CS101.3
Programing Language Semantics

Lecture 5

February 6, 2004

Axiomatic Semantics

- $\{A\}\texttt{skip}\{A\}$
- $\{A[a/X]\}X\texttt{:=}a\{A\}$
- $$\frac{\{A\}c_1\{C\} \quad \{C\}c_2\{B\}}{\{A\}c_1;c_2\{B\}}$$
- $$\frac{\{A\wedge b\}c_1\{B\} \quad \{A\wedge\neg b\}c_2\{B\}}{\{A\}\texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\{B\}}$$
- $$\frac{\{A\wedge b\}c\{A\}}{\{A\}\texttt{while}\ b\ \texttt{do}\ c\{A\wedge\neg b\}}$$
- $$\frac{A\Rightarrow A' \quad \{A'\}c\{B'\} \quad B'\Rightarrow B}{\{A\}c\{B\}}$$

Axiomatic Semantics — Defining Validity

What does $\{A\}c\{B\}$ mean?

Suppose we define $\sigma \models A$ (“A is true in state σ”) somehow.

Then “$\models \{A\}c\{B\}$” can be defined as
“$\forall(\sigma, \sigma') \in \mathcal{C}[\![c]\!].\ (\sigma \models A) \Rightarrow (\sigma' \models B)$”.

Note: “$F_1 \models F_2$” (where F_1 could be empty) is a standard notation for “formula F_2 is true (valid) under assumptions described by formula F_1”; and “$F_1 \vdash F_2$” is a standard notation for “formula F_2 is derivable under assumptions described by formula F_1”.

Expressions with Variables; Assertions

Arithmetical expressions with variables (**Aexpv**) — an extension of **Aexp** with variables (variables range over **Intvar**):

$$a \ ::= \ n \mid X \mid i \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2$$

Assertions (**Assn**) is an extension of the **Bexp**:

$$\begin{aligned} A ::= & \ \mathtt{true} \mid \mathtt{false} \mid a_1 = a_2 \mid a_1 \leq a_2 \\ & \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid \neg A_1 \mid A_1 \Rightarrow A_2 \\ & \mid \forall i.A \mid \exists i.A \end{aligned}$$

Meaning of `Aexpv` and `Assn`

Given $\sigma \in \Sigma$ and *an interpretation* $I : \texttt{Intvar} \to \mathbb{Z}$, we can define $\mathcal{A}v[\![\cdot]\!]I\sigma$:

$$\mathcal{A}v[\![n]\!]I\sigma := n, \quad \mathcal{A}v[\![X]\!]I\sigma := \sigma(X), \quad \mathcal{A}v[\![i]\!]I\sigma := I(i), \ldots$$

Now we can define $\sigma \models^I A$:

- $\sigma \models^I \texttt{true}$
- $\sigma \models^I a_1 \leq a_2$, if $\mathcal{A}v[\![a_1]\!]I\sigma \leq \mathcal{A}v[\![a_2]\!]I\sigma$
- $\sigma \models^I A \wedge B$, if $\sigma \models^I A$ and $\sigma \models^I B$
- $\sigma \models^I \forall i.A$, if $\sigma \models^{I[n/i]} A$ for all $n \in \mathbb{Z}$.

Lemma: $\mathcal{A}[\![a]\!]$ and $\mathcal{B}[\![b]\!]$ agree with the above definitions.

Meaning of Hoare Rules

What is the meaning of $\{A\}c\{B\}$?

$\models^I \{A\}c\{B\}$ if and only if
$\forall(\sigma, \sigma') \in \mathcal{C}[\![c]\!].(\sigma \models^I A) \Rightarrow (\sigma' \models^I B)$.

$\models \{A\}c\{B\}$ if and only if $\forall I \in (\texttt{Intvar} \rightarrow \mathbb{Z}). \models^I \{A\}c\{B\}$.

Theorem (soundness): $\vdash \{A\}c\{B\} \quad \Rightarrow \quad \models \{A\}c\{B\}$

The opposite is also true if we state the consequence rule as follows: $\dfrac{\models (A \Rightarrow A') \qquad \{A'\}c\{B'\} \qquad \models (B' \Rightarrow B)}{\{A\}c\{B\}}$