Scribe: Xinyang Zhang, Xiangyang Lan Lecturer: Radu Rugina

1 Partial Correctness Assertions

- Partial correctness assertions have the form $\{A\}c\{B\}$. We define the satisfaction relation between states and partial correctness assertion, with respect to an interpretation I, by:

$$\sigma \models^I \{A\}c\{B\} \text{ iff } (\sigma \models^I A \;\wedge\; \mathcal{C}[\![c]\!]\sigma \neq \perp) \implies \mathcal{C}[\![c]\!]\sigma \models^I B$$

  Since $\perp$ satisfies any assertion, we can write this as follows:

$$\sigma \models^I \{A\}c\{B\} \text{ iff } (\sigma \models^I A \implies \mathcal{C}[\![c]\!]\sigma \models^I B)$$

- Using operational semantics to express partial correctness assertion

$$(\sigma \models^I A \;\wedge\; \langle \sigma, c\rangle \Rightarrow \sigma') \implies \sigma' \models^I B$$

- **Validity:** is satisfaction with respect to any state and interpretation:
  - Partial correctness assertion $\{A\}c\{B\}$ is *valid*: $\models \{A\}c\{B\}$ iff $\forall \sigma, I : \sigma \models^I \{A\}c\{B\}$
  - Assertion A is *valid*: $\models A$ iff $\forall \sigma, I : \sigma \models^I A$

2 Hoare Logic

2.1 Hoare rules

skip ($c \equiv skip$)

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

assignment ($c \equiv X := a$)

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

sequencing ($c \equiv c_0; c_1$)

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

conditionals ($c \equiv if\ b\ then\ c_0\ else\ c_1$)

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

while loops ($c \equiv while\ b\ do\ c$)

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

consequence rule

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

The Hoare rules are thought of as a proof system, derivation are called *proofs* and any conclusion of a derivation a *theorem*. We shall write $\vdash \{A\}c\{B\}$ when $\{A\}c\{B\}$ is a theorem.

2.2 Soundness of Hoare Logic

- **Soundness**: show that each theorem in Hoare logic is valid, i.e., $\vdash \{A\}c\{B\} \;\Rightarrow\; \models \{A\}c\{B\}$.
- Can prove soundness by rule induction, where the property that we want to prove for each triple is $P(\{A\}c\{B\}) = \;\models \{A\}c\{B\}$. For this we need to show for each rule that, if triples in the premise are theorems and satisfy the property, then conclusion satisfies the property P.
- $c \equiv skip$

$$\forall \sigma, I \;\; \sigma \models^I \{A\} \implies \mathcal{C}[\![skip]\!]\sigma \models^I \{A\} \quad (\text{since } \mathcal{C}[\![skip]\!]\sigma = \sigma)$$

- $c \equiv X := a$

$$\begin{aligned} \forall \sigma, I\; \sigma \models^I \{A[X \to a]\} &\implies \sigma[X \to \mathcal{A}[\![a]\!]\sigma] \models^I \{A\} && (\text{This can be proved by structural induction on A}) \\ &\implies \mathcal{C}[\![X := a]\!]\sigma \models^I \{A\} && (\mathcal{C}[\![X := a]\!]\sigma \;=\; \sigma[X \to \mathcal{A}[\![a]\!]\sigma]) \end{aligned}$$

- $c \equiv c_0; c_1$
  Consider two theorems $\vdash \{A\}c_0\{C\}$ and $\vdash \{C\}c_1\{B\}$. By induction hypothesis, these partial correctness assertions are valid: $\models \{A\}c_0\{C\}$ and $\models \{C\}c_1\{B\}$

  Consider arbitrary σ and I such that $\sigma \models^I \{A\}$. We have two subcases.

