IIT CS536: Science of Programming

Homework 4: Proofs, WP and SP

Prof. Stefan Muller
TAs: Chaoqi Ma, Zhenghao Zhao

Out: Thursday, Mar. 3
Due: Friday, Mar. 11, 11:59pm CST

This assignment contains 5 task(s) for a total of 40 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 Substitution

Task 1.1 (Written, 8 points).

Compute the given substitutions. Just substitute the expression for the value; you don't need to simplify anything further. **Show the intermediate steps of substitution when quantifiers are involved, as we did in class.**

a) $[y + x/x](2x + y \geq z)$

b) $[z/x](x \geq 0 \rightarrow (\forall x.x * z > y) \wedge x > -1)$

c) $[x/y]\forall x.(y > 0 \rightarrow \exists y.y = x)$

d) $[x + 2/x]\exists x.\forall y.x > y$

a) $2(y + x) + y \geq z$

b) $z \geq 0 \rightarrow [z/x](\forall x.x * z > y) \wedge z > -1 = z \geq 0 \rightarrow (\forall x.x * z > y) \wedge z > -1$

c) $[x/y](\forall z.[z/x](y > 0 \rightarrow \exists y.y = x)) = [x/y](\forall z.(y > 0 \rightarrow \exists y.y = z)) = \forall z.x > 0 \rightarrow \exists y.y = z$

d) $\exists x.\forall y.x > y$

2 Proofs and Proof Outlines

Task 2.1 (Written, 10 points).

Consider the following triple:

$$\{x \neq y\} \text{ if } y > x \text{ then } \{t := x; x := y; y := t\} \text{ else } \{\text{skip}\} \{x > y\}$$

Write a proof outline for the triple above. You can use either rule for if that we discussed in class.

$$\begin{array}{ll}
\{T\} & \\
\text{if}(y > x)\ \{ & \{x \neq y \wedge y > x\} \\
\quad t := x; & \{t \neq y \wedge y > t\} \\
\quad x := y; & \{t \neq x \wedge x > t\} \\
\quad y := t & \{y \neq x \wedge x > y\} \Rightarrow \{x > y\} \\
\}\ \text{else}\ \{ & \{x \neq y \wedge y \leq x\} \\
\quad \text{skip} & \{x \neq y \wedge y \leq x\} \Rightarrow \{x > y\} \\
\} & \{x > y\}
\end{array}$$

Task 2.2 (Written, 7 points).

Convert the following proof outline to a Hilbert-style proof. Note that we're using both rules for if, in different places.

$$
\begin{array}{ll}
\{T\} & \\
\mathsf{if}(x = \overline{0})\ \{ & \{T \wedge x = 0\} \Rightarrow \{x = 0 \wedge 0 = 0\} \\
\quad s := \overline{0} & \{x = 0 \wedge s = 0\} \\
\}\ \mathsf{else}\ \{ & \{T \wedge x \neq 0\} \Rightarrow \{x \neq 0\} \\
\quad \mathsf{if}(x < \overline{0})\ \{ & \{x \neq 0 \wedge x < 0\} \Rightarrow \{x < 0 \wedge -1 = -1\} \\
\quad\quad s := \overline{-1} & \{x < 0 \wedge s = -1\} \Rightarrow \{s = \frac{x}{|x|}\} \\
\quad \}\ \mathsf{else}\ \{ & \{x \neq 0 \wedge x \geq 0\} \Rightarrow \{x > 0 \wedge 1 = 1\} \\
\quad\quad s := \overline{1} & \{x > 0 \wedge s = 1\} \Rightarrow \{s = \frac{x}{|x|}\} \\
\quad \} & \{s = \frac{x}{|x|}\} \\
\} & \{(x = 0 \wedge s = 0) \vee s = \frac{x}{|x|}\}
\end{array}
$$

