CSCI 740 - Programming Language Theory

Lecture 20

Hoare Rules

Instructor: Hossein Hojjat

October 20, 2017

Hoare Rules: Summary

$$\frac{}{\vdash \{A[x \mapsto e]\}\ x := e\ \{A\}} \qquad \frac{\vdash \{A \land b\}\ c_1\ \{B\} \qquad \vdash \{A \land \neg b\}\ c_2\ \{B\}}{\vdash \{A\}\ \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\ \{B\}}$$

$$\frac{\vdash \{A \land b\}\ c\ \{A\}}{\vdash\ \{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{A \land \neg b\}} \qquad \frac{\vdash \{A\}\ c_1\ \{C\} \qquad \vdash \{C\}\ c_2\ \{B\}}{\vdash \{A\}\ c_1\ ;\ c_2\ \{B\}}$$

$$\frac{\vdash A' \Rightarrow A \quad \vdash \{A\}\ c\ \{B\} \quad \vdash\ B \Rightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

Hoare Rules: Conditional

$$\frac{\vdash \{A \wedge b\}\ c_1\ \{B\} \qquad \vdash \{A \wedge \neg b\}\ c_2\ \{B\}}{\vdash \{A\}\ \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\ \{B\}}$$

- Suppose we know A holds before if statement and want to show B holds afterwards
- At beginning of `then` branch, we know $A \wedge b$ we prove B holds after executing the branch
- At beginning of `else` branch, we know $A \wedge \neg b$ we prove B holds after executing the branch

Exercise

$$\frac{}{\vdash \{A[x \mapsto e]\}\ x := e\ \{A\}} \qquad \frac{\vdash \{A \wedge b\}\ c_1\ \{B\} \qquad \vdash \{A \wedge \neg b\}\ c_2\ \{B\}}{\vdash \{A\}\ \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\ \{B\}}$$

$$\frac{\vdash \{A\}\ c_1\ \{C\} \qquad \vdash \{C\}\ c_2\ \{B\}}{\vdash \{A\}\ c_1\ ;\ c_2\ \{B\}} \qquad \frac{\vdash A' \Rightarrow A \quad \vdash \{A\}\ c\ \{B\} \quad \vdash\ B \Rightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- Under what condition $\{x > 0\}$ holds after the following statement:

$$\texttt{if}\ (x < 0)\ \texttt{then}\ x := -x\ \texttt{else}\ x := x$$

Exercise

$$\frac{}{\vdash \{A[x \mapsto e]\}\ x := e\ \{A\}} \qquad \frac{\vdash \{A \wedge b\}\ c_1\ \{B\} \qquad \vdash \{A \wedge \neg b\}\ c_2\ \{B\}}{\vdash \{A\}\ \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\ \{B\}}$$

$$\frac{\vdash \{A\}\ c_1\ \{C\} \qquad \vdash \{C\}\ c_2\ \{B\}}{\vdash \{A\}\ c_1\ ;\ c_2\ \{B\}} \qquad \frac{\vdash A' \Rightarrow A \quad \vdash \{A\}\ c\ \{B\} \quad \vdash\ B \Rightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- Under what condition $\{x > 0\}$ holds after the following statement:

$$\texttt{if}\ \ (x < 0)\ \ \texttt{then}\ \ x := -x\ \ \texttt{else}\ \ x := x$$

Solution: x should not be 0 initially

$$\frac{\dfrac{\vdash \{(x < 0)\}\ x := -x\ \{x > 0\}}{\vdash \{(x \neq 0) \wedge (x < 0)\}\ x := -x\ \{x > 0\}} \qquad \dfrac{\vdash \{(x > 0)\}\ x := -x\ \{x > 0\}}{\vdash \{(x \neq 0) \wedge (x \geq 0)\}\ x := x\ \{x > 0\}}}{\vdash \{x \neq 0\}\ \texttt{if}\ (x < 0)\ \texttt{then}\ x := -x\ \texttt{else}\ x := x + 1\ \{x > 0\}}$$

Hoare Rules: Sequences

$$\frac{\vdash \{A\}\ c_1\ \{C\} \qquad \vdash \{C\}\ c_2\ \{B\}}{\vdash \{A\}\ c_1\ ;\ c_2\ \{B\}}$$

- To prove a sequence $\{A\}\ c1; c2\ \{B\}$ we must find an intermediate assertion C
- Implied by A after c_1 and implying B after c_2
  - (often denoted $\{A\}\ c_1\ \{C\}\ c_2\ \{B\}$)

