CS101.3
Programing Language Semantics

Lecture 6

February 13, 2004

Axiomatic Semantics

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

Meaning of `Aexpv` and `Assn`

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

- $\mathcal{A}v[\![n]\!]I\sigma := n;\ \mathcal{A}v[\![X]\!]I\sigma := \sigma(X);\ \mathcal{A}v[\![i]\!]I\sigma := I(i); \ldots$
- $\sigma \models^I$ **`tt`**
- $\sigma \models^I a_1 \leq a_2$, 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 $n \in \mathbb{Z}$.

$\models^I \{A\}c\{B\}$ 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 $\forall I \in (\mathbf{Intvar} \rightarrow \mathbb{Z}).\ \models^I \{A\}c\{B\}$.

Soundness

Lemma: $\sigma \vDash b$ iff $(\sigma, \texttt{tt}) \in \mathcal{B}[\![b]\!]$

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

Induction step of the soundness proof:
For an arbitrary $I \in \texttt{Intvar} \to \mathbb{Z}$,

Assuming $\vDash^I \{A \wedge b\}c\{A\}$

Establish $\vDash^I \{A\}\texttt{while}\ b\ \texttt{do}\ c\{A \wedge \neg b\}$

Reminder: $\vDash^I \{A\}c\{B\}$ is defined as
$\forall(\sigma, \sigma') \in \mathcal{C}[\![c]\!].(\sigma \vDash^I A) \Rightarrow (\sigma' \vDash^I B)$

Soundness — II

For an arbitrary $I \in \texttt{Intvar} \to \mathbb{Z}$,

Given $\forall(\sigma, \sigma') \in \mathcal{C}[\![c]\!].(\sigma \vDash^I A \wedge b) \Rightarrow (\sigma' \vDash^I A)$

Prove $\forall(\sigma, \sigma') \in \mathcal{C}[\![w]\!].(\sigma \vDash^I A) \Rightarrow (\sigma' \vDash^I A \wedge \neg b)$

Given $\forall(\sigma, \sigma') \in \mathcal{C}[\![c]\!].((\sigma \vDash^I A) \wedge (\sigma \vDash^I b)) \Rightarrow (\sigma' \vDash^I A)$

Prove $\forall(\sigma, \sigma') \in \mathcal{C}[\![w]\!].(\sigma \vDash^I A) \Rightarrow ((\sigma' \vDash^I A) \wedge \neg(\sigma' \vDash b))$

Given $\forall(\sigma, \sigma') \in \mathcal{C}[\![c]\!].((\sigma \vDash^I A) \wedge (\langle \sigma, b\rangle \to \texttt{tt})) \Rightarrow (\sigma' \vDash^I A)$

Prove $\forall(\sigma, \sigma') \in \mathcal{C}[\![w]\!].(\sigma \vDash^I A) \Rightarrow ((\sigma' \vDash^I A) \wedge (\langle \sigma', b\rangle \to \texttt{ff}))$

Or, equivalently

$\mathcal{C}[\![w]\!] \subseteq \{(\sigma, \sigma') \mid (\sigma \vDash^I A) \Rightarrow ((\sigma' \vDash^I A) \wedge (\langle \sigma', b\rangle \to \texttt{ff}))\}$

Soundness — III

Remember, $\mathcal{C}[\![w]\!] = \mathtt{fix}(F)$, where
$F(S) := \{(\sigma, \sigma) \mid \langle \sigma, b\rangle \rightarrow \mathtt{ff}\} \bigcup$
$\{(\sigma, \sigma') \mid \langle \sigma, b\rangle \rightarrow \mathtt{tt} \wedge \exists \sigma''.(\sigma, \sigma'') \in \mathcal{C}[\![c]\!] \wedge (\sigma'', \sigma') \in S\}$

