Assignment 2 (Written): Semantics and Hoare Logic

17-654/17-754: Analysis of Software Artifacts
Jonathan Aldrich (jonathan.aldrich@cs.cmu.edu)

Due: Thursday, February 2, 2006 (5:00 pm)

100 points total

Turn in a file named <username>-17654-A2.{txt,pdf,doc}, where username is your Andrew id, or hand in a paper response in class. At the top of the document, state your name, Andrew id, and how long you spent on the assignment.

Assignment Objectives:

- Simulate WHILE programs using formal semantics, and prove simple properties of their behavior
- Write with specification constructs including pre- and post-conditions, loop invariants and variant functions
- Prove small programs correct using Hoare logic techniques

1 Formal Semantics (50 points)

Question 1 (10 points).

> Produce a derivation showing how the following expression reduces to a value in the context of the variable environment given, using the big-step semantics for WHILE given in class: $[x \mapsto 7, y \mapsto 4] \vdash x * y > 26 \; and \; x - y = 3$

Produce a derivation showing the first step of each of the following programs, using the small-step semantics for WHILE given in class. The appropriate environment is given for each program.

Question 2a (5 points).

$$[\,],\ \ x := 1 + 2;\ y := x - 5$$

Question 2b (5 points).

$$[x \mapsto 3],\quad skip;\ y := x - 5$$

Question 2c (5 points).

$$[x \mapsto 3],\quad while\ x{>}0\ do\ x := x - 1$$

Question 2d (5 points).

$$[x \mapsto 3],\quad if\ x{>}1\ then\ x := x{-}1\ else\ x := x{+}1$$

Consider the following WHILE program:

$i := 1;$
$r := 1;$
$while\ (i < n)\ do$
  $i := i + 1;$
  $r := r + i$

Question 3 (20 points).

Using the semantics of WHILE, prove that in the environment $[n \mapsto N]$ and assuming $N \geq 1$, the program above reduces to $([n \mapsto N, r \mapsto N * (N + 1)/2, i \mapsto N], skip)$. Your proof should have the level of detail done for the factorial function in lecture. Hint: as with the proof done in lecture, you will need to use induction to prove the while loop correct.

2 Hoare Logic (50 points)

Question 4 (10 points).

For the while program given above, state a (a) precondition, (b) postcondition, (c) loop invariant, and (d) variant function. The postcondition should precisely define the value of r in terms of N.

Question 5 (20 points).

Using weakest preconditions, state the proof obligations that assure (a) the invariant is initially true on entry to the loop, (b) the loop invariant holds after execution of each loop, (c) the variant function is greater than zero at loop entry, (d) the variant function decreases in the loop, and (e) the postcondition holds.

Question 6 (10 points).

Prove each of the proof obligations above. Your proof should be done at the level of detail shown in lecture, i.e. small steps with justifications given for each step.

Question 7 (10 points).

Which of the proof techniques above—semantics-based and Hoare Logic-based—do you prefer, and why? Are there any advantages of your second choice, whatever it is?