Exercise

$$\frac{\vdash \{A\}\ c_1\ \{C\} \qquad \vdash \{C\}\ c_2\ \{B\}}{\vdash \{A\}\ c_1\ ;\ c_2\ \{B\}}$$

- What is the intermediate assertion to prove the following Hoare triple?

$$\{\mathsf{true}\}\ x := 1; y := x\ \{x = 1 \wedge y = 1\}$$

Exercise

$$\frac{\vdash \{A\}\ c_1\ \{C\} \qquad \vdash \{C\}\ c_2\ \{B\}}{\vdash \{A\}\ c_1\ ;\ c_2\ \{B\}}$$

- What is the intermediate assertion to prove the following Hoare triple?

$$\{\mathsf{true}\}\ x := 1; y := x\ \{x = 1 \wedge y = 1\}$$

Solution: $(x = 1)$

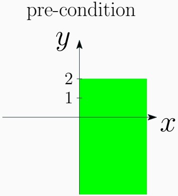
$$\frac{\vdash \{\mathsf{true}\}\ x := 1\ \{x = 1\} \qquad \vdash \{x = 1\}\ y := x\ \{x = 1 \wedge y = 1\}}{\vdash \{\mathsf{true}\}\ x := 1; y := x\ \{x = 1 \wedge y = 1\}}$$

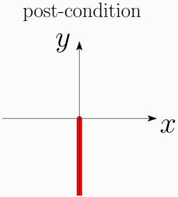
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

$$\frac{\vdash A' \Rightarrow A \;\; \vdash \{A\}\ c\ \{B\} \;\; \vdash\ B \Rightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- Suppose we can prove $\{x \geq 0 \wedge y < 2\}\ c\ \{x = 0 \wedge y \leq 0\}$
- Which of the following Hoare triples can we prove?





$$\begin{array}{lcl} \{x \geq 0 \wedge y \leq 0\} & c & \{x = 0 \wedge y \leq 0\} \\ \{x \geq 0 \wedge y \geq 0\} & c & \{x = 0 \wedge y \leq 0\} \\ \{x = 5\} & c & \{y \leq 1\} \end{array}$$

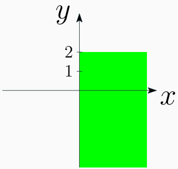
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

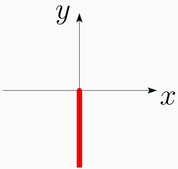
$$\frac{\vdash A' \Rightarrow A \quad \vdash \{A\}\ c\ \{B\} \quad \vdash\ B \Rightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- Suppose we can prove $\{x \geq 0 \wedge y < 2\}\ c\ \{x = 0 \wedge y \leq 0\}$
- Which of the following Hoare triples can we prove?

pre-condition



post-condition



$\{x \geq 0 \wedge y \leq 0\}$	c	$\{x = 0 \wedge y \leq 0\}$	✓
$\{x \geq 0 \wedge y \geq 0\}$	c	$\{x = 0 \wedge y \leq 0\}$	
$\{x = 5\}$	c	$\{y \leq 1\}$	

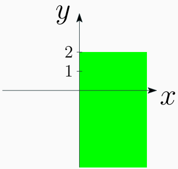
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

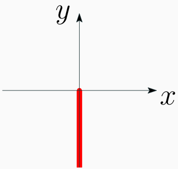
$$\frac{\vdash A' \Rightarrow A \quad \vdash \{A\}\ c\ \{B\} \quad \vdash\ B \Rightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- Suppose we can prove $\{x \geq 0 \land y < 2\}\ c\ \{x = 0 \land y \leq 0\}$
- Which of the following Hoare triples can we prove?

pre-condition



post-condition



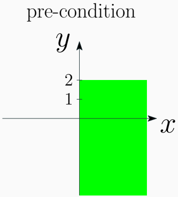
$\{x \geq 0 \land y \leq 0\}$	c	$\{x = 0 \land y \leq 0\}$	✓
$\{x \geq 0 \land y \geq 0\}$	c	$\{x = 0 \land y \leq 0\}$	✗
$\{x = 5\}$	c	$\{y \leq 1\}$	

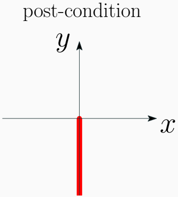
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

$$\frac{\vdash A' \Rightarrow A \quad \vdash \{A\}\ c\ \{B\} \quad \vdash\ B \Rightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- Suppose we can prove $\{x \geq 0 \wedge y < 2\}\ c\ \{x = 0 \wedge y \leq 0\}$
- Which of the following Hoare triples can we prove?





