CS 4110

Programming Languages & Logics

Lecture 10
Hoare Logic

19 September 2012

Announcements

- Homework #3 out
- Foster office hours today 11am-12pm

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 valid in any store and interpretation: $\forall \sigma, I.\ \sigma \vDash_I \{P\}\ c\ \{Q\}$.

Question

Is it decidable whether $\{P\}\ c\ \{Q\}$?

1. Yes
2. No

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

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

Question

Which of the following is the correct axiom for assignment?

1. $$\overline{\vdash \{P\}\ x := a\ \{P \land x = a\}}$$

2. $$\overline{\vdash \{P \land x = a\}\ x := a\ \{P\}}$$

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

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

5. All of the above.

Hoare Logic: Assignment

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

Hoare Logic: Assignment

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

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

Hoare Logic: Sequence

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

Hoare Logic: Conditionals

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

Hoare Logic: Loops

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

Hoare Logic: Consequence

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

Note: $\models P \Rightarrow P'$ denotes assertion validity

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

Text

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

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

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

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

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

Example: Factorial

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

$$\mathsf{y} := 1;$$
$$\textbf{while } \mathsf{x} > 0 \textbf{ do}$$
$$(\mathsf{y} := \mathsf{y} * \mathsf{x};$$
$$\mathsf{x} := \mathsf{x} - 1)$$
$$\}$$

$$\{\mathsf{y} = n!\}$$

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

Wednesday: 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 $\{P\}\ c\ \{Q\}$... □

Soundness and Completeness

Theorem (Soundness)

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

Proof.

By induction on $\{P\}\, c\, \{Q\}$... $\square$

Lemma (Substitution)

- $\sigma \models_I P[a/x] \Leftrightarrow \sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma] \models_I P$
- $\mathcal{A}[\![a_0[a/x]]\!]\,(\sigma, I) \Leftrightarrow \mathcal{A}[\![a_0]\!]\,(\sigma[x \mapsto \mathcal{A}[\![a]\!]\,(\sigma, I)], I)$