Semantics and Verification of Software

Lecture 11: Axiomatic Semantics of WHILE III (Completeness and Equivalence)

Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)

RWTH Aachen University

noll@cs.rwth-aachen.de

http://www-i2.informatik.rwth-aachen.de/i2/svsw08/

Winter semester 2008/09

Outline

1. Repetition: Correctness of Hoare Logic
2. (In-)Completeness of Hoare Logic
3. Equivalence of Axiomatic and Operational/Denotational Semantics

Partial Correctness Properties

Definition (Partial correctness properties)

Let $A, B \in Assn$ and $c \in Cmd$.

- An expression of the form $\{A\}\,c\,\{B\}$ is called a partial correctness property with precondition A and postcondition B.
- Given $\sigma \in \Sigma_\perp$ and $I \in Int$, we let

$$\sigma \models^I \{A\}\,c\,\{B\}$$

  if $\sigma \models^I A$ implies $\mathfrak{C}[\![c]\!]\sigma \models^I B$
  (or equivalently: $\sigma \in A^I \implies \mathfrak{C}[\![c]\!]\sigma \in B^I$).
- $\{A\}\,c\,\{B\}$ is called valid in I (notation: $\models^I \{A\}\,c\,\{B\}$) if $\sigma \models^I \{A\}\,c\,\{B\}$ for every $\sigma \in \Sigma_\perp$ (or equivalently: $\mathfrak{C}[\![c]\!]A^I \subseteq B^I$).
- $\{A\}\,c\,\{B\}$ is called valid (notation: $\models \{A\}\,c\,\{B\}$) if $\models^I \{A\}\,c\,\{B\}$ for every $I \in Int$.

Hoare Logic

Goal: syntactic derivation of valid partial correctness properties

Definition (Hoare Logic)

The Hoare rules are given by

$$(\text{skip})\ \frac{}{\{A\}\,\texttt{skip}\,\{A\}} \qquad (\text{asgn})\ \frac{}{\{A[x \mapsto a]\}\,x\,\texttt{:=}a\,\{A\}}$$

$$(\text{seq})\ \frac{\{A\}\,c_1\,\{C\}\ \ \{C\}\,c_2\,\{B\}}{\{A\}\,c_1\,\texttt{;}c_2\,\{B\}} \qquad (\text{if})\ \frac{\{A \land b\}\,c_1\,\{B\}\ \ \{A \land \neg b\}\,c_2\,\{B\}}{\{A\}\,\texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\,\{B\}}$$

$$(\text{while})\ \frac{\{A \land b\}\,c\,\{A\}}{\{A\}\,\texttt{while}\ b\ \texttt{do}\ c\,\{A \land \neg b\}}$$

$$(\text{cons})\ \frac{\models (A \implies A')\ \ \{A'\}\,c\,\{B'\}\ \ \models (B' \implies B)}{\{A\}\,c\,\{B\}}$$

A partial correctness property is provable (notation: $\vdash \{A\}\,c\,\{B\}$) if it is derivable by the Hoare rules. In case of (while), A is called a (loop) invariant.

Here $A[x \mapsto a]$ denotes the syntactic replacement of every occurrence of x by a in A.

Soundness of Hoare Logic

Theorem (Soundness of Hoare Logic)

For every partial correctness property $\{A\}\, c\, \{B\}$,

$$\vdash \{A\}\, c\, \{B\} \implies \models \{A\}\, c\, \{B\}.$$

Proof.

Let $\vdash \{A\}\, c\, \{B\}$. By induction over the structure of the corresponding proof tree we show that, for every $\sigma \in \Sigma$ and $I \in Int$ such that $\sigma \models^I A$, $\mathfrak{C}[\![c]\!]\sigma \models^I B$ (on the board).
(If $\sigma = \bot$, then $\mathfrak{C}[\![c]\!]\sigma = \bot \models^I B$ holds trivially.) □

Outline

Incompleteness of Hoare Logic I

Soundness: only valid partial correctness properties are provable $\surd$

Completeness: all valid partial correctness properties are systematically derivable $\lightning$

Theorem 11.1 (Gödel's Incompleteness Theorem)

The set of all valid assertions

$$\{A \in Assn \mid \models A\}$$

is not recursively enumerable, i.e., there exists no proof system for Assn in which all valid assertions are systematically derivable.

