Introduction to Formal Methods

Lecture 7

Hoare Logic Rules

Hossein Hojjat & Fatemeh Ghassemi

October 14, 2018

Review of Key Definitions

Hoare triple:

$$\{P\}\ r\ \{Q\} \Leftrightarrow \forall s, s' \in S.\big((s \in P \land (s, s') \in r) \to s' \in Q\big)$$

$\{P\}$ does not denote a singleton set containing P but is just a notation for an "assertion" around a command. Likewise for $\{Q\}$.

Strongest postcondition:

$$\mathit{sp}(P, r) = \{s' \mid \exists s. s \in P \land (s, s') \in r\}$$

Weakest precondition:

$$\mathit{wp}(r, Q) = \{s \mid \forall s'. (s, s') \in r \to s' \in Q\}$$

Exercise: Prove *wp* Distributivity

$$\mathit{wp}(r_1 \cup r_2, Q) = \mathit{wp}(r_1, Q) \cap \mathit{wp}(r_2, Q)$$

Exercise: Prove *wp* Distributivity

$$\textit{wp}(r_1 \cup r_2, Q) = \textit{wp}(r_1, Q) \cap \textit{wp}(r_2, Q)$$

$$\begin{aligned}
\textit{wp}(r_1 \cup r_2, Q) &= \{s \mid \forall s'.(s, s') \in r_1 \cup r_2 \to s' \in Q\} \\
&= \{s \mid \forall s'.((s, s') \in r_1 \vee (s, s') \in r_2) \to s' \in Q\} \\
&= \{s \mid \forall s'.\neg((s, s') \in r_1 \vee (s, s') \in r_2) \vee s' \in Q\} \\
&= \{s \mid \forall s'.(\neg(s, s') \in r_1 \wedge \neg(s, s') \in r_2) \vee s' \in Q\} \\
&= \{s \mid \forall s'.(\neg(s, s') \in r_1 \vee s' \in Q) \wedge (\neg(s, s') \in r_2 \vee s' \in Q)\} \\
&= \{s \mid \forall s'.((s, s') \in r_1 \to s' \in Q) \wedge ((s, s') \in r_2 \to s' \in Q)\} \\
&= \{s \mid (\forall s'.(s, s') \in r_1 \to s' \in Q) \wedge (\forall s'.(s, s') \in r_2 \to s' \in Q)\} \\
&= \{s \mid \forall s'.(s, s') \in r_1 \to s' \in Q\} \cap \{s \mid \forall s'.(s, s') \in r_2 \to s' \in Q\} \\
&= \textit{wp}(r_1, Q) \cap \textit{wp}(r_2, Q)
\end{aligned}$$

Proving Correctness

- Key problem: How to prove valid Hoare triples?

$$\{P\}\ r\ \{Q\} \Leftrightarrow \forall s, s' \in S.\big((s \in P \wedge (s, s') \in r) \rightarrow s' \in Q\big)$$

- Use notation $\vdash \{P\}\ S\ \{Q\}$ to indicate that we can prove validity of Hoare triple
- Hoare gave a sound and (relatively-) complete proof system that allows semi-mechanizing correctness proofs

C. A. R. Hoare, "An Axiomatic Basis for Computer Programming", CACM, 12(1969) 576-580

Inference Rules

- Proof rules in Hoare logic are written as inference rules:

$$\frac{\vdash \{P_1\}\ S_1\ \{Q_1\} \cdots \vdash \{P_n\}\ S_n\ \{Q_n\}}{\vdash \{P\}\ S\ \{Q\}}$$

- Says if Hoare triples $\{P_1\}\ S_1\ \{Q_1\}, \cdots, \{P_n\}\ S_n\ \{Q_n\}$ are provable in our proof system, then $\{P\}\ S\ \{Q\}$ is also provable
- Not all rules have hypotheses: these correspond to bases cases in the proof
- Rules with hypotheses correspond to inductive cases in proof

Background: Inference Systems

- Example inference rule:

All great universities have smart students	Premise 1
U Tehran is a great university	Premise 2
U Tehran has smart students	Conclusion

- Example inference rule:

e_1 has type `int`	Premise 1
e_2 has type `int`	Premise 2
$e_1 + e_2$ has type `int`	Conclusion