$\{x \geq 0 \wedge y \leq 0\}$	c	$\{x = 0 \wedge y \leq 0\}$	✓
$\{x \geq 0 \wedge y \geq 0\}$	c	$\{x = 0 \wedge y \leq 0\}$	✗
$\{x = 5\}$	c	$\{y \leq 1\}$	✗

Hoare Rules: Loops

$$\frac{\vdash \{A \land b\}\ c\ \{A\}}{\vdash\ \{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{A \land \neg b\}}$$

- Assertion A is a loop invariant: assertion that remains true before and after every iteration of the loop

$$\vdash \{A \land b\}\ c\ \{A\}$$

- Both a pre-condition for the loop (holds before the first iteration) and a post-condition for the loop (holds after the last iteration)

Hoare Rules: Loops

$$\frac{\vdash \{A \wedge b\}\ c\ \{A\}}{\vdash\ \{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{A \wedge \neg b\}}$$

Loop Invariant:

- What has been done so far and what remains to be done
- That nothing has been done initially
- That nothing remains to be done when b is false

Example

- Consider the statement $(x, n \in \mathbb{Z})$

$$S = \texttt{while } x < n \texttt{ do } x := x + 1$$

- Prove validity of $\{x \leq n\}\ S\ \{x \geq n\}$
- First Step: What is appropriate loop invariant?

Example

- Consider the statement $(x, n \in \mathbb{Z})$

$$S = \texttt{while } x < n \texttt{ do } x := x + 1$$

- Prove validity of $\{x \leq n\}\ S\ \{x \geq n\}$
- First Step: What is appropriate loop invariant? $x \leq n$
- First, we need to prove $\{x \leq n \land x < n\}\ x := x + 1\ \{x \leq n\}$
- Required proof rules: assignment, precondition strengthening

$$\dfrac{\dfrac{\vdash \{x \leq n[x \mapsto x+1]\}\ x := x+1\ \{x \leq n\}}{\vdash \{x + 1 \leq n\}\ x := x+1\ \{x \leq n\}} \qquad x \leq n \land x < n \Rightarrow x + 1 \leq n}{\vdash \{x \leq n \land x < n\}\ x := x+1\ \{x \leq n\}}$$

Example

- Let's instantiate proof rule for `while` with this loop invariant:

$$\frac{\vdash \{x \leq n \land x < n\}\ x := x + 1\ \{x \leq n\}}{\vdash \{x \leq n\}\ \texttt{while}\ x < n\ \texttt{do}\ x := x + 1\ \{x \leq n \land \neg(x < n)\}}$$

- Recall: We wanted to prove the Hoare triple

$$\{x \leq n\}\ S\ \{x \geq n\}$$

- In addition to proof rule for while, what other rule do we need?

Example

- Let's instantiate proof rule for `while` with this loop invariant:

$$\frac{\vdash \{x \leq n \land x < n\}\ x := x + 1\ \{x \leq n\}}{\vdash \{x \leq n\}\ \texttt{while}\ x < n\ \texttt{do}\ x := x + 1\ \{x \leq n \land \neg(x < n)\}}$$

- Recall: We wanted to prove the Hoare triple

$$\{x \leq n\}\ S\ \{x \geq n\}$$

- In addition to proof rule for while, what other rule do we need? postcondition weakening

Proving Loops

$$\frac{A \Rightarrow I \qquad \vdash \{b \wedge I\}\ c\ \{I\} \qquad I \wedge \neg b \Rightarrow B}{\vdash\ \{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{B\}}$$

To prove the Hoare triple $\{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{B\}$

- Find I and prove it is an invariant: $\vdash \{b \wedge I\}\ c\ \{I\}$
- Prove I is *true* at the start: $A \Rightarrow I$
- Prove B is *true* after the loop: $I \wedge \neg b \Rightarrow B$

Exercise

- Suppose we add a for loop construct to IMP

$$\texttt{for } x := e_1 \texttt{ until } e_2 \texttt{ do } S$$

- Initializes x to e_1, increments x by 1 in each iteration and terminates when $x > e_2$
- Write a proof rule for this for loop construct