  Case 1: $\mathcal{C}[\![c_0]\!]\sigma = \bot$

$$\begin{aligned} \mathcal{C}[\![c_0]\!]\sigma = \bot &\implies \mathcal{C}[\![c_0; c_1]\!]\sigma = \bot \\ &\implies \mathcal{C}[\![c_0; c_1]\!]\sigma \models^I \{B\} \quad (\bot \text{ satisfies any assertion}) \end{aligned}$$

  Case 2: $\mathcal{C}[\![c_0]\!]\sigma \neq \bot$

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

- $c \equiv \textbf{if}\, b\, \textbf{then}\, c_0\, \textbf{else}\, c_1$
  Consider two theorems $\vdash \{A \wedge b\}c_0\{B\}$ and $\vdash \{A \wedge \neg b\}c_1\{B\}$. By induction hypothesis, these partial correctness assertions are valid: $\models \{A \wedge b\}c_0\{B\}$ and $\models \{A \wedge \neg b\}c_1\{B\}$

  Consider arbitrary σ and I such that $\sigma \models^I \{A\}$. We have two subcases.

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

$$\begin{aligned} \mathcal{B}[\![b]\!]\sigma = \textbf{true} &\implies \sigma \models^I b \\ \sigma \models^I \{A\} &\implies \sigma \models^I A \wedge b \\ &\implies \mathcal{C}[\![c_0]\!]\sigma \models^I \{B\} && (\models \{A \wedge b\}c_0\{B\}) \end{aligned}$$

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

$$\begin{aligned} \mathcal{B}[\![b]\!]\sigma = \textbf{false} &\implies \sigma \models^I \neg b \\ \sigma \models^I \{A\} &\implies \sigma \models^I A \wedge \neg b \\ &\implies \mathcal{C}[\![c_1]\!]\sigma \models^I \{B\} && (\models \{A \wedge \neg b\}c_1\{B\}) \end{aligned}$$

  Combine the two cases:

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

- $c \equiv \textbf{while}\, b\, \textbf{do}\, c$
  Consider a theorem $\vdash \{A \wedge b\}c\{A\}$. By induction hypothesis, it is valid: $\models \{A \wedge b\}c\{A\}$.

  We'd like to prove that:

  $$\forall \sigma, I\ .\ \sigma \models^I A \implies \mathcal{C}[\![\textbf{while}\, b\, \textbf{do}\, c]\!]\sigma \models^I \{A \wedge \neg b\})$$

  Recall that $\mathcal{C}[\![\textbf{while}\, b\, \textbf{do}\, c]\!] = \mathit{fix}(\Gamma) = \bigsqcup \Gamma^n(\perp)$. We claim that it's sufficient to show:

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

  Why this is sufficient is left as an exercise (recall the cpo domain Σ for states).

  We next prove (1) by 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 that

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

  We attempt to prove that:

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

  Recall that $\Gamma(\Gamma^n(\perp)) = \mathit{cond} \circ \langle \mathcal{B}[\![b]\!], (\Gamma^n(\perp))^* \circ \mathcal{C}[\![c]\!], \mathit{id}\rangle$.
  Consider arbitrary σ and I such that $\sigma \models^I A$. We then have two subcases.

  Case 1: $\mathcal{B}[\![b]\!]\sigma = \textbf{false}\quad \Gamma(\Gamma^n(\perp))(\sigma) = \sigma$

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

  Case 2: $\mathcal{B}[\![b]\!]\sigma = \textbf{true}\quad \Gamma(\Gamma^n(\perp))(\sigma) = ((\Gamma^n(\perp))^* \circ \mathcal{C}[\![c]\!])(\sigma)$
  Subcase 1: $\mathcal{C}[\![c]\!]\sigma = \perp$

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

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

  $$\begin{aligned} \mathcal{B}[\![b]\!]\sigma = \textbf{true} &\implies \sigma \models^I b \\ \sigma \models^I \{A\} &\implies \sigma \models^I \{A \wedge b\} \\ &\implies \mathcal{C}[\![c]\!]\sigma \models^I \{A\} && (\models \{A \wedge b\}c\{A\}) \\ &\implies \Gamma^n(\perp)(\mathcal{C}[\![c]\!]\sigma) \models^I \{A \wedge \neg b\} && \text{(Induction Hypothesis)} \\ &\implies \Gamma(\Gamma^n(\perp))(\sigma) \models^I \{A \wedge \neg b\} \end{aligned}$$

  Thus, we proved that in all cases:

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