CS 4110

Programming Languages & Logics



Overview

Last time

- Assertion language: P
- Assertion satisfaction: $\sigma \models_{l} P$
- Assertion validity: ⊨ P
- Partial/total correctness statements: {P} c {Q} and [P] c [Q]
- Partial correctness satisfaction $\sigma \models_{l} \{P\} \ c \{Q\}$
- 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 $\sigma \models_I \{P\}$ c $\{Q\}$, if:

$$\forall \sigma'$$
. if $\sigma \vDash_{l} P$ and $\mathcal{C}\llbracket c \rrbracket \sigma = \sigma'$ then $\sigma' \vDash_{l} Q$

Definition (Partial correctness validity)

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

3

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



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

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

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

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

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

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

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

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

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

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

$$\overline{ \vdash \{P\}\, x := a\; \{P[a/x]\}}$$
 BrokenAssign $\{x=0\}\, x := 5\; \{\qquad\}$

$$\overline{ \vdash \{P\}\, x := a\; \{P[a/x]\}}$$
 BrokenAssign $\{x=0\}\, x := 5\; \{5=0\}$

$$\overline{ \left\{ P
ight\} x := a \left\{ P[a/x]
ight\} }$$
 BrokenAssign $\left\{ x = 0
ight\} x := 5 \left\{ 5 = 0
ight\}$

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

$$\overline{ \left\{ P \right\} x := a \left\{ P[a/x] \right\} }$$
 BrokenAssign $\left\{ x = 0 \right\} x := 5 \left\{ 5 = 0 \right\}$

$$\frac{}{\vdash \{P\} \, x := a \, \{P[x/a]\}} \, \mathsf{BROKENASSIGN2}$$

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

$$\overline{ \left\{ P \right\} x := a \left\{ P[a/x] \right\} }$$
 BrokenAssign $\left\{ x = 0 \right\} x := 5 \left\{ 5 = 0 \right\}$

$$\frac{}{\vdash \{P\} \, x := a \, \{P[x/a]\}} \, \mathsf{BROKENASSIGN2}$$

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

Hoare Logic: Assignment

Here's the *correct* rule again:

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

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

Hoare Logic: Sequence

$$\frac{\vdash \{P\}\,c_1\,\{R\} \qquad \vdash \{R\}\,c_2\,\{Q\}}{\vdash \{P\}\,c_1;c_2\,\{Q\}}\,\,\mathsf{SeQ}$$

Hoare Logic: Conditionals

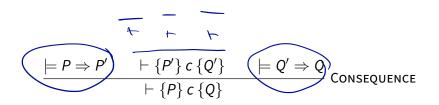
$$\frac{\vdash \{P \land b\} \, c_1 \, \{Q\} \qquad \vdash \{P \land \neg b\} \, c_2 \, \{Q\}}{\vdash \{P\} \, \text{if} \, b \, \, \text{then} \, c_1 \, \, \text{else} \, c_2 \, \{Q\}} \, \, \, \mathsf{IF}$$

Hoare Logic: Loops

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

P works as a loop invariant.

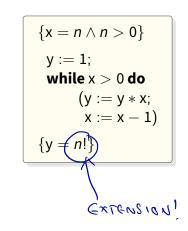
Hoare Logic: Consequence



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

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

Example: Factorial



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

Completeness: If it's true, then a proof exists.

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

Theorem (Soundness)

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

Theorem (Soundness)

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

Proof.

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

Definition (Completeness)

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

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 (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.