Background: Inference Systems

- An inference system has two parts:
  1. Definition of **Judgments**
     - Judgment: statement asserting a certain fact for an object
  2. Finite set of **Inference Rules**

- An inference rule has:
  1. a finite number of judgments P_1, P_2, $\cdots$, P_n as premises;
  2. a single judgment C as conclusion
- If a rule has no premises, it is called an **axiom**

$$\frac{P_1 \qquad P_2 \qquad \cdots \qquad P_n}{C} \text{ (Rule name)}$$

Premises above the line (0 or more)
Conclusion below the line

Example: Use an inference system to define the set of even numbers

- Judgment: $\mathit{Even}(n)$ asserts that n is an even number
- Inference rules:

- Axiom:

$$\frac{}{\mathit{Even}(0)}\ \text{(Even0)}$$

- Successor Rule:

$$\frac{\mathit{Even}(n)}{\mathit{Even}(n+2)}\ \text{(EvenS)}$$

Background: Derivation Tree

$$\frac{}{\textit{Even}(0)}\ (\text{Even0}) \qquad\qquad \frac{\textit{Even}(n)}{\textit{Even}(n+2)}\ (\text{EvenS})$$

- To derive more judgments we create **trees** of inference rules

$$\cfrac{\cfrac{\cfrac{\cfrac{}{\textit{Even}(0)}\ (\text{Even0})}{\textit{Even}(2)}\ (\text{EvenS})}{\textit{Even}(4)}\ (\text{EvenS})}{\textit{Even}(6)}\ (\text{EvenS})$$

Background: Derivation Tree

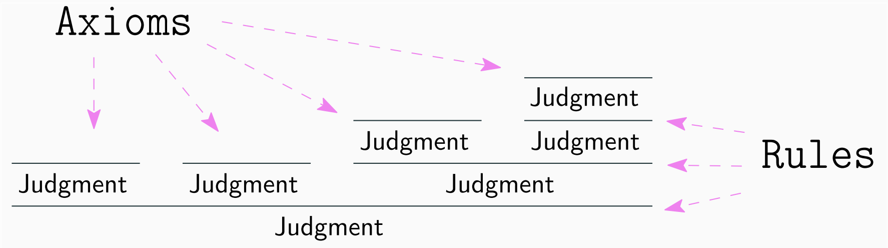
$$\frac{}{\textit{Even}(0)}\ (\text{Even0}) \qquad\qquad \frac{\textit{Even}(n)}{\textit{Even}(n+2)}\ (\text{EvenS})$$

- To derive more judgments we create **trees** of inference rules

$$\cfrac{\cfrac{\cfrac{\cfrac{}{\textit{Even}(0)}\ (\text{Even0})}{\textit{Even}(2)}\ (\text{EvenS})}{\textit{Even}(4)}\ (\text{EvenS})}{\textit{Even}(6)}\ (\text{EvenS})$$

- Does *Even*(1) hold?
- No, because there exists no possible derivation

Background: Derivation Tree



Background: Less-than (Example)

Example: Use an inference system to define the less-than relation

- Judgment: $n < m$ asserts that n is smaller than m
- Inference rules:

- Axiom:

$$\frac{}{n < n+1}\ (\text{Suc})$$

- Transitivity Rule:

$$\frac{k < n \qquad n < m}{k < m}\ (\text{Trans})$$

Exercise: Prove $0 < 3$.

Understanding Proof Rule for Assignment

- Consider the assignment $x := y$ and post-condition $x > 5$
- What do we need before the assignment so that $x > 5$ holds afterwards?
- Consider $i := i + 1$ and post-condition $i > 1$
- What do we need to know before the assignment so that $i > 1$ holds afterwards?

Proof Rule for Assignment

$$\frac{}{\vdash \{A[x := e]\}\ x := e\ \{A\}}$$

To make sure that Q holds for x after the assignment of e to x, it suffices to make sure that Q holds for e before the assignment

Using this rule, which of these are provable?

- $\{y = 4\}\ x := 4\ \{y = x\}$
- $\{x + 1 = n\}\ x := x + 1\ \{x = n\}$
- $\{y = x\}\ y := 2\ \{y = x\}$
- $\{z = 3\}\ y := x\ \{z = 3\}$

Exercise

Your friend suggests the following proof rule for assignment:

$$\frac{}{\vdash \{\textit{True}\}\ x := e\ \{x = e\}}$$

Is the proposed proof rule correct?

