Lecture 10
Hoare Logic
Overview

Last time

- Assertion language: $P$
- Assertion satisfaction: $\sigma \models_I P$
- Assertion validity: $\models P$

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

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

\[ \vdash \{P\} \text{skip} \{P\} \]
Hoare Logic: Assignment (this one’s weird)

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

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

**Assign**

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

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

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

\[ \{ \} \ x := 5 \ \{ x = 5 \} \]
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 \( P \)

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

\[
\begin{align*}
\vdash & \{P\} x := a \{P[a/x]\} \\
\{x = 0\} x := 5 & \{\quad\}
\end{align*}
\]

\text{BROKENASSIGN}
The rule for assignment is definitely *not*:

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

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

The rule for assignment is definitely not:

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

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

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

The rule for assignment is definitely \textit{not}:

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

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

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

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

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

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

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

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

Here’s the \textit{correct} rule again:

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

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

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

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

\[ \vdash \{ P \} \ \text{if} \ b \ \text{then} \ c_1 \ \text{else} \ c_2 \ \{ Q \} \]
$\vdash \{P \land b\} \ c \ \{P\}$

$\vdash \{P\} \ \textbf{while} \ b \ \textbf{do} \ c \ \{P \land \neg b\}$

$P$ works as a loop invariant.
Hoare Logic: Consequence

\[ \vdash P \Rightarrow P' \quad \vdash \{P'\} \circ \{Q'\} \quad \vdash Q' \Rightarrow Q \]

CONSEQUENCE

Recall: \( \vdash P \Rightarrow P' \) denotes assertion validity.

It’s always free to strengthen pre-conditions and weaken post-conditions.
\[\begin{align*}
\Gamma \vdash \{P\} \text{skip} \{P\} & \quad \text{SKIP} \\
\Gamma \vdash \{P[a/x]\} x := a \{P\} & \quad \text{ASSIGN} \\
\Gamma \vdash \{P\} c_1 \{R\} & \quad \Gamma \vdash \{R\} c_2 \{Q\} \\
& \quad \Gamma \vdash \{P\} c_1; c_2 \{Q\} & \quad \text{SEQ} \\
\Gamma \vdash \{P \land b\} c_1 \{Q\} & \quad \Gamma \vdash \{P \land \neg b\} c_2 \{Q\} \\
& \quad \Gamma \vdash \{P\} \text{if } b \text{ then } c_1 \text{ else } c_2 \{Q\} & \quad \text{IF} \\
\Gamma \vdash \{P \land b\} c \{P\} & \quad \Gamma \vdash \{P\} \text{while } b \text{ do } c \{P \land \neg b\} & \quad \text{WHILE} \\
\models P \Rightarrow P' & \quad \Gamma \vdash \{P'\} c \{Q'\} & \quad \models Q' \Rightarrow Q \quad \text{CONSEQUENCE} \\
& \quad \Gamma \vdash \{P\} c \{Q\} 
\end{align*}\]
Example: Factorial

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

\[
y := 1;
\]

**while** \( x > 0 \) **do**

\[
(y := y \cdot x; \\
x := x - 1)
\]

\[ \{ y = n! \} \]
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 $\vdash \{P\} \sqsubseteq \{Q\}$ then $\models \{P\} \sqsubseteq \{Q\}$.

Definition (Completeness)

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

Today: Soundness

Next time: Relative completeness
Soundness and Completeness

Theorem (Soundness)

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

Theorem (Soundness)

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

Proof.

By induction on derivation of $\vdash \{P\} c \{Q\}$...
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:

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

Definition (Completeness)

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

CONSEQUENCE spoils completeness:

$$
\models P \Rightarrow P' \quad \vdash \{P'\} c \{Q'\} \quad \models Q' \Rightarrow Q
\quad \vdash \{P\} c \{Q\}
$$

Definition (Relative completeness)

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