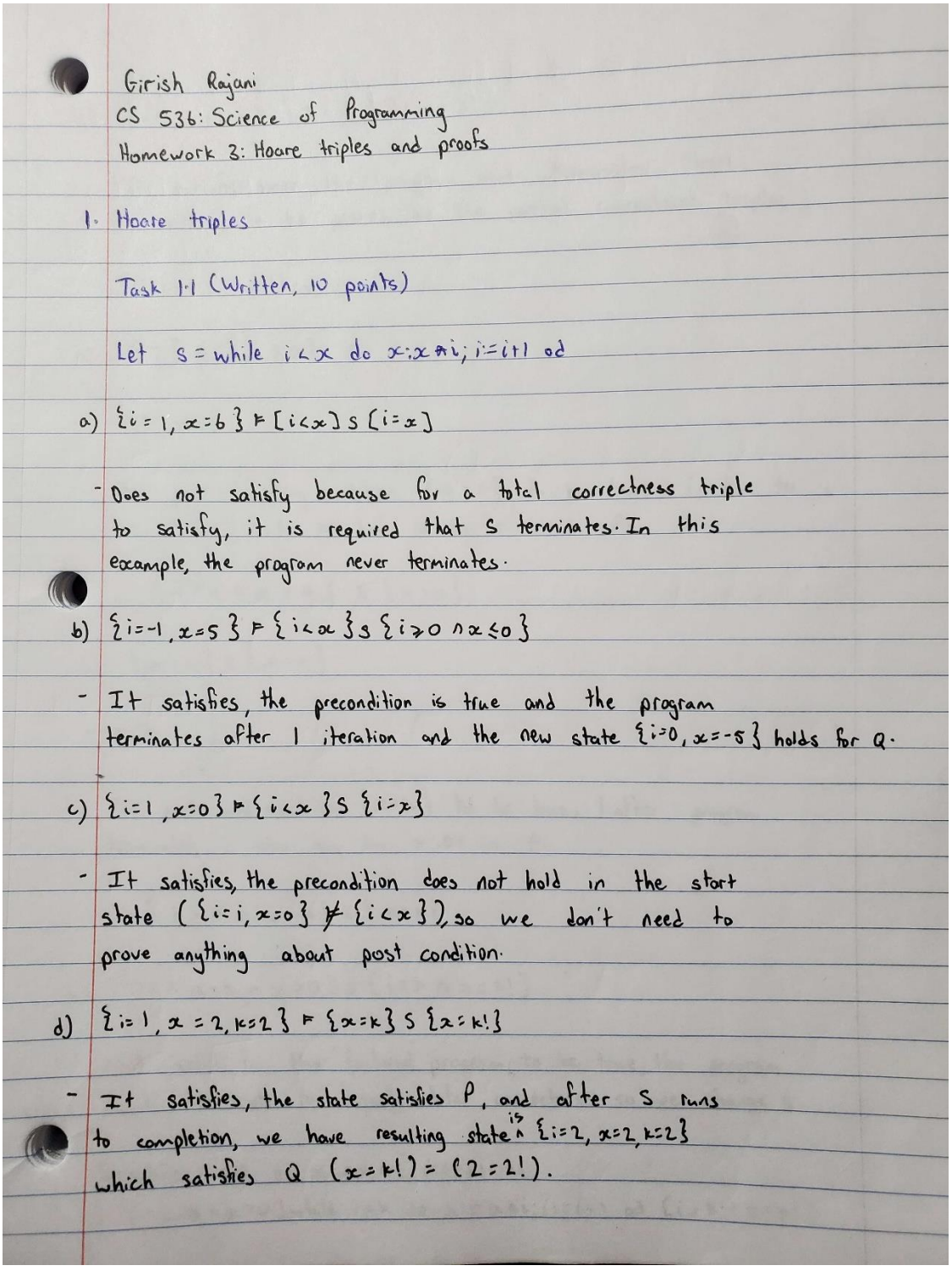
CS 536 – Science of Programming

Homework 3 – Hoare triples and proofs

Girish Rajani

A20503736



Girish Rajani
CS 536: Science of Programming
Homework 3: Hoare triples and proofs

1. Hoare triples

Task 1.1 (Written, 10 points)

Let S = while $i < x$ do $x := x * i$; $i := i + 1$ od

a) $\{i = 1, x = 6\} \vdash [i < x]\, S\, [i = x]$

- Does not satisfy because for a total correctness triple to satisfy, it is required that S terminates. In this example, the program never terminates.

b) $\{i = -1, x = 5\} \vdash \{i < x\}\, S\, \{i \geq 0 \wedge x \leq 0\}$

- It satisfies, the precondition is true and the program terminates after 1 iteration and the new state $\{i = 0, x = -5\}$ holds for Q.

