Semantics and Verification of Software

Lecture 10: Axiomatic Semantics of WHILE II (Soundness of Hoare Logic)

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

Tag der Informatik
am 5. Dezember 2008

tdi2008

Program:

10:30–12:00	PhD Kolloquium (AH 5)
13:00–16:15	Opening and Talks (AH 5)
16:45–17:45	Software Award (AH 5)
18:00–19:15	Graduation Ceremony (Aula 2)
from 19:30	Party Time (AH 5)

Outline

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 I

Goal: syntactic derivation of valid partial correctness properties

Definition (Hoare Logic)

The Hoare rules are given by

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

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

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

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

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.

Example

Proof of $\{A\}\,\texttt{y:=1;}c\,\{B\}$ where

$$c := (\texttt{while } \neg\texttt{(x=1) do (y:=y*x; x:=x-1)})$$
$$A := (\texttt{x} = i)$$
$$B := (\texttt{y} = i!)$$

(on the board)

Structure of the proof:

$$\dfrac{\dfrac{\dfrac{}{4}\,(\text{asgn})\,\dfrac{}{5}\;\dfrac{}{6}}{2}\,(\text{cons})\;\dfrac{\dfrac{}{7}\,(\text{while})\,\dfrac{\dfrac{\dfrac{}{11}\,(\text{seq})\,\dfrac{(\text{asgn})\,\dfrac{}{14}\;(\text{asgn})\,\dfrac{}{15}}{12}\;\dfrac{}{13}}{10}\,(\text{cons})}{8}\;\dfrac{}{9}}{3}}{1}\,(\text{seq})$$

Example (continued)

Here the single propositions are given by:

0. $C := (\mathtt{x} > 0 \implies \mathtt{y} * \mathtt{x}! = i! \wedge i \geq \mathtt{x})$
1. $\{A\}\,\mathtt{y := 1};c\,\{B\}$
2. $\{A\}\,\mathtt{y := 1}\,\{C\}$
3. $\{C\}\,c\,\{B\}$
4. $\models (A \implies C[\mathtt{y} \mapsto 1])$
5. $\{C[\mathtt{y} \mapsto 1]\}\,\mathtt{y := 1}\,\{C\}$
6. $\models (C \implies C)$
7. $\models (C \implies C)$
8. $\{C\}\,c\,\{\neg(\neg(\mathtt{x = 1})) \wedge C\}$
9. $\models (\neg(\neg(\mathtt{x = 1})) \wedge C \implies B)$
10. $\{\neg(\mathtt{x = 1}) \wedge C\}\,\mathtt{y := y*x;\ x := x-1}\,\{C\}$
11. $\models (\neg(\mathtt{x = 1}) \wedge C \implies C[\mathtt{x} \mapsto \mathtt{x-1}, \mathtt{y} \mapsto \mathtt{y*x}])$
12. $\{C[\mathtt{x} \mapsto \mathtt{x-1}, \mathtt{y} \mapsto \mathtt{y*x}]\}\,\mathtt{y := y*x;\ x := x-1}\,\{C\}$
13. $\models (C \implies C)$
14. $\{C[\mathtt{x} \mapsto \mathtt{x-1}, \mathtt{y} \mapsto \mathtt{y*x}]\}\,\mathtt{y := y*x}\,\{C[\mathtt{x} \mapsto \mathtt{x-1}]\}$
15. $\{C[\mathtt{x} \mapsto \mathtt{x-1}]\}\,\mathtt{x := x-1}\,\{C\}$

Outline

Soundness of Hoare Logic I

Soundness: no wrong propositions can be derived, i.e., every (syntactically) provable partial correctness property is also (semantically) valid

Soundness of Hoare Logic I

Soundness: no wrong propositions can be derived, i.e., every (syntactically) provable partial correctness property is also (semantically) valid

For the corresponding proof we use:

Lemma 10.1 (Substitution lemma)

For every $A \in Assn$, $x \in Var$, $a \in AExp$, $\sigma \in \Sigma$, *and* $I \in Int$:

$$\sigma \models^I A[x \mapsto a] \iff \sigma[x \mapsto \mathfrak{A}[\![a]\!]\sigma] \models^I A.$$

Soundness of Hoare Logic I

Soundness: no wrong propositions can be derived, i.e., every (syntactically) provable partial correctness property is also (semantically) valid

For the corresponding proof we use:

Lemma 10.1 (Substitution lemma)

For every $A \in Assn$, $x \in Var$, $a \in AExp$, $\sigma \in \Sigma$, *and* $I \in Int$:

$$\sigma \models^I A[x \mapsto a] \iff \sigma[x \mapsto \mathfrak{A}[\![a]\!]\sigma] \models^I A.$$

Proof.

by induction over $A \in Assn$ (omitted) □

Soundness of Hoare Logic II

Theorem 10.2 (Soundness of Hoare Logic)

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

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

Soundness of Hoare Logic II

Theorem 10.2 (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.) □