CS 4110

Programming Languages & Logics

Lecture 11
Weakest Preconditions

19 September 2012

Announcements

- Foster office hours today 11-12pm in Upson 4137
- Contact me if you'd like to participate in WitsOn!

Overview

Monday

- Hoare Logic
- Examples

Today

- “Decorated” programs
- Soundness
- Completeness
- Weakest Preconditions

Review: Hoare Logic

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

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

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

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

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

Example: "Decorated" Programs

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

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

$\{y = n!\}$

Example: "Decorated" Programs

$\{x = n \wedge n > 0\} \Rightarrow$
$\{1 = 1 \wedge x = n \wedge n > 0\}$
$y := 1;$
$\{y = 1 \wedge x = n \wedge n > 0\} \Rightarrow$
$\{y * x! = n! \wedge x \geq 0\}$
while $x > 0$ **do** $\{$
    $\{y * x! = n! \wedge x > 0 \wedge x \geq 0\} \Rightarrow$
    $\{y * x * (x - 1)! = n! \wedge (x - 1) \geq 0\}$
    $y := y * x;$
    $\{y * (x - 1)! = n! \wedge (x - 1) \geq 0\}$
    $x := x - 1$
    $\{y * x! = n! \wedge x \geq 0\}$
$\}$
$\{y * x! = n! \wedge (x \geq 0) \wedge \neg(x > 0)\} \Rightarrow$
$\{y = n!\}$

Soundness and Completeness

Definition (Soundness)

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

Definition (Completeness)

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

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 $\{P\}\, c\, \{Q\}$... □

Lemma (Substitution)

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

Decidability

Suppose we had an algorithm for deciding the validity of partial correctness statements...

Then we could decide

$$\{\textbf{true}\}\ \textbf{skip}\ \{P\}$$

Decidability

Suppose we had an algorithm for deciding the validity of partial correctness statements...

Then we could decide

$$\{\textbf{true}\}\ \textbf{skip}\ \{P\}$$

and

$$\{\textbf{true}\}\ c\ \{\textbf{false}\}$$

Decidability

Suppose we had an algorithm for deciding the validity of partial correctness statements...

Then we could decide

$$\{\mathbf{true}\}\ \mathbf{skip}\ \{P\}$$

and

$$\{\mathbf{true}\}\ c\ \{\mathbf{false}\}$$

The first is valid if and only if the assertion P is valid

The second is valid if and only if the command c halts.

Completeness

But although we cannot decide validity, Hoare logic does enjoy the completeness property stated in the following theorem:

Theorem (Cook (1974))

$\forall P, Q \in \mathbf{Assn}, c \in \mathbf{Com}.\ \vDash \{P\}\, c\, \{Q\}$ *implies* $\vdash \{P\}\, c\, \{Q\}$.

Completeness

But although we cannot decide validity, Hoare logic does enjoy the completeness property stated in the following theorem:

Theorem (Cook (1974))

$\forall P, Q \in \textbf{Assn}, c \in \textbf{Com}.\ \vDash \{P\}\, c\, \{Q\}$ *implies* $\vdash \{P\}\, c\, \{Q\}$.

It turns out that the key culprit that breaks decidability is the Consequence rule.

It includes two premises involving the validity of implications between arbitrary assertions.

But if we had an oracle that could decide the validity of assertions, then we could decide the validity of partial correctness specifications.

Weakest Preconditions

Cook's proof is based on weakest preconditions

Intuition: the weakest liberal precondition for c and Q is the weakest assertion P such that $\{P\}\ c\ \{Q\}$ is valid

More formally...

