CS611 Lecture 25: Axiomatic semantics: soundness — October 27, 1999

Dongmin Liang

1 Introduction

Last time we introduced the notion of particial correctness assertion: $\{A\}c\{B\}$. The notation

$$\models \{A\}c\{B\}$$

means

$$\forall I \forall \sigma \in \Sigma_\perp \,.\, (\ \sigma \models^I A \quad \Longrightarrow \quad \mathcal{C}[\![c]\!]\sigma \models^I B\ )$$

Note that $\perp \models B$.

2 Hoare Rules

Now we need a proof system to prove partial correctness assetions. The notation

$$\vdash \{A\}c\{B\}$$

means $\{A\}c\{B\}$ is proved with the proof system. We don't know if or not the proof system will generate precisely the true partial correctness assertions. We will be interested to look into this issue later on.

We are going to introduce a set of rules, which are usually called Hoare rules (or Floyd-Hoare Rules).

Rule for skip:

$$\frac{}{\{A\}\textbf{skip}\{A\}}$$

Rule for assignment:

$$\frac{}{\{B[a/X]\}X := a\{B\}}$$

Rule for sequencing:

$$\frac{\{A\}c_0\{C\} \qquad \{C\}c_1\{B\}}{\{A\}c_0;c_1\{B\}}$$

C is called intermediate assertion.

Rule for conditionals:

$$\frac{\{A \wedge b\}c_0\{B\} \qquad \{A \wedge \neg b\}c_1\{B\}}{\{A\}\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1\{B\}}$$

Rule for while loops:

$$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while } b \textbf{ do } c\{A \wedge \neg b\}}$$

A is called loop invariant of the "**while**" statement.

Rule of consequence:

$$\frac{\models (A \Rightarrow A') \qquad \{A'\}c\{B'\} \qquad \models (B' \Rightarrow B)}{\{A\}c\{B\}}$$

This proof system is called Hoare Logic.

3 An Example

Let's look at an example of using Hoare Logic:

$$\dfrac{\dfrac{\models X<Y \Rightarrow (Y\geq X \wedge Y\geq Y) \quad \overline{\{Y\geq X\wedge Y\geq Y\}Z:=Y\{Z\geq X\wedge Z\geq Y\}} \quad \models \ldots}{\{X<Y\}Z:=Y\{Z\geq X\wedge Z\geq Y\}} \qquad \dfrac{\models \neg(X<Y) \Rightarrow (X\geq X\wedge X\geq Y) \quad \overline{\{X\geq X\wedge X\geq Y\}Z:=X\{Z\geq X\wedge Z\geq Y\}} \quad \models \ldots}{\{\neg(X<Y)\}Z:=X\{Z\geq X\wedge Z\geq Y\}}}{\{\mathbf{true}\}\mathbf{if}\ X<Y\ \mathbf{then}\ Z:=Y\ \mathbf{else}\ Z:=X\{Z\geq X\wedge Z\geq Y\}}$$

4 Soundness of Hoare Rules

We would like the proof system to be sound. The notation

$$\vdash \{A\}c\{B\} \quad \Longrightarrow \quad \models \{A\}c\{B\}$$

is called soundness. We actually can prove that for Hoare Logic.

We will use standard rule induction. It suffices to show that each individual rule preserve the truth properties. Let's look at each rule.

Rule for skip: Clearly,

$$\models \{A\}\mathbf{skip}\{A\}$$

Rule for assignment:

We need the following lemma:

Lemma

$$\sigma \models^I B[a/X] \quad \Longleftrightarrow \quad \sigma[X \mapsto \mathcal{A}[\![a]\!]\sigma] \models^I B$$

The proof for this lemma is left for homework.

We need to show

$$\models \{B[a/X]\}X := a\{B\} \ ,$$

or equivalently,

$$\sigma \models^I B[a/X] \quad \Longrightarrow \quad \mathcal{C}[\![X := a]\!]\sigma \models^I B \ .$$

$\mathcal{C}[\![X := a]\!]$ is $\lambda\sigma'.\sigma'[X \mapsto \mathcal{A}[\![a]\!]\sigma']$. Thus, by the lemma the above statement is clearly true.

Rule for sequencing: (left for exercise)

Rule for conditionals: (left for exercise)

Rule for while loops:

Given $\models \{A \wedge b\}c\{A\}$, we need to show $\models \{A\}\mathbf{while}\ b\ \mathbf{do}\ c\{A \wedge \neg b\}$. We write

$$w \equiv \mathbf{while}\ b\ \mathbf{do}\ c$$

to keep things shorter. Equivalently, we need to show

$$\sigma \models^I A \quad \Longrightarrow \quad \mathcal{C}[\![w]\!]\sigma \models^I \{A \wedge \neg b\} \ .$$

Recall that

$$\mathcal{C}[\![w]\!] = \mathbf{fix}\ \lambda f : \Sigma_\perp \to \Sigma_\perp.\ \lambda\sigma : \Sigma_\perp.\ \ \mathbf{if}\ B[\![b]\!]\sigma\ \mathbf{then}\ f(\mathcal{C}[\![c]\!]\sigma)\ \mathbf{else}\ \sigma \ ,$$

i.e.,

$$\mathcal{C}[\![w]\!] = \bigsqcup_{n\in\omega} \Gamma^n(\perp) \ ,$$

where

$$\Gamma = \lambda f : \Sigma_\perp \to \Sigma_\perp.\ \lambda\sigma : \Sigma_\perp.\ \ \mathbf{if}\ B[\![b]\!]\sigma\ \mathbf{then}\ f(\mathcal{C}[\![c]\!]\sigma)\ \mathbf{else}\ \sigma \ .$$

Therefore,

$$\mathcal{C}[\![w]\!]\sigma = (\bigsqcup_{n\in\omega} \Gamma^n(\perp))\sigma = \bigsqcup_{n\in\omega} (\Gamma^n(\perp)\sigma)\ .$$

Notice that $\Sigma_\perp$ is a pointed flat cpo. It is sufficient to show that

$$\sigma \models^I A \quad\Longrightarrow\quad \Gamma^n(\perp)\sigma \models^I A \wedge \neg b$$

holds for all $n \in \omega$.

