{x \geq 0 \wedge y \geq 0\}\ z := x/y\ \{z \geq 0\}$

b) $[\ x \geq 0 \wedge y \geq 0\ ]\ z := x/y\ [\ z \geq 0\ ]$

c) $\{x > 0\}\ x := x - 1\ \{x \geq 0\}$

d) $\{i \geq 0 \wedge |a| > i\}\ x := a[i]\ \{x \geq 0\}$

a) Valid.

b) Not valid. Valid options include:

- $[\ x \geq 0 \wedge y > 0\ ]\ z := x/y\ [\ z \geq 0\ ]$
- $[\ x \geq 0 \wedge y \geq 0\ ]\ z := y = 0 ? 0 : x/y\ [\ z \geq 0\ ]$

c) Valid.

d) Not valid. Valid options include:

- $\{i \geq 0 \wedge |a| > i \wedge \forall 0 < j \leq |a|.a[j] \geq 0\}\ x := a[i]\ \{x \geq 0\}$
- $\{i \geq 0 \wedge |a| > i\}\ x := |a[i]|\ \{x \geq 0\}$
- $\{i \geq 0 \wedge |a| > i\}\ x := a[i]\ \{x = a[i]\}$

Task 3.3 (Written, 7 points).

Fill in an appropriate precondition such that the following triple is valid. **You may not change the program or postcondition.**

$$[\ \_\_\_\_\ ]\ m := n; \textsf{while}\ n \neq 0\ \{r := r * -2; n := n - 1\}\ [\ r = 2^m\ ]$$

$r = 1 \wedge n \geq 0 \wedge n = 2 * k$

4 One more wrap-up question

Task 4.1 (Written, 0 points).

How long (approximately) did you spend on this homework, in total hours of actual working time? Your honest feedback will help us with future homeworks.