1	$\{x = 0 \wedge 0 = 0\}\ s := \overline{0}\ \{x = 0 \wedge s = 0\}$	Assign
2	$\{x < 0 \wedge -1 = -1\}\ s := \overline{-1}\ \{x < 0 \wedge s = -1\}$	Assign
3	$\{x \neq 0 \wedge x < 0\}\ s := \overline{-1}\ \{s = \frac{x}{\lvert x \rvert}\}$	Weaken 2
4	$\{x > 0 \wedge 1 = 1\}\ s := \overline{1}\ \{x > 0 \wedge s = 1\}$	Assign
5	$\{x \neq 0 \wedge x \geq 0\}\ s := \overline{1}\ \{s = \frac{x}{\lvert x \rvert}\}$	Weaken 4
6	$\{x \neq 0\}$ if $x < 0$ then $\{s := \overline{-1}\}$ else $\{s := \overline{1}\}\ \{s = \frac{x}{\lvert x \rvert}\}$	If 3, 5
7	$\{T \wedge x \neq 0\}$ if $x < \overline{0}$ then $\{s := \overline{-1}\}$ else $\{s := \overline{1}\}\ \{s = \frac{x}{\lvert x \rvert}\}$	Weaken 6
8	$\{T \wedge x = 0\}\ s := \overline{0}\ \{x = 0 \wedge s = 0\}$	Weaken 1
9	$\{T\}$ if $x = \overline{0}$ then $\{s := \overline{0}\}$ else $\{$if $x < \overline{0}$ then $\{s := \overline{-1}\}$ else $\{s := \overline{1}\}\}\ \{(x = 0 \wedge s = 0) \vee s = \frac{x}{\lvert x \rvert}\}$	If 7, 8

3 Weakest Preconditions and Strongest Postconditions

Task 3.1 (Written, 15 points).

Compute the following using the algorithms given in class. **Show the steps you take to get to your answer.** You don't need to simplify the conditions.

a) (3 points) $wlp(x := x + y; n := x * z, n = 0)$

$$\begin{aligned} &= wlp(x := x + y, wlp(n := x * z, n = 0 \land z > 0)) \\ &= wlp(x := x + y, x * z = 0 \land z > 0) \\ &= (x + y) * z = 0 \land z > 0 \\ (\Leftrightarrow\ &x = y) \end{aligned}$$

b) (6 points) $wp(\mathsf{if}\ x = y\ \mathsf{then}\ \{z := \overline{1}\}\ \mathsf{else}\ \{z := x/y\}, z = 1)$

$$\begin{aligned} &= wlp(\mathsf{if}\ x = y\ \mathsf{then}\ \{z := \overline{1}\}\ \mathsf{else}\ \{z := x/y\}, z = 1) \land D(\mathsf{if}\ x = y\ \mathsf{then}\ \{z := \overline{1}\}\ \mathsf{else}\ \{z := x/y\}) \\ &= (x = y \to wlp(z := \overline{1}, z = 1)) \land (x \neq y \to wlp(z := x/y, z = 1)) \\ &\quad \land D(x = y) \land (x = y \to D(z := \overline{1})) \land (x \neq y \to D(z := x/y)) \\ &= (x = y \to 1 = 1) \land (x \neq y \to x/y = 1) \land T \land (x = y \to T) \land (x \neq y \to y \neq 0) \\ (\Leftrightarrow\ &x \neq y \to (x/y = 1 \land y \neq 0)) \end{aligned}$$

c) (3 points) $sp(x = 1, \mathsf{if}\ y > 0\ \mathsf{then}\ \{x := x + 1\}\ \mathsf{else}\ \{\mathsf{skip}\})$

$$\begin{aligned} &= sp(x = 1 \land y > 0, x := x + 1) \lor sp(x = 1 \land y \leq 0, \mathsf{skip}) \\ &= (x_0 = 1 \land y > 0 \land x = x_0 + 1) \lor (x = 1 \land y \leq 0) \\ (\Leftrightarrow\ &(x = 2 \land y > 0) \lor (x = 1 \land y \leq 0)) \end{aligned}$$

d) (3 points) $sp(x \geq 0, x := 1; \mathsf{if}\ x > 0\ \mathsf{then}\ \{x := x - 1\}\ \mathsf{else}\ \{x := 0\})$

$$\begin{aligned} &= sp(sp(T, x := 1), \mathsf{if}\ x > 0\ \mathsf{then}\ \{x := x - 1\}\ \mathsf{else}\ \{x := 0\}) \\ &= sp(x_0 \geq 0 \land x = 1, \mathsf{if}\ x > 0\ \mathsf{then}\ \{x := x - 1\}\ \mathsf{else}\ \{x := 0\}) \\ &= sp(x_0 \geq 0 \land x = 1 \land x > 0, x := x - 1) \lor sp(x_0 \geq 0 \land x = 1 \land x \leq 0, x := 0) \\ &= (x_0 \geq 0 \land x_1 = 1 \land x_1 > 0 \land x = x_1 - 1) \lor (x_0 \geq 0 \land x_1 = 1 \land x_1 \leq 0 \land x = 0) \\ (\Leftrightarrow\ &(x_0 \geq 0 \land x_1 = 1 \land x = 0) \lor F) \\ (\Leftrightarrow\ &x_0 \geq 0 \land x_1 = 1 \land x = 0) \end{aligned}$$

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.