Week 12 Tutorial

More Hoare Triples

Joe Scott / Jan Gorzny

Prepared based off of the notes of CS245 Instructors, past and present.

24 March 2017

Plan

1. Hoare Logic
   - Assignment and Implied Inference Rules
2. If-Then-Else
3. The End

Hoare Triple

Assertions of programs take the following form:

1. $(\!|P|\!)$ - a precondition
2. C - a program
3. $(\!|Q|\!)$ - a post condition

That is if a program C satisfies $(\!|P|\!)$ then upon execution, C will satisfy $(\!|Q|\!)$

This is a Hoare Triple.

Proving Correctness

1. $(\!|Assertion|\!)$, precondition
2. Some Code
3. $(\!|ClaimaboutProgram|\!)$, Inference Rule Used
4. More Code
5. $(\!|AnotherClaim|\!)$, Inference Rule
6. More Code
7. ....
8. End Code
9. $(\!|Specification|\!)$, Inference Rule

Correctness

Your proof is partial correct if the proof is valid. Your proof is total correct if the proof is valid and it terminates.

You can not always prove if a program terminates or if it hangs. (The Halting Problem)

Outline

The Assignment Inference Rule

$$\begin{array}{r|l} 1 & \varnothing \\ \hline 2 & (\!|Q[E/x]|\!)x = E(\!|Q|\!) \end{array}$$

1. $(\!|y = 2|\!)x = y(\!|x = 2|\!)$
2. $(\!|y \leq 2|\!)x = y(\!|x \leq 2|\!)$
3. $(\!|y + 1 = 7|\!)x = y + 1(\!|x = 7|\!)$

Inference rules of Implication

Precondition Strengthening

$$
\begin{array}{ll|l}
1 & & P \implies P', \quad (\!|P'|\!)\, C\, (\!|Q|\!) \\
\hline
2 & & (\!|P|\!)\ C\ (\!|Q|\!)
\end{array}
$$

Postcondition Weakening

$$
\begin{array}{ll|l}
1 & & Q' \implies Q, \quad (\!|P|\!)\, C\, (\!|Q'|\!) \\
\hline
2 & & (\!|P|\!)\ C\ (\!|Q|\!)
\end{array}
$$

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!|((x \geq 0) \wedge (0 = 0))|\!)$
2. $y = 0$
3. $(\!|(x + y \geq 0)|\!)$

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $\llparenthesis ((x \geq 0) \wedge (0 = 0)) \rrparenthesis$
2. $y = 0$
3. $\llparenthesis (x + y \geq 0) \rrparenthesis$

1. $\llparenthesis ((x \geq 0) \wedge (0 = 0)) \rrparenthesis$

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!|((x \geq 0) \wedge (0 = 0))|\!)$
2. $y = 0$
3. $(\!|(x + y \geq 0)|\!)$

1. $(\!|((x \geq 0) \wedge (0 = 0))|\!)$
2. $y = 0$
3. $(\!|((x \geq 0) \wedge (y = 0))|\!)$ Assignment

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $\llparenthesis((x \geq 0) \wedge (0 = 0))\rrparenthesis$
2. $y = 0$
3. $\llparenthesis(x + y \geq 0)\rrparenthesis$

1. $\llparenthesis((x \geq 0) \wedge (0 = 0))\rrparenthesis$
2. $y = 0$
3. $\llparenthesis((x \geq 0) \wedge (y = 0))\rrparenthesis$ Assignment

Observe that we then can prove $(((x \geq 0) \wedge (y = 0)) \implies (x + y \geq 0))$ to invoke postcondition weakening.
Because there are no loops, the program will terminate, thus we have also proved the total correctness.

Problem 2

For the following program, correctly identify the missing pre- and post-conditions.

1. $((x = ??? \wedge y = ???)$
2. $x = x + y;$
3. $y = x - y;$
4. $x = x - y;$
5. $((x = y_0) \wedge (y = x_0))$

Problem 2

For the following program, correctly identify the missing pre- and post-conditions.

