CS611 Lecture 15 **Soundness of Hoare Logic** 1 October 2003

Scribe: Maya Haridasan, Mohamed ElHawary Lecturer: Radu Rugina

---

In the last lecture we defined the concept of validity, as being the satisfaction with respect to any state and interpretation. We defined validity of

- Assertions:

$$(\models A) \quad \text{iff} \quad (\forall \sigma, I.\ \ \sigma \models^I A)$$

- Partial Correctness Assertions:

$$(\models \{A\}c\{B\}) \quad \text{iff} \quad (\forall \sigma, I.\ \ \sigma \models^I \{A\}c\{B\})$$

  This can also be written as

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

1 Hoare Logic

In the last lecture we also saw the Hoare Logic, which is a proof system that defines a collection of proof rules, often called Hoare rules.

What's the relation between things that can be defined by the Hoare Logic ($\vdash$) and valid assertions ($\models$)? To answer this question we need to verify the soundness and the completeness of Hoare Logic.

- Soundness: Is every theorem in Hoare Logic a valid assertion?

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

- Completeness: Is every valid assertion also a theorem in Hoare Logic?

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

In this lecture we will prove the answer to the first question: The Hoare Logic is a sound system.

2 Soundness of Hoare Logic

When every rule of a proof system is sound, the proof system itself is considered to be sound. We will prove soundness by induction on derivation of

$$P(d) \iff ((d \vdash \{A\}c\{B\}) \implies (\models \{A\}c\{B\}))$$

We need to show for each Hoare rule that, if triples in the premise are theorems and satisfy the property above, then the conclusion also satisfies the property. We next examine all the rules for Hoare Logic:

- *Skip* ($c \equiv \textbf{skip}$)

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

  we want to show that:

$$\forall \sigma, I.\ \ (\sigma \models^I A) \quad \Longrightarrow \quad (\mathcal{C}[\![\textbf{skip}]\!]\sigma \models^I A)$$

  This is trivial, since $\mathcal{C}[\![\textbf{skip}]\!]\sigma = \sigma$.

- *Assignment* ($c \equiv X := a$)

$$\overline{\{A[X \to a]\}X := a\{A\}}$$

We want to show that:

$$\forall \sigma, I.\ (\sigma \models^I A[X \to a]) \implies (\mathcal{C}[\![X := a]\!]\sigma \models^I A)$$

We can prove by structural induction on assertion A that:

$$\forall \sigma, I.\ (\sigma \models^I A[X \to a]) \implies (\sigma[X \to \mathcal{A}[\![a]\!]\sigma] \models^I A)$$

Since we have

$$\mathcal{C}[\![X := a]\!]\sigma = \sigma[X \to \mathcal{A}[\![a]\!]\sigma]$$

$$\forall \sigma, I.\ (\sigma \models^I A[X \to a]) \implies (\mathcal{C}[\![X := a]\!]\sigma \models^I A)$$

- *Sequencing* ($c \equiv c_0; c_1$)

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

We want to show that:

$$\forall \sigma, I.\ (\sigma \models^I A) \implies (\mathcal{C}[\![c_0; c_1]\!]\sigma \models^I B)$$

Let's consider the two following theorems:

$$\vdash \{A\}c_0\{C\} \quad \text{and} \quad \vdash \{C\}c_1\{B\}$$

By induction hypothesis, these partial correctness assertions are valid:

$$\models \{A\}c_0\{C\} \quad \text{and} \quad \models \{C\}c_1\{B\}$$

We need to consider two subcases:

  - Case 1: if $\mathcal{C}[\![c_0]\!]\sigma = \perp$

$$(\mathcal{C}[\![c_0]\!]\sigma = \perp) \implies (\mathcal{C}[\![c_0; c_1]\!]\sigma = \perp) \quad \models^I B$$

(Because $\perp$ satisfies any assertion)

  - Case 2: if $\mathcal{C}[\![c_0]\!]\sigma \neq \perp$

$$\mathcal{C}[\![c_0; c_1]\!]\sigma = \mathcal{C}[\![c_1]\!](\mathcal{C}[\![c_0]\!]\sigma)$$