Proof.

see [Winskel 1996, p. 110 ff] □

Incompleteness of Hoare Logic II

Corollary 11.2

There is no proof system in which all valid partial correctness properties can be enumerated.

Proof.

Given $A \in Assn$, $\models A$ is obviously equivalent to $\{\mathsf{true}\}\,\texttt{skip}\,\{A\}$. Thus the enumerability of all valid partial correctness properties would imply the enumerability of all valid assertions. □

Remark: alternative proof (using computability theory):
$\{\mathsf{true}\}\,c\,\{\mathsf{false}\}$ is valid iff c does not terminate on any input state. But the set of all non-terminating WHILE statements is not enumerable.

Relative Completeness of Hoare Logic I

- We will see: actual reason of incompleteness is rule

$$(\text{cons})\ \frac{\models (A \implies A')\ \{A'\}\, c\, \{B'\}\ \models (B' \implies B)}{\{A\}\, c\, \{B\}}$$

  since it is based on the validity of implications within $Assn$
- The other language constructs are "enumerable"
- Therefore: separation of proof system (Hoare Logic) and assertion language ($Assn$)
- One can show: if an "oracle" is available which decides whether a given assertion is valid, then all valid partial correctness properties can be systematically derived

$\implies$ Relative completeness

Relative Completeness of Hoare Logic I

Theorem 11.3 (Cook's Completeness Theorem)

Hoare Logic is relatively complete, i.e., for every partial correctness property $\{A\}\,c\,\{B\}$*:*

$$\models \{A\}\,c\,\{B\} \implies \vdash \{A\}\,c\,\{B\}.$$

Thus: if we know that a partial correctness property is valid, then we know that there is a corresponding derivation.

The proof uses the following concept: assume that, e.g., $\{A\}\,c_1\,;c_2\,\{B\}$ has to be derived. This requires an intermediate assertion $C \in Assn$ such that $\{A\}\,c_1\,\{C\}$ and $\{C\}\,c_2\,\{B\}$. How to find it?

Weakest Preconditions I

Definition 11.4 (Weakest precondition)

Given $c \in Cmd$, $B \in Assn$ and $I \in Int$, the weakest precondition of B with respect to c under I is defined by:

$$wp^I[\![c, B]\!] := \{\sigma \in \Sigma_\perp \mid \mathfrak{C}[\![c]\!]\sigma \models^I B\}.$$

Corollary 11.5

For every $c \in Cmd$, $A, B \in Assn$, and $I \in Int$:

1. $\models^I \{A\}\, c\, \{B\} \iff A^I \subseteq wp^I[\![c, B]\!]$
2. *If $A_0 \in Assn$ such that $A_0^I = wp^I[\![c, B]\!]$ for every $I \in Int$, then*
$$\models \{A\}\, c\, \{B\} \iff \models (A \implies A_0)$$

Remark: (2) justifies the notion of weakest precondition: it is implied by every precondition A which makes $\{A\}\, c\, \{B\}$ valid

Weakest Preconditions II

Definition 11.6 (Expressivity of assertion languages)

An assertion language $Assn$ is called expressive if, for every $c \in Cmd$ and $B \in Assn$, there exists $A_{c,B} \in Assn$ such that

$$A^I_{c,B} = wp^I[\![c, B]\!]$$

for every $I \in Int$.

Theorem 11.7 (Expressivity of $Assn$)

$Assn$ is expressive.

Proof.

(idea; see [Winskel 1996, p. 103 ff for details])
Given $c \in Cmd$ and $B \in Assn$, construct $A_{c,B} \in Assn$ with
$\sigma \models^I A_{c,B} \iff \mathfrak{C}[\![c]\!]\sigma \models^I B$ (for every $\sigma \in \Sigma_\perp$, $I \in Int$). For example:

$$A_{\texttt{skip},B} := B \qquad A_{x\texttt{:=}a,B} := B[x \mapsto a]$$
$$A_{c_1\texttt{;}c_2,B} := A_{c_1,A_{c_2,B}} \qquad \ldots$$

(for `while`: "Gödelization" of sequences of intermediate states) □

Relative Completeness of Hoare Logic II

The following lemma shows that weakest preconditions are "derivable":

Lemma 11.8

For every $c \in Cmd$ and $B \in Assn$:

$$\vdash \{A_{c,B}\}\, c\, \{B\}$$

Proof.

by structural induction over c (omitted) □

Proof (Cook's Completeness Theorem 11.3).

