Announcements

- Homework #3 out! Happy OCamling.
Overview

Last time

- Assertion language: $P$
- Assertion satisfaction: $\sigma \models_i P$
- Assertion validity: $\models P$
- Partial/total correctness statements: $\{P\} \circ \{Q\}$ and $[P] \circ [Q]$
- Partial correctness satisfaction $\sigma \models_i \{P\} \circ \{Q\}$
- Partial correctness validity: $\models \{P\} \circ \{Q\}$

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 valid in 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 proof system in which every theorem is a valid partial correctness statement.

Judgements of the form $\vdash \{P\} c \{Q\}$ defined inductively using compositional and (mostly) syntax-directed axioms and inference rules.
Hoare Logic: Skip

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

\[ \vdash \{ P[a/x] \} \ x := a \ \{ P \} \]
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 \( P \).
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 $P$

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

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

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

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

The rule for assignment is definitely not:

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

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

\[
\quad \vdash \{P\} \ x := a \ \{P[x/a]\} \quad \text{BROKENASSIGN2}
\]
Hoare Logic: Broken Assignment

The rule for assignment is definitely not:

\[
\begin{align*}
\vdash \{ P \} x := a \{ P[a/x] \} & \quad \text{BrokenAssign} \\
\{ x = 0 \} x := 5 \{ 5 = 0 \} & \\
\vdash \{ P \} x := a \{ P[x/a] \} & \quad \text{BrokenAssign2} \\
\{ x = 0 \} x := 5 \{ \} &
\end{align*}
\]
The rule for assignment is definitely not:

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

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

\[
\frac{}{\vdash \{P\} \ x := a \ {P[x/a]\}} \quad \text{BrokenAssign2}
\]

\[
\{x = 0\} \ x := 5 \ {x = 0}\]
Here’s the correct rule again:

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

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

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

\[ \vdash \{P\} c_1; c_2 \{Q\} \]  

\text{SEQ}
Hoare Logic: Conditionals

\[
\begin{align*}
\vdash & \{ P \land b \} \quad c_1 \quad \{ Q \} & \vdash & \{ P \land \neg b \} \quad c_2 \quad \{ Q \} \\
\hline
\vdash & \{ P \} \quad \textbf{if} \ b \ \textbf{then} \ c_1 \ \textbf{else} \ c_2 \ \{ Q \} \quad \text{IF}
\end{align*}
\]
Hoare Logic: Loops

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

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

\( P \) works as a loop invariant.
Recall: \( \models P \Rightarrow P' \) denotes assertion validity.

It’s always free to strengthen pre-conditions and weaken post-conditions.
\[ \vdash \{ P \} \text{skip} \{ P \} \quad \text{SKIP} \]

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

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

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

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

\[ \vdash P \Rightarrow P' \quad \vdash \{ P' \} \ c \ \{ Q' \} \quad \vdash Q' \Rightarrow Q \quad \text{CONSEQUENCE} \]
Example: Factorial

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

\[
y := 1;
\]

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

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

\[
x := x - 1
\]

\[
\{ y = n! \}
\]
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 \( \vdash P \)  then \( \models P \).

Proof.
By induction on derivation of \( \vdash P \).
Soundness and Completeness

Theorem (Soundness)

If \( \not\vdash \{P\} c \{Q\} \) then \( \not\models \{P\} c \{Q\} \).

Proof.

By induction on derivation of \( \vdash \{P\} c \{Q\} \).
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:**

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

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

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

Consequence spoils completeness:

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

Definition (Relative completeness)
Hoare logic is *no more incomplete* than those implications.