Motivation for Consequence Rule

- Is the Hoare triple $\vdash \{z = 0\}\ y := x\ \{y = x\}$ valid?
- Is this Hoare triple provable using our assignment rule?
- Instantiating the assignment rule, we get:

$$\begin{aligned}\vdash \{y = x[y := x]\}\ y := x\ \{y = x\} \\ \vdash \{x = x\}\ y := x\ \{y = x\} \\ \vdash \{\mathit{True}\}\ y := x\ \{y = x\}\end{aligned}$$

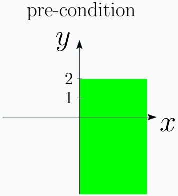
- Intuitively, if we can prove $y = x$ w/o any assumptions, we should also be able to prove it if we do make assumptions!

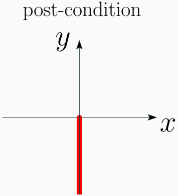
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

$$\frac{\vdash A' \to A \ \ \vdash \{A\}\ c\ \{B\} \ \ \vdash\ B \to B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- 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?





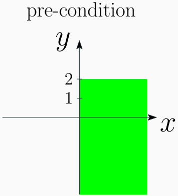
$$\begin{array}{lcl}
\{x \geq 0 \wedge y \leq 0\} & c & \{x = 0 \wedge y \leq 0\} \\
\{x \geq 0 \wedge y \geq 0\} & c & \{x = 0 \wedge y \leq 0\} \\
\{x = 5\} & c & \{y \leq 1\}
\end{array}$$

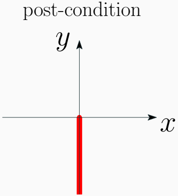
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

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

- 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	$\{y \leq 1\}$	

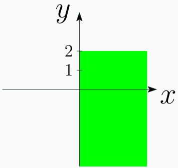
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

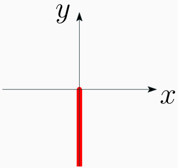
$$\frac{\vdash A' \to A \quad \vdash \{A\}\; c\; \{B\} \quad \vdash \; B \to B'}{\vdash \{A'\}\; c\; \{B'\}}$$

- 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	$\{y \leq 1\}$	

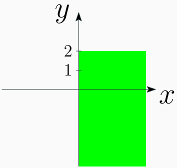
Hoare Rules: Consequence

Pre-condition strengthening, Post-condition weakening

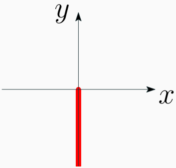
$$\frac{\vdash A' \to A \quad \vdash \{A\}\ c\ \{B\} \quad \vdash\ B \to B'}{\vdash \{A'\}\ c\ \{B'\}}$$

- 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	$\{y \leq 1\}$	✗

Example

Using this rule and rule for assignment, we can now prove
$\vdash \{z = 0\}\ y := x\ \{y = x\}$

Proof:

$$\dfrac{\dfrac{\vdash \{y = x[y := x]\}\ y := x\ \{y = x\}}{\vdash \{\mathit{True}\}\ y := x\ \{y = x\}} \qquad z = 0 \to \mathit{True}}{\vdash \{z = 0\}\ y := x\ \{y = x\}}$$

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?

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

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: 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

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

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

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

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

Exercise

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

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

- 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: Loops

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

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

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

- 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 $\quad (x, n \in \mathbb{Z})$

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

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

Example

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

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

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

$$\dfrac{\dfrac{\vdash \{x \leq n[x := x+1]\}\ x := x+1\ \{x \leq n\}}{\vdash \{x + 1 \leq n\}\ x := x+1\ \{x \leq n\}} \qquad x \leq n \wedge x < n \rightarrow x + 1 \leq n}{\vdash \{x \leq n \wedge x < n\}\ x := x+1\ \{x \leq n\}}$$

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:

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

- Recall: We wanted to prove the Hoare triple

$$\{x \le n\}\ S\ \{x \ge n\}$$

- 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

- Let's consider the for-loop statement:

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

- 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

Hoare Rules: Summary

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

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

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