c) $\{i = 1, x = 0\} \vdash \{i < x\}\, S\, \{i = x\}$

- It satisfies, the precondition does not hold in the start state ($\{i = i, x = 0\} \not\Rightarrow \{i < x\}$), so we don't need to prove anything about post condition.

d) $\{i = 1, x = 2, k = 2\} \vdash \{x = k\}\, S\, \{x = k!\}$

- It satisfies, the state satisfies P, and after S runs to completion, we have resulting state is $\{i = 2, x = 2, k = 2\}$ which satisfies Q $(x = k!) = (2 = 2!)$.

e) $\{i=1, x=6\} \vdash \{\top\}\ S\ \{\exists k.\, s=k!\}$

It satisfies, since the program never terminates, there is nothing to be proved for the partial correctness triple.

Task 1.2 (Written, 6 points)

a) $\{\top\}\ S\ \{x>0\}$

- Not valid

For post ~~conditing~~ condition $\{x>0\}$ to be true, i has to be >0 and x has to be >0, in P.

$\therefore \{i>0 \wedge x>0\}\ S\ \{x>0\}$

b) $\{x=k\}\ S\ \{x=k\}$

- Not valid

For post ~~cod~~ condition $\{x=k\}$ to be true, & after program terminates, i also has to >0 in P.

$\therefore \{i>0 \wedge x=k\}\ S\ \{x=k\}$

c) $[i=1 \wedge x=k \wedge x>0]\ S\ [i=k \wedge x=k!]$

- Not valid, for this factorial program to be true, the program must terminate to satisfy total correctness so we change S:

S = while $i<k$ do $x := x * i;\ i := i+1$ od

$[i=1 \wedge x=k \wedge x>0]$ while $i<k$ do $x := x*i;\ i := i+1$ od $[i=k \wedge x=k!]$

Task 1.3 (Written, 5 points)

$[m<0 \wedge ((m\%2 \neq 0 \wedge r=-1) \vee (m\%2=0 \wedge r=1))]$

- m has to be negative in [P] so that the $-m$ in the post condition becomes positive which will give 3^m.
- If m is even ($m\%2=0$), r has to be 1 so that S terminates & Q holds
- If m is odd, r has to be -1 then only will Q hold true after S terminates.

Task 1.4 (Written, 3 points)

$\vDash [P_1] x := sqrt(x)/y \; [T]$

For this to be valid, the total ~~complet~~ correctness triple has to terminate and have no errors. We need to make sure $y \neq 0$ so that it doesn't divide by 0. Lastly, we need to avoid errors in sqrt such as square root of negative numbers so we can just use ghost variable to make x a perfect square.

$\vDash [\, y \neq 0 \wedge x = k^2 \,] \; x := sqrt(x)/y \; [T]$

Task 1.5 (Written, 8 points)

For a total correctness triple to not be valid, we can make the program an ~~infict~~ infinite loop (never terminates) or it always returns an error:

a) Using while clause: $S_2 =$ while $x \neq 0$ do $x := x - 1$ od

$P_2 = x < 0 \therefore \not\vDash [x < 0]$ while $x \neq 0$ do $x := x - 1$ od $[T]$

Program never terminates successfully - always diverges which means that this total correctness triple is never satisfied.

b) Without while clause:

$S_2 =$ $x := a[i]$

~~$P_2 = [i < 0$~~

$P_2 = [i \geq size(a)]$

$\therefore \not\models [i \geq size(a)]\ x := a[i]\ [T]$

This program, when P is satisfied, will always access an array out of bound which means the program never terminates successfully - always returns an error. Thus, this total correctness triple is never satisfied.

Task 1.6 (Written, 8 points)

a) $[x > 3]\ S\ [x \leq 1]$

S = while $x > 1$ do if even(x) then $x := 5x+1$ else $x := x/2$ fi od

This satisfies the wording of the question.

b) ~~Ex~~ $[x \leq 3]\ S\ [x > 1]$

S = while $x > 1$ do if even(x) then $x := 5x+1$ else $x := x/2$ fi od

This satisfies the wording of the question.

2. Substitution

Task 2.1 (Written, 10 points)

a) $[y+2/y]\ \exists z.\forall x.(x+y \geqslant z+y)$

$= \exists z.\forall x.(x+y+2 \geqslant z+y+2)$

b) ~~$[y+2/z]$~~ $[y+2/x]\ \exists z.\forall x.(x+y \geqslant z+y)$

x is not a free variable

$\exists z.\forall x.(x+y \geqslant z+y)$

c) $[x+2/y]\ \exists z.\forall x.(x+y \geqslant z+y)$

Rename the variable x that is bound to $\forall x$ first then apply substitution.

