CS 4110

Programming Languages & Logics

Lecture 11
Hoare Logic Metatheory

24 September 2014

Announcements

- PS #3 due today
- PS #4 out today
- Foster Friday office hours canceled
- Friday 9/26: Guest lecture by Michael Clarkson
- Wednesday 10/1: CS 50 and Gates Dedication! No lecture
- Monday 10/6: Preliminary Exam I

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

Soundness and Completeness

Theorem (Soundness)

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

Proof.

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

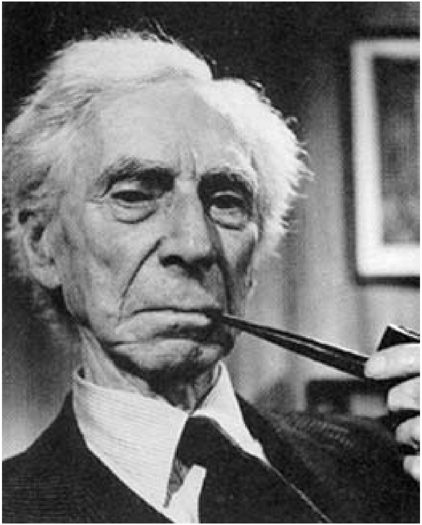
Lemma (Substitution)

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

Who is this?

A. Otto von Bismarck
B. David Hilbert
C. Gottlob Frege
D. LEJ Brouwer
E. Georg Cantor

Who is this?



A. Ludwig Wittgenstein

B. Virginia Woolf

C. EM Forster

D. Bertrand Russell

E. Giuseppe Peano

Who is this?

A. Haskell Curry

B. Alan Turing

C. Alonzo Church

D. David Gries

E. Kurt Gödel

Completeness

Hoare logic enjoys the completeness property stated in the following theorem:

Theorem (Cook (1974))

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

Completeness

Hoare logic enjoys the completeness property stated in the following theorem:

Theorem (Cook (1974))

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

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:

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

Weakest Preconditions

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

Weakest Preconditions

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

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

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

Weakest Preconditions

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

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)

$$
\begin{aligned}
&\forall c \in \textbf{Com}, Q \in \textbf{Assn}. \\
&\qquad \vDash \{\mathit{wlp}(c, Q)\}\, c\, \{Q\} \ \ \mathit{and} \\
&\qquad \forall R \in \textbf{Assn}.\ \vDash \{R\}\, c\, \{Q\}\ \mathit{implies}\, (R \implies \mathit{wlp}(c, Q))
\end{aligned}
$$

Properties of Weakest Precondition

Lemma (Correctness of Weakest Preconditions)

$$\begin{aligned} &\forall c \in \mathbf{Com}, Q \in \mathbf{Assn}. \\ &\qquad \vDash \{wlp(c, Q)\}\ c\ \{Q\}\ \textit{and} \\ &\qquad \forall R \in \mathbf{Assn}.\ \vDash \{R\}\ c\ \{Q\}\ \textit{implies}\ (R \implies wlp(c, Q)) \end{aligned}$$

Lemma (Provability of Weakest Preconditions)

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

Relative Completeness

Theorem (Cook (1974))

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

Proof Sketch.

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

By the first Lemma we have $\models P \implies wlp(c, Q)$.

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

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