CS 4110

Programming Languages & Logics

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

Review

Definition (Partial correctness satisfaction)

A partial correctness statement $\{P\}\ c\ \{Q\}$ is satisfied by store σ and interpretation I, written $\sigma \vDash_I \{P\}\ c\ \{Q\}$, if:

$$\forall \sigma'.\ \text{if } \sigma \vDash_I P \text{ and } \mathcal{C}[\![c]\!]\ \sigma = \sigma' \text{ then } \sigma' \vDash_I Q$$

Definition (Partial correctness validity)

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

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.

$(P, c, Q) \in$ "$\vdash$"

Hoare Logic: Skip

$$\frac{}{\vdash \{P\}\ \textbf{skip}\ \{P\}}\ \textsc{Skip}$$

$\vdash \{x = y * i\}$ skip $\{x = y * i\}$

Hoare Logic: Assignment (this one's weird)

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

↑

"FIND AND REPLACE"
x WITH a

$\vdash \{2+ = y\}\ x := 2+1\ \{x = y\}$

Hoare Logic: Assignment (this one's weird)

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

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

Hoare Logic: Assignment (this one's weird)

$$\overline{\vdash \{P[a/x]\}\ x := a\ \{P\}}\ \textsc{Assign}$$

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

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

Hoare Logic: Assignment (this one's weird)

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

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:*

$$\frac{}{\vdash \{P\}\; x := a\; \{P[a/x]\}}\ \textsc{BrokenAssign}$$

Hoare Logic: Broken Assignment

The rule for assignment is definitely *not:*

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

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

Hoare Logic: Broken Assignment

The rule for assignment is definitely *not:*

$$\frac{}{\vdash \{P\}\, x := a\, \{P[a/x]\}}\ \textsc{BrokenAssign}$$

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

Hoare Logic: Broken Assignment

The rule for assignment is definitely *not:*

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

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

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

Hoare Logic: Broken Assignment

The rule for assignment is definitely *not:*

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

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

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

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

Hoare Logic: Broken Assignment

The rule for assignment is definitely *not:*

$$\frac{}{\vdash \{P\}\; x := a\; \{P[a/x]\}}\ \textsc{BrokenAssign}$$

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

$$\frac{}{\vdash \{P\}\; x := a\; \{P[x/a]\}}\ \textsc{BrokenAssign2}$$

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

Hoare Logic: Assignment

Here's the *correct* rule again:

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

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

Hoare Logic: Sequence

$$\frac{\vdash \{P\}\, c_1\, \{R\} \qquad \vdash \{R\}\, c_2\, \{Q\}}{\vdash \{P\}\, c_1; c_2\, \{Q\}}\ \textsc{Seq}$$

Hoare Logic: Conditionals

$$\frac{\vdash \{P \wedge b\}\ c_1\ \{Q\} \qquad \vdash \{P \wedge \neg b\}\ c_2\ \{Q\}}{\vdash \{P\}\ \textbf{if}\ b\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{Q\}}\ \textsc{If}$$

Hoare Logic: Loops

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

P works as a loop invariant.

Hoare Logic: Consequence

$$\frac{\models P \Rightarrow P' \qquad \vdash \{P'\}\ c\ \{Q'\} \qquad \models Q' \Rightarrow Q}{\vdash \{P\}\ c\ \{Q\}}\ \textsc{Consequence}$$

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

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

$$\frac{}{\vdash \{P\}\ \textbf{skip}\ \{P\}}\ \textsc{Skip}$$

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

$$\frac{\vdash \{P\}\ c_1\ \{R\} \qquad \vdash \{R\}\ c_2\ \{Q\}}{\vdash \{P\}\ c_1; c_2\ \{Q\}}\ \textsc{Seq}$$

$$\frac{\vdash \{P \wedge b\}\ c_1\ \{Q\} \qquad \vdash \{P \wedge \neg b\}\ c_2\ \{Q\}}{\vdash \{P\}\ \textbf{if}\ b\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{Q\}}\ \textsc{If}$$

$$\frac{\vdash \{P \wedge b\}\ c\ \{P\}}{\vdash \{P\}\ \textbf{while}\ b\ \textbf{do}\ c\ \{P \wedge \neg b\}}\ \textsc{While}$$

$$\frac{\models P \Rightarrow P' \qquad \vdash \{P'\}\ c\ \{Q'\} \qquad \models Q' \Rightarrow Q}{\vdash \{P\}\ c\ \{Q\}}\ \textsc{Consequence}$$

Example: Factorial

$\{x = n \wedge n > 0\}$

$$
\begin{array}{l}
y := 1; \\
\textbf{while } x > 0 \textbf{ do} \\
\qquad (y := y * x; \\
\qquad\ \ x := x - 1)
\end{array}
$$

$\{y = n!\}$

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

Soundness and Completeness

Definition (Completeness)

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

CONSEQUENCE spoils completeness:

$$\frac{\models P \Rightarrow P' \qquad \vdash \{P'\}\, c\, \{Q'\} \qquad \models Q' \Rightarrow Q}{\vdash \{P\}\, c\, \{Q\}}$$

Soundness and Completeness

Definition (Completeness)

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

CONSEQUENCE spoils completeness:

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

Definition (Relative completeness)

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