CS 4110
Programming Languages & Logics

Lecture 10
Hoare Logic
Overview

Last time

- Assertion language: \( P \)
- Assertion satisfaction: \( \sigma \models P \)
- Assertion validity: \( \models P \)

- Partial/total correctness statements: \( \{P\} \text{ c } \{Q\} \) and \( [P] \text{ c } [Q] \)
- Partial correctness satisfaction \( \sigma \models \{P\} \text{ c } \{Q\} \)
- Partial correctness validity: \( \models \{P\} \text{ c } \{Q\} \)

Today

- Hoare Logic
- Examples
- Metatheory
Definition (Partial correctness satisfaction)

A partial correctness statement \( \{ P \} \ c \ \{ Q \} \) is satisfied by store \( \sigma \) and interpretation \( I \), written \( \sigma \models_I \{ P \} \ c \ \{ Q \} \), if:

\[
\forall \sigma'. \text{ if } \sigma \models_I P \text{ and } C[c] \sigma = \sigma' \text{ then } \sigma' \models_I Q
\]

Definition (Partial correctness validity)

A partial correctness statement is valid (written \( \models \{ P \} \ c \ \{ Q \} \)), if it is satisfied by any store and interpretation: \( \forall \sigma, I. \ \sigma \models_I \{ P \} \ c \ \{ Q \} \).
Hoare Logic

Want a way to prove partial correctness statements valid...

... without having to consider explicitly every store and interpretation!
Hoare Logic

Want a way to prove partial correctness statements valid...

... without having to consider explicitly every store and interpretation!

Idea: Develop a formal proof system as an inductively-defined set! Every member of the set will be a valid partial correctness statement.

We’ll define a judgment of the form $\vdash \{P\} c \{Q\}$ using inference rules.
Hoare Logic: Skip

$$\vdash \{P\} \text{skip} \{P\}$$

SKIP
Hoare Logic: Assignment (this one’s weird)

\[ \vdash \{P[a/x]\} x := a \{P\} \quad \text{ASSIGN} \]
Hoare Logic: Assignment (this one’s weird)

\[ \vdash \{ P[a/x] \} \ x := \ a \ { P } \]

Notation: \( P[a/x] \) denotes substitution of \( a \) for \( x \) in \( P \)
Hoare Logic: Assignment (this one’s weird)

\[ \vdash \{P[a/x]\} \ x := a \ \{P\} \quad \text{Assign} \]

**Notation:** $P[a/x]$ denotes substitution of $a$ for $x$ in $P$

\[ \{ \quad \} \ x := 5 \ \{x = 5\} \]
Hoare Logic: Assignment (this one’s weird)

\[ \vdash \{P[a/x]\} \ x := \ a \ \{P\} \quad \text{Assign} \]

**Notation:** $P[a/x]$ denotes substitution of $a$ for $x$ in $P$

\[ \{5 = 5\} \ x := 5 \ \{x = 5\} \]
Hoare Logic: Broken Assignment

The rule for assignment is definitely not:

\[
\vdash \{ P \} \ x := \ a \ \{ P[a/x] \} \ \text{BROKENASSIGN}
\]
Hoare Logic: Broken Assignment

The rule for assignment is definitely not:

\[ \vdash \{P\} x := a \{P[a/x]\} \quad \text{BROKENASSIGN} \]

\[ \{x = 0\} x := 5 \{ \} \]
The rule for assignment is definitely not:

\[ \vdash \{P\} x := a \{P[a/x]\} \]

\[ \{x = 0\} x := 5 \{5 = 0\} \]
Hoare Logic: Broken Assignment

The rule for assignment is definitely not:

\[
\vdash \{P\} x := a \{P[a/x]\} \quad \text{\textsc{BrokenAssign}}
\]

\[
\{x = 0\} x := 5 \{5 = 0\}
\]

\[
\vdash \{P\} x := a \{P[x/a]\} \quad \text{\textsc{BrokenAssign2}}
\]
Hoare Logic: Broken Assignment

The rule for assignment is definitely not:

\[
\color{red}{\vdash \{P\} \ x := \ a \ \{P[a/x]\}} \quad \text{BROKENASSIGN}
\]

\[
\{x = 0\} \ x := 5 \ \{5 = 0\}
\]

\[
\color{red}{\vdash \{P\} \ x := \ a \ \{P[x/a]\}} \quad \text{BROKENASSIGN2}
\]

\[
\{x = 0\} \ x := 5 \ \{
\}
\]
Hoare Logic: Broken Assignment

The rule for assignment is definitely not:

\[
\vdash \{P\} \ x := a \ \{P[a/x]\} \quad \text{BROKENASSIGN}
\]

\[
\{x = 0\} \ x := 5 \ \{5 = 0\}
\]

\[
\vdash \{P\} \ x := a \ \{P[x/a]\} \quad \text{BROKENASSIGN2}
\]

