CS 536: Midterm Exam (60 min) Solution

Instructions

This exam is closed book, closed notes, and no support equipment (calculators, phones, computers, etc). All the questions are short-answer. The usual penalty for copying or sharing answers on a quiz or exam is a final grade of E for the course. If you have any questions, please ask during the quiz, not after. When a problem says "all" states, ignore improper states. Program variables range over the integers unless otherwise specified.

Histogram - with India Exams
100 100
99 98 98 98 96 96 96 94 94 94 93 92 92 92 92 91 91 91 91 90 90 90
88 88 87 87 87 86 86 85 85 84 84 84 84 83 83 83 83 82 82 82 80 80
79 78 78 75 74 74 71
69 68 68 67 66 66 65 65 65 64 62 62 61
57 54 52
49 45
Avg 81.1
Stdev 13.49

Questions

1. [9 points] Say $\sigma(x) = 4$ and $\sigma(y) = 3$. Do either of $\sigma(\textbf{if } x < 0 \textbf{ then } 1 \textbf{ else } x \textbf{ fi})$ and $\sigma(\textbf{if } \sigma(x < 0) \textbf{ then } \sigma(1) \textbf{ else } \sigma(x) \textbf{ fi})$ use incorrect notation? If not, then briefly (in a sentence or two) explain why.

The first is fine; the second is incorrect: the outer σ expects a syntactic argument, but it's being passed a mix of syntactic and semantic values.

2. [16 = 2*8 points] Say $\sigma(w) = 5$, $\sigma(z) = 10$. Let $\tau_1 = \sigma[w := 6][w := 7][z := 9]$ and $\tau_2 = \sigma[z := 9][w := 7]$. (2a) Is $\tau_1 = \tau_2$? (If not, briefly explain why.) (2b) Is $\tau_1 \equiv \tau_2$? (If not, briefly explain why.)

Ignoring overridden updates, we have $\tau_1 = \sigma[w := 7][z := 9] = \sigma[z := 9][w := 7] = \tau_2$. But $\tau_1 \equiv \tau_2$ is bad notation: you can't check states for syntactic equality.

3. [9 points] Briefly describe all the preconditions p and states σ such that $\sigma \models \{p\}\ h{:=}0\ \{h < 0\}$ under partial correctness.

Recall $\sigma \models \{p\}\ S\ \{q\}$ iff $\sigma \not\models p$ or $\mathcal{M}[\![h := 0]\!](\sigma) \neq \emptyset$ or $\mathcal{M}[\![h := 0]\!](\sigma) \models h < 0$. But these last two cases are false: $\mathcal{M}[\![h := 0]\!](\sigma) = \{\sigma[h := 0]\} \neq \emptyset$ and $\not\models h > 0$, so for σ to satisfy the triple, we need $\sigma \not\models p$.

4. [16 = 8*8 points] Let $p \equiv x \geq z \vee \exists z : z \leq x$. (a) What is $p[x := z]$? (b) What is $p[z := x]$? (For both parts, just do the substitution; don't logically simplify the result.)

(4a) $p[x := z] \equiv (x \geq z \vee \exists z : z \leq x)\ [x := z] \equiv z \geq z \vee \exists v : v \leq z$ (renamed $\exists z$ to $\exists v$).

(4b) $p[z := x] \equiv (x \geq z \vee \exists z : z \leq x)\ [z := x] \equiv x \geq x \vee \exists z : z \leq x$ (the $\exists z$ prevents substitution inside its body).

5. [15 points] Write a full proof outline for the following partial correctness triple. List any predicate logic obligations and show the results of substitution somewhere. Is the triple valid? If not, briefly describe the states under which it is invalid.

$$\{\textbf{true}\}\ y := x;\ z := y+1\ \{y < z\}.$$

$\{\textbf{true}\}\ \{x < x{+}1\}\ y := x;\ \{y < y{+}1\}\ z := y+1\ \{y < z\}.$

Predicate logic obligation: $\textbf{true} \to x < x{+}1$, which is valid.

6. [15 points] Repeat the previous problem, on the following triple: Write a full proof outline, list any predicate logic obligations and show the results of substitution somewhere. Is the triple valid? If not, briefly describe the states under which it is invalid.

$$\{m = x\}\ \textbf{if}\ m < y\ \textbf{then}\ m := y\ \textbf{fi}\ \{(m = x \vee m = y) \wedge m \le x \wedge m \le y\}$$

Let $q \equiv (m = x \vee m = y) \wedge m \le x \wedge m \le y$, then one outline is

$\{m = x\}$ **if** $m < y$ **then**
  $\{m = x \wedge m < y\}\ \{q[m := y]\}\ m := y\ \{q\}$
else
  $\{m = x \wedge m \ge y\}\ \{q\}$ **skip** $\{q\}$
fi $\{q\}$

where $q[m := y] \equiv (y = x \vee y = y) \wedge y \le x \wedge y \le y$

(Remember, an **if-then** is just an **if-else** with **skip** for the false branch.)

The predicate logic obligations are

- $(m = x \wedge m < y) \to ((y = x \vee y = y) \wedge y \le x \wedge y \le y)$, which is invalid, since $m = x < y$ and $y \le x$ contradict, and
- $(m = x \wedge m \ge y \to q)$, which is invalid in general (it's satisfiable only if $m = x = y$).

(For the program to work, we need to reverse the test: **if** $y < m$ **then** $m := y$ **fi**.)

7. [20 points] Consider the incomplete full proof outline:

$\{x \ge 0\}\ \{\_\_\_\_\_\}\ \_\_\_\_\_\ ;\ \{\textbf{inv}\ y^2 \le x\}$
while _____ **do**
  $\{y^2 \le x \wedge \_\_\_\_\_\}\ \{\_\_\_\_\_\}\ y := y+1\ \{y^2 \le x\}$
od $\{y^2 \le x < (y+1)^2\}$

Below, rewrite the program and proof outline, filling in the missing parts. List any proof obligations and show the results of substitution somewhere.

The outline is

$\{x \ge 0\}\ \{0^2 \le x\}\ y := 0\ ;\ \{\textbf{inv}\ y^2 \le x\}$
while $x \ge (y{+}1)^2$ **do**
  $\{y^2 \le x \wedge x \ge (y{+}1)^2\}\ \{(y{+}1)^2 \le x\}\ y := y+1\ \{y^2 \le x\}$
od $\{y^2 \le x < (y+1)^2\}$

The predicate logic obligations are $(x \ge 0 \to 0^2 \le x)$ and $(y^2 \le x \wedge x \ge (y{+}1)^2 \to (y{+}1)^2 \le x)$; both are valid.