Homework 3

CS 477: Spring 2019

April 26, 2019

Points: Problem 1: 50, Problem 2: 20, Problem 3: 20

Problem 1. In this problem, you will have to prove given statements about programs using Floyd-Hoare logic. For this assignment, we are requiring that the rules of Floyd-Hoare logic be applied precisely, with absolutely no simplification. An automatic grader will be released for this assignment, and it will require the syntactic rules of Hoare logic to be applied exactly.

The exact rules of Hoare logic being used here are as follows -

$$\frac{}{\{P[e/x]\}x\texttt{:=}e\{P\}}\ [\text{Assign}] \quad \frac{\{P\}S_1\{Q\} \quad \{Q\}S_2\{R\}}{\{P\}S_1; S_2\{R\}}\ [\text{Seq}] \quad \frac{\{P \wedge e\}S_1\{Q\} \quad \{P \wedge \neg e\}S_2\{Q\}}{\{P\}\texttt{if } e \texttt{ then } S_1 \texttt{ else } S_2 \texttt{ fi}\{Q\}}\ [\text{If}]$$

$$\frac{\{P \wedge e\}S\{P\}}{\{P\}\texttt{while } e \texttt{ do } S \texttt{ od}\{P \wedge \neg e\}}\ [\text{While}] \quad \frac{\{P'\}S\{Q\} \quad P \to P'}{\{P\}S\{Q\}}\ [\text{PreStr}] \quad \frac{\{P\}S\{Q'\} \quad Q' \to Q}{\{P\}S\{Q\}}\ [\text{PostWeak}]$$

With that, prove the given statements about programs in Floyd-Hoare logic.

(a)
```
{x >= 0}
if y > x then
  m := y
else
  m := x
fi
{m >= 0}
```

(b)
```
{x = 0 & n >= 0}
y := 0;
while x < n do
  y := y + x;
  x := x + 1
od
{y = n * (n - 1) div 2}
```

Problem 2. This is a predicate abstraction setting.

Fix the following predicates P:

$$p_1 : x \geq y, \quad p_2 : x < y - 5$$

Let us have two Boolean variables associated with the two predicates, b_1 for p_1 and b_2 for p_2.

Consider the precondition, Pre: $b_1 \wedge \neg b_2$.

We would like to find the best monomial that abstracts the post state after executing the statement $x := x + 1$.

- For each of the literals b_1, $\neg b_1$, b_2, $\neg b_2$, write down a logical formula that expresses for an *arbitrary* predicate over b_1, b_2 that it is valid precisely when the literal must hold true in the post state.
- Instantiate the above formulas with α being the precondition $b_1 \wedge \neg b_2$, and evaluate which of the formulas corresponding to each literal is valid.
- Using the above, write down the precise monomial that abstracts the post state starting with the precondition Pre as a monomial over B.

Problem 3. Let $A_i = (S_i, \sqsubseteq_i, \sqcup_i, \sqcap_i, \top_i, \bot_i)$, where $i = 1, 2$, be two complete lattices.
Consider the partial order $A = (S_1 \times S_2, \sqsubseteq)$ where $(a_1, a_2) \sqsubseteq (b_1, b_2)$ iff $(a_1 \sqsubseteq b_1) \wedge (a_2 \sqsubseteq b_2)$
Prove that any *arbitrary* subset R of $S_1 \times S_2$ has a least upper bound in the partial order A.