1. $((x = ??? \wedge y = ???)$
2. $x = x + y;$
3. $y = x - y;$
4. $x = x - y;$
5. $((x = y_0) \wedge (y = x_0))$

Solution: I claim that the required precondition is :
$(\!|((x = x_0) \wedge (y = y_0))|\!)$.

Problem 3

For the following program, correctly identify the missing pre- and post-conditions.

1. $(\!|....|\!)$
2. $x = x + y;$
3. .... , Assignment
4. $y = x - y;$
5. .... , Assignment
6. $x = x - y;$
7. ..... , Assignment

Problem 3

For the following program, correctly identify the missing pre- and post-conditions.

1. $(\!|....|\!)$
2. $x = x + y;$
3. .... , Assignment
4. $y = x - y;$
5. .... , Assignment
6. $x = x - y;$
7. $(\!|((x = y_0) \wedge (y = x_0))|\!)$, Assignment

Problem 3

For the following program, correctly identify the missing pre- and post-conditions.

1. $(\!|....|\!)$
2. $x = x + y;$
3. .... , Assignment
4. $y = x - y;$
5. $(\!|((x - y = y_0) \wedge (y = x_0))|\!)$, Assignment
6. $x = x - y;$
7. $(\!|((x = y_0) \wedge (y = x_0))|\!)$, Assignment

Problem 3

For the following program, correctly identify the missing pre- and post-conditions.

1. $(\!|\ldots|\!)$
2. $x = x + y;$
3. $(\!|((x - (x - y) = y_0) \wedge ((x - y) = x_0))|\!)$, Assignment
4. $y = x - y;$
5. $(\!|((x - y = y_0) \wedge (y = x_0))|\!)$, Assignment
6. $x = x - y;$
7. $(\!|((x = y_0) \wedge (y = x_0))|\!)$, Assignment

Problem 3

For the following program, correctly identify the missing pre- and post-conditions.

1. $(\!|(((x+y)-((x+y)-y)=y_0)\wedge(((x+y)-y)=x_0)|\!)$
2. $x = x + y;$
3. $(\!|((x-(x-y)=y_0)\wedge((x-y)=x_0))|\!)$, Assignment
4. $y = x - y;$
5. $(\!|((x-y=y_0)\wedge(y=x_0))|\!)$, Assignment
6. $x = x - y;$
7. $(\!|((x=y_0)\wedge(y=x_0))|\!)$, Assignment

From here we can show
$(\!|(((x+y)-((x+y)-y)=y_0)\wedge(((x+y)-y)=x_0)|\!)$

Plan

if-then else rules

if then else

$$\begin{array}{r|l} 1 & (\!|P \wedge B|\!)\ C_1\ (\!|Q|\!), (\!|P \wedge \neg B|\!)\ C_2\ (\!|Q|\!) \\ \hline 2 & (\!|P \wedge B|\!)\ \mathit{if}\,(B)\ C_1\ \mathit{else}\ C_2 (\!|Q|\!) \end{array}$$

if then

$$\begin{array}{r|l} 1 & (\!|P \wedge B|\!)\ C\ (\!|Q|\!), (P \wedge \neg B) \implies Q|\!) \\ \hline 2 & (\!|P|\!)\ \mathit{if}\,(B)\ C (\!|Q|\!) \end{array}$$

Problem 4

Verify that at the end of the following program M contains a value greater than or equal to both of A and B.

```
if (A > B) {
    M = A;
} else {
    M = B;
}
```

What is the pre/post condition?

Problem 4 (cont)

The proof some look something like this:

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. .... , if then else
4. .... , ...,implied(1)
5. $M = A$
6. ....
7. } else {
8. .... if then else
9. ....,implied(2)
10. $M = B$
11. ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Problem 4 (cont)

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $\quad (\!|A > B|\!)$, if then else
4. $\quad$ .... , ...,implied(1)
5. $\quad M = A$
6. $\quad$ ....
7. } else {
8. $\quad$ .... if then else
9. $\quad$ ....,implied(2)
10. $\quad M = B$
11. $\quad$ ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Problem 4 (cont)