Given that $\models \{A\}c_0\{C\}$ and $\models \{C\}c_1\{B\}$

$$\begin{aligned} \sigma \models^I A &\implies \mathcal{C}[\![c_0]\!]\sigma \models^I C \\ &\implies \mathcal{C}[\![c_1]\!](\mathcal{C}[\![c_0]\!]\sigma) \models^I B \end{aligned}$$

- *Conditionals* ($c \equiv \textbf{if}\, b\, \textbf{then}\, c_0\, \textbf{else}\, c_1$)

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

  Let's consider the two following theorems:

$$\vdash \{A \wedge b\}c_0\{B\} \quad \text{and} \quad \vdash \{A \wedge \neg b\}c_1\{B\}$$

  By induction hypothesis, these partial correctness assertions are valid:

$$\models \{A \wedge b\}c_0\{B\} \quad \text{and} \quad \models \{A \wedge \neg b\}c_1\{B\}$$

  We will consider 2 subcases:

  - Case 1: $\mathcal{B}[\![b]\!]\sigma = \textbf{true}$

$$\begin{array}{rcl} (\mathcal{B}[\![b]\!]\sigma = \textbf{true}) & \implies & (\sigma \models^I b) \\ (\sigma \models^I A) & \implies & (\sigma \models^I \{A \wedge b\}) \end{array}$$

    By induction hypothesis we know that $(\vdash \{A \wedge b\}c_0\{B\}) \implies (\models \{A \wedge b\}c_0\{B\})$. Therefore,

$$\implies \mathcal{C}[\![c_0]\!]\sigma \models^I B$$

  - Case 2: $\mathcal{B}[\![b]\!]\sigma = \textbf{false}$

$$\begin{array}{rcl} (\mathcal{B}[\![b]\!]\sigma = \textbf{false}) & \implies & (\sigma \models^I \neg b) \\ (\sigma \models^I A) & \implies & (\sigma \models^I \{A \wedge \neg b\}) \end{array}$$

    By induction hypothesis we know that $(\vdash \{A \wedge \neg b\}c_1\{B\}) \implies (\models \{A \wedge \neg b\}c_1\{B\})$. Therefore,

$$\implies \mathcal{C}[\![c_1]\!]\sigma \models^I B$$

  By combining these two cases:

$$\forall \sigma, I.\ (\sigma \models^I A) \implies (\mathcal{C}[\![\textbf{if}\, b\, \textbf{then}\, c_0\, \textbf{else}\, c_1]\!]\sigma \models^I B)$$

- *While loops* ($c \equiv \textbf{while}\, b\, \textbf{do}\, c$)

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

  Let $\sigma \models^I A$.
  Assuming the induction hypothesis (**IH 1**):

$$(\vdash \{A \wedge b\}c\{A\}) \implies (\models \{A \wedge b\}c\{A\})$$

  We want to prove that: $\mathcal{C}[\![\textbf{while}\, b\, \textbf{do}\, c]\!]\sigma \models^I \{A \wedge \neg b\}$

Recall that $\mathcal{C}[\![\textbf{while}\, b\, \textbf{do}\, c]\!] = \mathit{fix}(\Gamma) = \bigsqcup^n \Gamma^n(\perp)$. We will then prove that

$$\forall n\ (\forall \sigma, I.\ \ (\sigma \models^I A) \implies (\Gamma^n(\perp)(\sigma) \models^I \{A \wedge \neg b\}))$$

We will prove this by standard induction on n.

