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:

\[
\forall \sigma, I. \sigma \models_{I} \{ P \} c \{ Q \}.
\]
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

\[ \vdash \{ P \} \text{skip} \{ P \} \]

\text{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)

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

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

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

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

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

⊢ \{ P \} x := a \{ P \} \quad \text{Assign}

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

\{5 = 5\} x := 5 \{ x = 5 \}
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:

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

\textsc{BrokenAssign}

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

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

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

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

**BrokenAssign**

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

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

**BrokenAssign2**

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

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

$$\{x = 0\} \ x := 5 \ \{5 = 0\}$$

$$\vdash \{P\} \ x := a \ \{P[x/a]\}$$ \textbf{BrokenAssign2}

$$\{x = 0\} \ x := 5 \ \{x = 0\}$$
Here’s the *correct* rule again:

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

\[ \{ 5 = 5 \} \ x := 5 \ { x = 5 } \]
Hoare Logic: Sequence

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

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

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

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

\[ \vdash \{ P \land b \} \ c \ \{ P \} \quad \text{WHILE} \]

\[ \vdash \{ P \} \ \text{while} \ b \ \text{do} \ c \ \{ P \land \neg b \} \]

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

\[ \frac{\models P \Rightarrow P'}{\models \{P\} \text{c} \{Q\} \Rightarrow \{Q\} \text{c} \{Q\} \models Q' \Rightarrow Q} \]

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

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

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

\begin{align*}
y & := 1; \\
\textbf{while } x > 0 \textbf{ do } \\
& \quad (y := y \ast x; \\
& \quad \quad x := x - 1)
\end{align*}

\{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 $\vdash \{P\} \ c \ \{Q\}$ 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 $\vdash \{P\} \ c \ \{Q\}$ 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 $\vdash \{P\} c \{Q\}$.

Consequence spoils completeness:

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

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

Definition (Relative completeness)

Hoare logic is no more incomplete than those implications.
Definition (Completeness)

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

Consequence spoils completeness:

\[
\models P \Rightarrow P' \quad \vdash \{P'\} \ c\ \{Q'\} \quad \models Q' \Rightarrow Q
\]

\[
\vdash \{P\} \ c\ \{Q\}
\]
Soundness and Completeness

Definition (Completeness)
If $\models \{ P \} \ c \ \{ Q \}$ then $\vdash \{ P \} \ c \ \{ Q \}$.

Consequence spoils completeness:

\[
\vdash P \Rightarrow P' \quad \vdash \{ P' \} \ c \ \{ Q' \} \quad \models Q' \Rightarrow Q
\]

Definition (Relative completeness)
Hoare logic is \textit{no more incomplete} than those implications.