We proceed by induction on n.

Basis: $n = 0$. We need to show

$$\sigma \models^I A \quad\Rightarrow\quad \perp \models^I A \wedge \neg b$$

This is vacuously true, because by definition $\perp \models^I A \wedge \neg b$ is true.

Induction Hypothesis: Assume for all $m < n$,

$$\sigma \models^I A \quad\Longrightarrow\quad \Gamma^m(\perp)(\sigma) \models^I A \wedge \neg b$$

Induction Step: $n > 0$. Since $\Gamma^n(\perp) = \Gamma(\Gamma^{n-1}(\perp))$, it suffices to show

$$\sigma \models^I A \quad\Longrightarrow\quad (\textbf{if } B[\![b]\!]\sigma \textbf{ then } \Gamma^{n-1}(\perp)(\mathcal{C}[\![c]\!]\sigma) \textbf{ else } \sigma) \models^I A \wedge \neg b$$

There are two cases:

1. $B[\![b]\!]\sigma = \textbf{false}$. $\sigma \models \neg b$, since $B[\![b]\!]\sigma = \textbf{false}$. Therefore,

$$\sigma \models^I A \wedge \neg b$$

2. $B[\![b]\!]\sigma = \textbf{true}$. $\sigma \models b$, since $B[\![b]\!]\sigma = \textbf{true}$. Therefore,

$$\sigma \models^I A \wedge b$$

By the assumption $\models \{A \wedge b\}c\{A\}$, we have $\mathcal{C}[\![c]\!]\sigma \models^I A$. By induction hypothesis, we have

$$\Gamma^{n-1}(\perp)(\mathcal{C}[\![c]\!]\sigma) \models^I A \wedge \neg b$$

5 Weakest Pre-condition: An introduction

The consequence rule

$$\frac{\models (A \Rightarrow A') \qquad \{A'\}c\{B'\} \qquad \models (B' \Rightarrow B)}{\{A\}c\{B\}}$$

includes premises of the form "$\models A \Rightarrow A'$" and "$\models B' \Rightarrow B$". Proofs of assertions $A \Rightarrow A'$ and $B' \Rightarrow B$ rely on an underlying proof system. If we could plug-in such a proof system, we might have a automated way to produce proof for partial correctness assertions. But we don't know how to pick a intermediate assertion C for the sequencing rule

$$\frac{\{A\}c_0\{C\} \qquad \{C\}c_1\{B\}}{\{A\}c_0; c_1\{B\}}$$

and A' and B' for the consequence rule

$$\frac{\models (A \Rightarrow A') \qquad \{A'\}c\{B'\} \qquad \models (B' \Rightarrow B)}{\{A\}c\{B\}}$$

Define the weakest precondition of c with respect to B:

$$wp(c, B) = \{\sigma | \mathcal{C}[\![c]\!]\sigma \models^I B\}$$

We claim: $wp(c, B)$ is an assertion, i.e., we can write an assertion which captures exactly the set of states in $wp(c, B)$.

Moreover, we will show that $wp(c, B)$ is the weakest possible pre-condition. Let A' be an assertion which captures exactly the set of states in $wp(c, B)$, i.e., $\{\sigma \mid \sigma \models^I A'\} = wp(c, B)$. Suppose $\{A\}c\{B\}$. Recall that $\models \{A\}c\{B\}$ means

$$\forall I \forall \sigma \in \Sigma_\perp. \ (\models^I A \implies \mathcal{C}[\![c]\!]\sigma \models^I B)$$

or equivalently,

$$\forall I. \ \{\sigma \mid \sigma \models^I A\} \subseteq \{\sigma \mid \mathcal{C}[\![c]\!]\sigma \models^I B\} (= wp(c, B)) \ .$$

Then $A \Rightarrow A'$.

For the case of sequencing rule

$$\frac{\{A\}c_0\{C\} \qquad \{C\}c_1\{B\}}{\{A\}c_0; c_1\{B\}}$$

We can use $wp(c, B)$ as intermdiate assertion. If there exists C such that $\{A\}c_0\{C\}$ and $\{C\}c_1\{B\}$, then $C \Rightarrow wp(c, B)$. Hence by $\{A\}c_0\{C\}$, we have $\{A\}c_0\{wp(c, B)\}$.

We could also define the notion of strongest post-condition. For the case of consequence rule,

$$\frac{\models (A \Rightarrow A') \qquad \{A'\}c\{B'\} \qquad \models (B' \Rightarrow B)}{\{A\}c\{B\}}$$

We can let A' be the weakest pre-condition of c and B' be the strongest post-condition of c.

Next time we will introduce actual rules to produce weakest preconditions.