\[
\{x = 0\} \ x := 5 \ \{x = 0\}
\]
Hoare Logic: Assignment

Here’s the correct rule again:

$$\vdash \{P[a/x]\} x := a \{P\} \quad \text{Assign}$$

$$\{5 = 5\} x := 5 \{x = 5\}$$
Hoare Logic: Sequence

\[ \vdash \{P\} \ c_1 \ \{R\} \quad \vdash \{R\} \ c_2 \ \{Q\} \]

\[ \vdash \{P\} \ c_1; \ c_2 \ \{Q\} \quad \text{SEQ} \]
Hoare Logic: Conditionals

\[ \vdash \{ P \land b \} \ c_1 \ \{ Q \} \quad \vdash \{ P \land \neg b \} \ c_2 \ \{ Q \} \]

\[ \vdash \{ P \} \ \text{if} \ b \ \text{then} \ c_1 \ \text{else} \ c_2 \ \{ Q \} \]
Hoare Logic: Loops

\[
\vdash \{P \land b\} \ c \ {P} \\
\vdash \{P\} \ \textbf{while} \ b \ \textbf{do} \ c \ \{P \land \neg b\} \quad \textbf{WHILE}
\]

\(P\) works as a loop invariant.
Hoare Logic: Consequence

Recall: $\vdash P \Rightarrow P'$ denotes assertion validity.

It’s always free to strengthen pre-conditions and weaken post-conditions.

$$\vdash \{x = 4\} \text{skip} \{x = 4\}$$
\[
\begin{align*}
\vdash \{P\} \textbf{skip} \{P\} \quad \text{SKIP} \\
\vdash \{P[a/x]\} x := a \{P\} \\
\vdash \{P\} c_1 \{R\} & \quad \vdash \{R\} c_2 \{Q\} \\
\quad \vdash \{P\} c_1 ; c_2 \{Q\} \quad \text{SEQ} \\
\vdash \{P \land b\} c_1 \{Q\} & \quad \vdash \{P \land \neg b\} c_2 \{Q\} \\
\quad \vdash \{P\} \textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2 \{Q\} \quad \text{IF} \\
\vdash \{P \land b\} c \{P\} \\
\quad \vdash \{P\} \textbf{while } b \textbf{ do } c \{P \land \neg b\} \quad \text{WHILE} \\
\models P \Rightarrow P' & \quad \vdash \{P'\} c \{Q'\} \quad \models Q' \Rightarrow Q \quad \text{CONSEQUENCE}
\end{align*}
\]
Example: Factorial

\[
\{ x = n \land n > 0 \}
\]

\[
y := 1;
\]

\[
\textbf{while } x > 0 \textbf{ do}
\]

\[
(y := y \ast x;
\]

\[
x := x - 1)
\]

\[
\{ y = n! \}
\]

Extension!
Soundness and Completeness

Soundness: If we can prove it, then it’s actually true.

Completeness: If it’s true, then a proof exists.
Soundness and Completeness

Definition (Soundness)

If $\vdash \{P\} c \{Q\}$ then $\models \{P\} c \{Q\}$.

Definition (Completeness)

If $\models \{P\} c \{Q\}$ then $\vdash \{P\} c \{Q\}$.

Today: Soundness

Next time: Relative completeness
Soundness and Completeness

Theorem (Soundness)

If \( \vdash \{ P \} \triangleright \{ Q \} \) then \( \models \{ P \} \triangleright \{ Q \} \).
Soundness and Completeness

**Theorem (Soundness)**

If $\vdash \{P\} \triangleright \{Q\}$ then $\models \{P\} \triangleright \{Q\}$.

**Proof.**

By induction on derivation of $\vdash \{P\} \triangleright \{Q\}$...
Soundness and Completeness

Definition (Completeness)

If $\models \{P\} c \{Q\}$ then $\vdash \{P\} c \{Q\}$. 
Soundness and Completeness

**Definition (Completeness)**

If $\models \{P\} c \{Q\}$ then $\vdash \{P\} c \{Q\}$.

**CONSEQUENCE spoils completeness:**

\[
\begin{align*}
\models P \Rightarrow P' & \quad \vdash \{P'\} c \{Q'\} & \models Q' \Rightarrow Q \\
\vdash \{P\} c \{Q\} & \quad \vdash \{P\} c \{Q\}
\end{align*}
\]
Soundness and Completeness

Definition (Completeness)

If $\models \{P\} c \{Q\}$ then $\vdash \{P\} c \{Q\}$.

CONSEQUENCE spoils completeness:

\[
\begin{align*}
\models P \Rightarrow P' & \quad \vdash \{P'\} c \{Q'\} \quad \models Q' \Rightarrow Q \\
\vdash \{P\} c \{Q\} &
\end{align*}
\]

Definition (Relative completeness)

Hoare logic is *no more incomplete* than those implications.