Definition (Weakest Liberal Precondition)

P is a weakest liberal precondition of c and Q written $wlp(c, Q)$ if:

$$\forall \sigma, l.\ \sigma \vDash_l P \iff (\mathcal{C}[\![c]\!]\ \sigma) \text{ undefined } \vee\ (\mathcal{C}[\![c]\!]\sigma) \vDash_l Q$$

Weakest Preconditions

$$wlp(\textbf{skip}, P) \quad = \quad P$$

Weakest Preconditions

$$
\begin{aligned}
wlp(\textbf{skip}, P) &= P \\
wlp((\mathrm{x} := a, P) &= P[a/\mathrm{x}]
\end{aligned}
$$

Weakest Preconditions

$$
\begin{array}{rcl}
wlp(\textbf{skip}, P) & = & P \\
wlp((\mathrm{x} := a, P) & = & P[a/\mathrm{x}] \\
wlp((c_1; c_2), P) & = & wlp(c_1, wlp(c_2, P))
\end{array}
$$

Weakest Preconditions

$$
\begin{aligned}
wlp(\textbf{skip}, P) &= P \\
wlp((\mathrm{x} := a, P) &= P[a/\mathrm{x}] \\
wlp((c_1; c_2), P) &= wlp(c_1, wlp(c_2, P)) \\
wlp(\textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2, P) &= (b \implies wlp(c_1, P)) \wedge \\
&\quad (\neg b \implies wlp(c_2, P))
\end{aligned}
$$

Weakest Preconditions

$$
\begin{aligned}
wlp(\textbf{skip}, P) &= P \\
wlp((\mathrm{x} := a, P) &= P[a/\mathrm{x}] \\
wlp((c_1; c_2), P) &= wlp(c_1, wlp(c_2, P)) \\
wlp(\textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2, P) &= (b \implies wlp(c_1, P)) \wedge \\
&\quad (\neg b \implies wlp(c_2, P)) \\
wlp(\textbf{while } b \textbf{ do } c, P) &= \bigwedge_i F_i(P)
\end{aligned}
$$

Weakest Preconditions

$$
\begin{array}{rcl}
wlp(\textbf{skip}, P) & = & P \\
wlp((\mathrm{x} := a, P) & = & P[a/\mathrm{x}] \\
wlp((c_1; c_2), P) & = & wlp(c_1, wlp(c_2, P)) \\
wlp(\textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2, P) & = & (b \implies wlp(c_1, P)) \wedge \\
 & & (\neg b \implies wlp(c_2, P)) \\
wlp(\textbf{while } b \textbf{ do } c, P) & = & \bigwedge_i F_i(P)
\end{array}
$$

where

$$
\begin{array}{rcl}
F_0(P) & = & \textbf{true} \\
F_{i+1}(P) & = & (\neg b \implies P) \wedge (b \implies wlp(c, F_i(P)))
\end{array}
$$

Properties of Weakest Precondition

Lemma (Correctness of Weakest Preconditions)

$$\forall c \in \textbf{Com}, Q \in \textbf{Assn}.$$
$$\models \{wlp(c, Q)\}\, c\, \{Q\} \textit{ and}$$
$$\forall R \in \textbf{Assn}.\ \models \{R\}\, c\, \{Q\} \textit{ implies } (R \implies wlp(c, Q))$$

Properties of Weakest Precondition

Lemma (Correctness of Weakest Preconditions)

$$\forall c \in \textbf{Com}, Q \in \textbf{Assn}.$$
$$\models \{wlp(c, Q)\}\, c\, \{Q\} \textit{ and}$$
$$\forall R \in \textbf{Assn}.\ \models \{R\}\, c\, \{Q\} \textit{ implies } (R \implies wlp(c, Q))$$

Lemma (Provability of Weakest Preconditions)

$$\forall c \in \textbf{Com}, Q \in \textbf{Assn}.\ \vdash \{wlp(c, Q)\}\, c\, \{Q\}$$

Relative Completeness

Theorem (Cook (1974))

$\forall P, Q \in \mathbf{Assn}, c \in \mathbf{Com}.\ \vDash \{P\}\, c\, \{Q\}$ *implies* $\vdash \{P\}\, c\, \{Q\}$.

Proof Sketch.

Let $\{P\}\, c\, \{Q\}$ be a valid partial correctness specification.

By the first Lemma we have $\vDash P \implies \mathit{wlp}(c, Q)$.

By the second Lemma we have $\vdash \{\mathit{wlp}(c, Q)\}\, c\, \{Q\}$.

We conclude $\vdash \{P\}\, c\, \{Q\}$ using Consequence rule. □