$\exists z.\forall x.(x+y \geqslant z+y) \rightarrow \exists z.\forall w.(w+y \geqslant z+y)$

$\therefore [x+2/y]\ \exists z.\forall w.(w+y \geqslant z+y)$

$= \exists z.\forall w.(w+x+2 \geqslant z+x+2)$

d) $[z/x](x \geqslant z \rightarrow (\exists z.\forall x.\ x+y \geqslant z+y) \wedge y > z)$

Rename the free variable z so that both the substituted variable z and the free variable z are different.

$[z/x](x \geqslant w \rightarrow (\exists z.\forall x.\ x+y \geqslant z+y) \wedge y > w)$
$= z \geqslant w \rightarrow (\exists z.\forall x.\ x+y \geqslant z+y) \wedge y > w)$

e) $[z/x](x \geqslant z \rightarrow (\exists x.\ x+y \geqslant z+y) \wedge y > z)$

Rename the free variable z so that both the substituted variable z and the free variable z are different.

$[z/x](x \geqslant w \rightarrow (\exists x.\ x+y \geqslant w+y) \wedge y > w)$
$= z \geqslant w \rightarrow (\exists x.\ x+y \geqslant w+y) \wedge y > w)$

3. Proofs and Proof Outlines

Task 3.1 (Written, 20 points)

a)
```
if  a[0] > a[1]  then
        m := a[0]
else
        m := a[1]
fi
```

b) $\vDash \{T\}\ S\ \{m = max(a[0], a[1])\}$
$S =$ if $a[0] > a[1]$ then $m := a[0]$ else $m := a[1]$ fi

c) Hilbert-style proof

1. $\{a[0] = max(a[0], a[1])\}\ m := a[0]\ \{m = max(a[0], a[1])\}$ Assign

2. $\{T \wedge a[0] \geq a[1]\}\ m := a[0]\ \{m = max(a[0], a[1])\}$ Consequence (1)

3. $\{a[1] = max(a[0], a[1])\}\ m := a[1]\ \{m = max(a[0], a[1])\}$ Assign

4. $\{T \wedge a[0] < a[1]\}\ m := a[1]\ \{m = max(a[0], a[1])\}$ Consequence (3)

5. $\{T\}$ if $a[0] \geq a[1]$ then $m := a[0]$ else $m := a[1]$ fi $\{m = max(a[0], a[1])\}$ if (3, 4)

d) Proof Outline

$\{T\}$

if $a[0] > a[1]$ then $\{T \wedge a[0] \geq a[1]\}$

$\{m = a[0]\}$

$m := a[0]$

else $\{T \wedge a[0] < a[1]\} \Rightarrow \{F\}$

$\{F\} \Rightarrow \{m = a[0]\}$

$m := a[1]$

fi $\{m = a[0]\}$

Task 3.2 (Written, 7 points)

1. $\{x \% 3 = 0\}\ s := x\ \{s \% 3 = 0\}$ Assign

2. $\{x \geq 0 \wedge x \% 3 = 0\}\ s := x\ \{s \% 3 = 0\}$ Consequence (1)

3. $\{x - 1 \% 3 = 0\}\ s := x - 1\ \{s \% 3 = 0\}$ Assign

4. $\{x - 1 \geq 0 \wedge x - 1 \% 3 = 0\}\ s := x - 1\ \{s \% 3 = 0\}$ Consequence (3)

In order to use 'if' to prove, we need a common 'P' for both hoar triples such that the following is satisfied:

$$\frac{\vdash \{P \wedge e\}\ S_1\ \{Q\} \qquad \vdash \{P \wedge \neg e\}\ S_2\ \{Q\}}{\vdash \{P\}\ \text{if } e \text{ then } S_1 \text{ else } S_2 \text{ Fi } \{Q\}}\ \text{if}$$

Therefore, we perform another consequence to change P.

5. $\{x \geq 0 \wedge x \% 3 \neq 0 \wedge x \% 3 = 1\}\ s := x - 1\ \{s \% 3 = 0\}$ Consequence (4)

6. $\{x - 2 \% 3 = 0\}\ s := x - 2\ \{s \% 3 = 0\}$ Assign

7. $\{x - 2 \geq 0 \wedge x - 2 \% 3 = 0\}\ s := x - 2\ \{s \% 3 = 0\}$ Consequence (6)

8. $\{x \geq 0 \wedge x \% 3 \neq 0 \wedge x \% 3 \neq 1\}\ s := x - 2\ \{s \% 3 = 0\}$ Consequence (7)

9. $\{x \geq 0 \wedge x \% 3 \neq 0\}$ if $x \% 3 = 1$ then $s := x - 1$ else $s := x - 2\ \{s \% 3 = 0\}$ if (5, 8)

10. $\{x \geq 0\}$ if $x \% 3 = 0$ then $s := x$ else if $x \% 3 = 1$ then $s := x - 1$ else $s := x - 2\ \{s \% 3 = 0\}$ if (3, 9)

Task 4.1 → 20 hours