Semantics and Verification of Software

Lecture 9: 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

Assertions

Definition (Syntax of assertions)

The syntax of *Assn* is defined by the following context–free grammar:

$$a ::= z \mid x \mid i \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \in LExp$$
$$A ::= t \mid a_1 = a_2 \mid a_1 > a_2 \mid \neg A \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid \forall i.A \in Assn$$

Definition (Semantics of *LExp*)

An interpretation is an element of the set

$$Int := \{I \mid I : LVar \to \mathbb{Z}\}.$$

The value of an arithmetic expressions with logical variables is given by the functional

$$\mathfrak{L}[\![.]\!] : LExp \to (Int \to (\Sigma \to \mathbb{Z}))$$

where

$$\begin{aligned} \mathfrak{L}[\![z]\!]I\sigma &:= z & \mathfrak{L}[\![a_1+a_2]\!]I\sigma &:= \mathfrak{L}[\![a_1]\!]I\sigma + \mathfrak{L}[\![a_2]\!]I\sigma \\ \mathfrak{L}[\![x]\!]I\sigma &:= \sigma(x) & \mathfrak{L}[\![a_1-a_2]\!]I\sigma &:= \mathfrak{L}[\![a_1]\!]I\sigma - \mathfrak{L}[\![a_2]\!]I\sigma \\ \mathfrak{L}[\![i]\!]I\sigma &:= I(i) & \mathfrak{L}[\![a_1*a_2]\!]I\sigma &:= \mathfrak{L}[\![a_1]\!]I\sigma * \mathfrak{L}[\![a_2]\!]I\sigma \end{aligned}$$

Semantics of Assertions

Definition (Semantics of assertions)

Let $A \in Assn$, $\sigma \in \Sigma_\perp$, and $I \in Int$. The relation "σ satisfies A in I" (notation: $\sigma \models^I A$) is inductively defined by:

$$
\begin{array}{lll}
\sigma \models^I \mathsf{true} & & \\
\sigma \models^I a_1\mathsf{=}a_2 & \text{if } \mathfrak{L}[\![a_1]\!]I\sigma = \mathfrak{L}[\![a_2]\!]I\sigma \\
\sigma \models^I a_1\mathsf{>}a_2 & \text{if } \mathfrak{L}[\![a_1]\!]I\sigma > \mathfrak{L}[\![a_2]\!]I\sigma \\
\sigma \models^I \neg A & \text{if not } \sigma \models^I A \\
\sigma \models^I A_1 \wedge A_2 & \text{if } \sigma \models^I A_1 \text{ and } \sigma \models^I A_2 \\
\sigma \models^I A_1 \vee A_2 & \text{if } \sigma \models^I A_1 \text{ or } \sigma \models^I A_2 \\
\sigma \models^I \forall i.A & \text{if } \sigma \models^{I[i\mapsto z]} A \text{ for every } z \in \mathbb{Z} \\
\perp \models^I A & &
\end{array}
$$

Furthermore σ satisfies A ($\sigma \models A$) if $\sigma \models^I A$ for every interpretation $I \in Int$, and A is called valid ($\models A$) if $\sigma \models A$ for every state $\sigma \in \Sigma$.

Definition (Extension)

Let $A \in Assn$ and $I \in Int$. The extension of A with respect to I is given by

$$A^I := \{\sigma \in \Sigma_\perp \mid \sigma \models^I A\}.$$

Partial Correctness Properties

Definition (Partial correctness properties)

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

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

Outline

A Valid Partial Correctness Property

Example 9.1

- Let $\mathtt{x} \in \mathit{Var}$ and $i \in \mathit{LVar}$. We have to show:
$$\models \{i \leq \mathtt{x}\}\, \mathtt{x\ :=\ x+1}\, \{i < \mathtt{x}\}$$
- According to Def. 8.8, this is equivalent to
$$\sigma \models^I \{i \leq \mathtt{x}\}\, \mathtt{x\ :=\ x+1}\, \{i < \mathtt{x}\}$$
for every $\sigma \in \Sigma_\perp$ and $I \in \mathit{Int}$
- For $\sigma = \perp$ this is trivial. So let $\sigma \in \Sigma$:
$$\begin{aligned} & \sigma \models^I (i \leq \mathtt{x}) \\ \Longrightarrow\ & \mathfrak{L}[\![i]\!]I\sigma \leq \mathfrak{L}[\![\mathtt{x}]\!]I\sigma \quad \text{(Def. 8.5)} \\ \Longrightarrow\ & I(i) \leq \sigma(\mathtt{x}) \quad \text{(Def. 8.3)} \\ \Longrightarrow\ & I(i) < \sigma(\mathtt{x}) + 1 \\ & \qquad = (\mathfrak{C}[\![\mathtt{x\ :=\ x+1}]\!]\sigma)(\mathtt{x}) \\ \Longrightarrow\ & \mathfrak{C}[\![\mathtt{x\ :=\ x+1}]\!]\sigma \models^I (i < \mathtt{x}) \\ \Longrightarrow\ & \text{claim} \end{aligned}$$

Outline

Hoare Logic I

Goal: syntactic derivation of valid partial correctness properties

Definition 9.2 (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.

Example 9.3

Proof of $\{A\}$ `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:

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

Example 9.3 (continued)

Here the single propositions are given by:

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

Outline

1. Repetition: Assertions and Partial Correctness Properties
2. A Valid Partial Correctness Property
3. Proof Rules for Partial Correctness
4. Soundness of Hoare Logic

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 9.4 (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 9.5 (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.) □