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $(\!|A > B|\!)$, if then else
4. $(\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $M = A$
6. ....
7. } else {
8. .... if then else
9. ....,implied(2)
10. $M = B$
11. ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Problem 4 (cont)

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $(\!|A > B|\!)$, if then else
4. $(\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $M = A$
6. $(\!|((M \geq A) \wedge (M \geq B))|\!)$, assignment
7. } else {
8. .... if then else
9. ....,implied(2)
10. $M = B$
11. ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Problem 4 (cont)

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $\quad (\!|A > B|\!)$, if then else
4. $\quad (\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $\quad M = A$
6. $\quad (\!|((M \geq A) \wedge (M \geq B))|\!)$, assignment

What did we do? Due to the semantics of if,then,else in programs it helps to prove lemmas for each condition.
Here, we claimed the following:

$$((A > B) \implies ((A \geq A) \wedge (A \geq B)))$$

We need to prove this however. Exercise!

Problem 4 (cont)

Now finish the problem.

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $\qquad (\!|A > B|\!)$, if then else
4. $\qquad (\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $\qquad M = A$
6. $\qquad (\!|((M \geq A) \wedge (M \geq B))|\!)$, assignment
7. } else {
8. $\qquad$ .... if then else
9. $\qquad$ ....,implied(2)
10. $\qquad M = B$
11. $\qquad$ ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Problem 4 (cont)

Now finish the problem.

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $(\!|A > B|\!)$, if then else
4. $(\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $M = A$
6. $(\!|((M \geq A) \wedge (M \geq B))|\!)$, assignment
7. } else {
8. $(\neg(A > B))$ if then else
9. ....,implied(2)
10. $M = B$
11. ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Problem 4 (cont)

Now finish the problem.

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $\quad$ $(\!|A > B|\!)$, if then else
4. $\quad$ $(\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $\quad$ $M = A$
6. $\quad$ $(\!|((M \geq A) \wedge (M \geq B))|\!)$, assignment
7. } else {
8. $\quad$ $(\neg(A > B))$ if then else
9. $\quad$ $(\!|((B \geq A)) \wedge (B \geq B))|\!)$,implied(2)
10. $\quad$ $M = B$
11. $\quad$ ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Exercise: prove implied(2)

Problem 4 (cont)

Now finish the problem.

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $(\!|A > B|\!)$, if then else
4. $(\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $M = A$
6. $(\!|((M \geq A) \wedge (M \geq B))|\!)$, assignment
7. } else {
8. $(\neg(A > B))$ if then else
9. $(\!|((B \geq A)) \wedge (B \geq B))|\!)$,implied(2)
10. $M = B$
11. ....
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Problem 4 (cont)

Now finish the problem.

1. $(\!|true|\!)$
2. if $(A > B)$ {
3. $\quad (\!|A > B|\!)$, if then else
4. $\quad (\!|((A \geq A) \wedge (A \geq B))|\!)$,implied(1)
5. $\quad M = A$
6. $\quad (\!|((M \geq A) \wedge (M \geq B))|\!)$, assignment
7. } else {
8. $\quad (\neg(A > B))$ if then else
9. $\quad (\!|((B \geq A)) \wedge (B \geq B))|\!)$,implied(2)
10. $\quad M = B$
11. $\quad (\!|((M \geq A)) \wedge (M \geq B))|\!)$, assignment
12. }
13. $(\!|((M \geq A) \wedge (M \geq B))|\!)$

Plan

The end

That's it folks. Feel free to hang out and ask questions.

These slides are based off of the tutorial notes and lecture slides provided to you online.
If you want a copy feel free to email me. The are also available on my personal website joe-scott.net

IA Email:

IA	email
Jan Gorzny	jgorzny
Joe Scott	j29scott

Jan and Joe have an office hour Mondays at 3pm in the Tutorial Center in MC.

Instructor Office Hours:

Instructor	Time	Room	Email
Trefler	Tue, Thur 4:00pm	DC 2336	trefler
Rahkooy	Tue, Thur 4:00pm	DC 2302B	hamid.rahkooy