Base case: $n = 0$:

$$(\Gamma^0(\perp)(\sigma) = \perp) \implies (\Gamma^0(\perp)(\sigma) \models^I \{A \wedge \neg b\})$$

Induction step:

We assume (**IH 2**): $\forall n\ (\forall \sigma, I.\ \ (\sigma \models^I A) \implies (\Gamma^n(\perp)(\sigma) \models^I \{A \wedge \neg b\}))$

And we want to prove:

$$\forall \sigma, I.\ \ (\sigma \models^I A) \implies (\Gamma^{n+1}(\perp)(\sigma) \models^I \{A \wedge \neg b\})$$

It has been previously shown that:

$$\Gamma^{n+1}(\perp) = \Gamma(\Gamma^n(\perp)) = \mathit{cond} \circ \langle \mathcal{B}[\![b]\!], (\Gamma^n(\perp))^* \circ\ \mathcal{C}[\![c]\!], \mathit{id}\rangle$$

There are two possible subcases:

- Case 1: $\mathcal{B}[\![b]\!]\sigma = \textbf{false}$. Given that

  $$\Gamma^{n+1}(\perp)(\sigma) = \mathit{id}(\sigma) = \sigma \models^I A$$

  Then we have:

  $$\begin{aligned} (\mathcal{B}[\![b]\!]\sigma = \textbf{false}) &\implies (\sigma \models^I \neg b) \\ (\sigma \models^I A) &\implies (\sigma \models^I \{A \wedge \neg b\}) \\ &\implies (\Gamma^{n+1}(\perp)(\sigma) \models^I \{A \wedge \neg b\}) \end{aligned}$$

- Case 2: $\mathcal{B}[\![b]\!]\sigma = \textbf{true}$

  $$\Gamma^{n+1}(\perp)(\sigma) = ((\Gamma^n(\perp))^* \circ \mathcal{C}[\![c]\!])(\sigma)$$

  We need to analyze two subcases: when the execution of c yields $\perp$ or not:

  * Subcase 1: $\mathcal{C}[\![c]\!]\sigma = \perp$

    $$\begin{aligned} (\mathcal{C}[\![c]\!]\sigma = \perp) &\implies ((\Gamma^{n+1}(\perp))(\sigma) = \perp) \\ &\implies ((\Gamma^{n+1}(\perp))(\sigma) \models^I \{A \wedge \neg b\}) \end{aligned}$$

  * Subcase 2: $\mathcal{C}[\![c]\!]\sigma \neq \perp$

    $$(\mathcal{C}[\![c]\!]\sigma \neq \perp) \implies ((\Gamma^{n+1}(\perp))(\sigma) = (\Gamma^n(\perp))(\mathcal{C}[\![c]\!]\sigma))$$

    We know that

    $$(\sigma \models^I A)\ ,\ (\mathcal{C}[\![c]\!]\sigma \neq \perp) \text{ and } ((\mathcal{B}[\![b]\!]\sigma = \textbf{true}) \implies (\sigma \models^I b))$$

    Therefore, we have:

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

    Given that by induction hypothesis (**IH 1**) we have $(\models \{A \wedge b\} c \{A\})$,

$$\implies \mathcal{C}[\![c]\!]\sigma \models^I A$$

By applying induction hypothesis (**IH 2**), we finally conclude that:

$$\implies \Gamma^{n+1}(\perp)(\sigma) \models^I \{A \wedge \neg b\}$$

This concludes the proof for the while loop.

- *Consequence*

$$\frac{A \Rightarrow A' \quad \{A'\}\ c\ \{B'\} \quad B' \Rightarrow B}{\{A\}\ c\ \{B\}}$$

Let this proof tree be a derivation d. The above rule shows that $\{A'\}c\{B'\}$ is also a theorem, and its derivation d', where $d' \vdash \{A'\}c\{B'\}$, is a subderivation of d, where $d \vdash \{A\}c\{B\}$. By induction hypothesis:

$$(d' \vdash \{A'\}c\{B'\}) \implies (\models \{A'\}c\{B'\})$$

Hence $(\models \{A'\}c\{B'\})$.

Let I be an interpretation and let $(\sigma \models^I A)$.

Because $(\models A \Rightarrow A')$, $(\models \{A'\}c\{B'\})$, and $(\models B' \Rightarrow B)$, we have:

$$\begin{aligned} (\sigma \models^I A) &\implies (\sigma \models^I A') \\ &\implies (\mathcal{C}[\![c]\!]\sigma \models^I B') \\ &\implies (\mathcal{C}[\![c]\!]\sigma \models^I B) \end{aligned}$$

Thus, by induction on derivations we have proven that every theorem is valid.