We have to show that Hoare Logic is relatively complete, i.e., that

$$\models \{A\}\, c\, \{B\} \implies \vdash \{A\}\, c\, \{B\}.$$

- Lemma 11.8 $\implies \vdash \{A_{c,B}\}\, c\, \{B\}$
- Cor. 11.5 $\implies \models (A \implies A_{c,B})$
- (cons) rule $\implies \vdash \{A\}\, c\, \{B\}$

□

Outline

1. Repetition: Correctness of Hoare Logic
2. (In-)Completeness of Hoare Logic
3. Equivalence of Axiomatic and Operational/Denotational Semantics

Operational/Denotational Equivalence

Def. 4.1: $\mathfrak{O}[\![.]\!] : Cmd \to (\Sigma \dashrightarrow \Sigma)$ given by

$$\mathfrak{O}[\![c]\!](\sigma) = \sigma' \iff \langle c, \sigma \rangle \to \sigma'$$

Def. 4.2: Two statements $c_1, c_2 \in Cmd$ are called operationally equivalent (notation: $c_1 \sim c_2$) if

$$\mathfrak{O}[\![c_1]\!] = \mathfrak{O}[\![c_2]\!].$$

Theorem 8.1: For every $c \in Cmd$,

$$\mathfrak{O}[\![c]\!] = \mathfrak{C}[\![c]\!],$$

i.e., $\mathfrak{O}[\![.]\!] = \mathfrak{C}[\![.]\!]$.

Axiomatic Equivalence I

In the axiomatic semantics, two statements have to be considered equivalent if they are indistinguishable w.r.t. partial correctness properties:

Definition 11.9 (Axiomatic equivalence)

Two statements $c_1, c_2 \in Cmd$ are called axiomatically equivalent (notation: $c_1 \approx c_2$) if, for all assertions $A, B \in Assn$,

$$\models \{A\}\, c_1\, \{B\} \iff \models \{A\}\, c_2\, \{B\}.$$

Example 11.10

We show that $c_1 ; (c_2 ; c_3) \approx (c_1 ; c_2) ; c_3$. Let $A, B \in Assn$:

$$\begin{array}{ll}
& \models \{A\}\, c_1 ; (c_2 ; c_3)\, \{B\} \\
\iff & \vdash \{A\}\, c_1 ; (c_2 ; c_3)\, \{B\} \text{ (Theorem 10.2, 11.3)} \\
\iff & \text{ex. } C_1 \in Assn \text{ such that } \vdash \{A\}\, c_1\, \{C_1\}, \vdash \{C_1\}\, c_2 ; c_3\, \{B\} \text{ (rule (seq))} \\
\iff & \text{ex. } C_1, C_2 \in Assn \text{ such that } \vdash \{A\}\, c_1\, \{C_1\}, \vdash \{C_1\}\, c_2\, \{C_2\}, \\
& \vdash \{C_2\}\, c_3\, \{B\} \text{ (rule (seq))} \\
\iff & \text{ex. } C_2 \in Assn \text{ such that } \vdash \{A\}\, c_1 ; c_2\, \{C_2\}, \vdash \{C_2\}\, c_3\, \{B\} \text{ (rule (seq))} \\
\iff & \vdash \{A\}\, (c_1 ; c_2) ; c_3\, \{B\} \text{ (rule (seq))} \\
\iff & \models \{A\}\, (c_1 ; c_2) ; c_3\, \{B\} \text{ (Theorem 10.2, 11.3)}
\end{array}$$

Axiomatic Equivalence II

Theorem 11.11

Axiomatic and denotational/operational equivalence coincide, i.e., for all $c_1, c_2 \in Cmd$,

$$c_1 \approx c_2 \iff c_1 \sim c_2.$$

Proof.

on the board □