CS 4110

Programming Languages & Logics

Lecture 11

Hoare Logic

17 September 2012

Announcements

- Homework #3 due today at 11:59pm
- Foster office hours today 4-5pm in Upson 4137
- Rajkumar office hours today 5-6pm in 4135
- Additional help available on Piazza
- Homework #4 out today

Overview

Friday

- 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
- Soundness and Completeness
- Examples

Review

Definition (Partial correctness statement 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 statement validity)

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

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

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

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: Assignment

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

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

Question: Why is the assignment on the left?

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

Example: Factorial

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

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

$\{y = n!\}$

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

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)

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