For any T, if $F(T) \subseteq T$, then $\mathcal{C}[\![w]\!] \subseteq T$

Given $\forall (\sigma, \sigma') \in \mathcal{C}[\![c]\!].((\sigma \vDash^I A) \wedge (\langle \sigma, b\rangle \rightarrow \mathtt{tt})) \Rightarrow (\sigma' \vDash^I A)$
Prove
$\mathcal{C}[\![w]\!] \subseteq \{(\sigma, \sigma') \mid (\sigma \vDash^I A) \Rightarrow ((\sigma' \vDash^I A) \wedge (\langle \sigma', b\rangle \rightarrow \mathtt{ff}))\}$

E.g. for T defined as
$\{(\sigma, \sigma') \mid (\sigma \vDash^I A) \Rightarrow ((\sigma' \vDash^I A) \wedge (\langle \sigma', b\rangle \rightarrow \mathtt{ff}))\}$, prove
$F(T) \subseteq T$

Soundness — IV

$$T := \{(\sigma, \sigma') \mid (\sigma \vDash^I A) \Rightarrow ((\sigma' \vDash^I A) \wedge (\langle \sigma', b\rangle \rightarrow \texttt{ff}))\}$$

Define $F(S) := \{(\sigma, \sigma) \mid \langle \sigma, b\rangle \rightarrow \texttt{ff}\} \bigcup$

$$\{(\sigma, \sigma') \mid \langle \sigma, b\rangle \rightarrow \texttt{tt} \wedge \exists \sigma''.(\sigma, \sigma'') \in \mathcal{C}[\![c]\!] \wedge (\sigma'', \sigma') \in S\}$$

Given $\forall (\sigma, \sigma') \in \mathcal{C}[\![c]\!].((\sigma \vDash^I A) \wedge (\langle \sigma, b\rangle \rightarrow \texttt{tt})) \Rightarrow (\sigma' \vDash^I A)$

Prove $F(T) \subseteq T$

Assuming $(\sigma, \sigma') \in F(T)$, prove $(\sigma, \sigma') \in T$

If $\langle \sigma, b\rangle \rightarrow \texttt{ff}$, then $(\sigma, \sigma) \in T$ because

$(\sigma \vDash^I A) \Rightarrow ((\sigma \vDash^I A) \wedge (\langle \sigma, b\rangle \rightarrow \texttt{ff}))$

Assume $\langle \sigma, b\rangle \rightarrow \texttt{tt} \wedge \exists \sigma''.(\sigma, \sigma'') \in \mathcal{C}[\![c]\!] \wedge (\sigma'', \sigma') \in T$, need to show $(\sigma, \sigma') \in T$

Soundness — V

$T := \{(\sigma, \sigma') \mid (\sigma \models^I A) \Rightarrow ((\sigma' \models^I A) \wedge (\langle \sigma', b \rangle \rightarrow \texttt{ff}))\}$

Given $\forall (\sigma, \sigma') \in \mathcal{C}[\![c]\!].((\sigma \models^I A) \wedge (\langle \sigma, b \rangle \rightarrow \texttt{tt})) \Rightarrow (\sigma' \models^I A)$

Given σ'' s.t. $\langle \sigma, b \rangle \rightarrow \texttt{tt} \wedge (\sigma, \sigma'') \in \mathcal{C}[\![c]\!] \wedge (\sigma'', \sigma') \in T$

Given ~~$(\sigma \models^I A) \Rightarrow ((\sigma' \models^I A) \wedge (\langle \sigma', b \rangle \rightarrow \texttt{ff}))$~~

Prove $(\sigma' \models^I A) \wedge (\langle \sigma', b \rangle \rightarrow \texttt{ff})$

$\sigma \models^I A$, $\langle \sigma, b \rangle \rightarrow \texttt{tt}$, and $(\sigma, \sigma'') \in \mathcal{C}[\![c]\!]$, hence $\sigma'' \models^I A$

$\sigma'' \models^I A$ and $(\sigma'', \sigma') \in T$, hence $(\sigma' \models^I A) \wedge (\langle \sigma', b \rangle \rightarrow \texttt{ff})$

QED.

Exceptions

New Language

$$e \quad ::= \quad v \mid \lambda v.e \mid e_1\, e_2 \mid \texttt{throw}\, e \mid \texttt{try}\, e_1\, \texttt{catch}\, e_2$$