Semantics and Verification of Software

Lecture 10: Axiomatic Semantics of WHILE

Thomas Noll

Lehrstuhl für Informatik 2
RWTH Aachen University
noll@cs.rwth-aachen.de

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

Summer semester 2007

Outline

1. Repetition: Hoare Logic
2. (In-)Completeness of Hoare Logic

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

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

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

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

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

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 II

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 $I \in \mathit{Int}$ 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 10.1 (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 10.2

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 $\{\mathsf{true}\}\,\mathtt{skip}\,\{A\}$. 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

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

  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 derived

$\Longrightarrow$ Relative completeness

Relative Completeness of Hoare Logic I

Theorem 10.3 (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 $\{A\}\,c_1\,;c_2\,\{B\}$ 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 10.4 (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 10.5

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 10.6 (Expressivity of assertion languages)

An assertion language $Assn$ is called expressive if, for every $c \in Cmd$ and $B \in Assn$, there exists $A_0 \in Assn$ such that
$$A_0^I = wp^I[\![c, B]\!]$$
for every $I \in Int$.

Theorem 10.7 (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 10.8

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 10.3).

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

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

- Lemma 10.8 $\implies \vdash \{A_{c,B}\}\, c\, \{B\}$
- Cor. 10.5 $\implies \models (A \implies A_{c,B})$
- (cons) rule $\implies \vdash \{A\}\, c\, \{B\}$

□