Scribe: Zoya Svitkina and Ara Hayrapetyan Lecturer: Radu Rugina

In the previous lecture we defined two important notions that were motivated by the partial correctness assumptions of the axiomatic semantics.

- *Validity* ($\models$):

  Define $\models \{A\}c\{B\}$ if for all interpretations I and states σ, $\sigma \models^I \{A\}c\{B\}$, that is if $\sigma \models^I A$, then $\mathcal{C}[\![c]\!]\sigma \models^I B$. In this case we say that $\{A\}c\{B\}$ is *valid*.

- *Theorem* ($\vdash$)

  Define $\vdash \{A\}c\{B\}$ if $\{A\}c\{B\}$ has a derivation in the proof system consisting of Hoare rules. In this case we say that $\{A\}c\{B\}$ is a *theorem*.

We were also interested whether the Hoare proof rules satisfy two very general properties of logical systems: soundness and completeness.

Soundness: Hoare logic is sound if every theorem is valid. To prove this, it is shown that the axioms are valid, and that every rule in the Hoare proof system preserves validity. That is, if every premise of the rule is valid, then the conclusion is also valid.

Completeness: Hoare logic is complete if we are able to prove every valid partial correctness assertion using Hoare logic.

We ended last lecture in the middle of the soundness proof. In this lecture we will complete the soundness proof of Hoare rules, and will proceed with describing completeness results for it.

1 Soundness Proof (continued):

The rule for while-loops: $$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while}\, b\, \textbf{do}\, c\{A \wedge \neg b\}}$$

We know by the induction hypothesis that $\models \{A \wedge b\}c\{A\}$. In other words, for all states σ and interpretations I, $\sigma \models^I \{A \wedge b\} \Rightarrow \mathcal{C}[\![c]\!]\sigma \models^I \{A\}$. And we want to show that for all states σ and interpretations I, $\sigma \models^I \{A\} \Rightarrow \mathcal{C}[\![\textbf{while}\, b\, \textbf{do}\, c]\!]\sigma \models^I \{A \wedge \neg b\}$.

Note that since the semantics of the while loop w ($w \equiv \textbf{while}\, b\, \textbf{do}\, c$) was defined as $\mathcal{C}[\![w]\!] = \bigsqcup_n \Gamma^n(\perp)$, it is sufficient to show that $\forall n \forall \sigma \forall I \;\; \sigma \models^I \{A\} \Rightarrow \Gamma^n(\perp)\sigma \models^I \{A \wedge \neg b\}$.

We will prove this by induction on n.

Base Case: $n = 0$. Trivial, since $\Gamma^0(\perp)\sigma = \perp$, and $\perp$ satisfies anything under all interpretations.

Inductive Step: Let us assume that the claim holds for n. We want to show that $\sigma \models^I \{A\} \Rightarrow \Gamma^{n+1}(\perp)\sigma \models^I \{A \wedge \neg b\}$. Let $\sigma \models^I \{A\}$. Since $\Gamma(\gamma) = \mathit{cond} \circ \langle \mathcal{B}[\![b]\!], \gamma^* \circ \mathcal{C}[\![c]\!], \mathit{id}\rangle$, therefore $\Gamma(\Gamma^n(\perp)) = \mathit{cond} \circ \langle \mathcal{B}[\![b]\!], (\Gamma^n(\perp))^* \circ \mathcal{C}[\![c]\!], \mathit{id}\rangle$.

There are two cases:

- $\mathcal{B}[\![b]\!]\sigma = \textbf{false}$, then $\Gamma(\Gamma^n(\perp))\sigma = \sigma$. Therefore, from $\sigma \models^I \{A\}$ and $\sigma \models^I \{\neg b\}$ we will get $\sigma \models^I \{A \wedge \neg b\}$.

- $\mathcal{B}[\![b]\!]\sigma = \textbf{true}$, then $\Gamma^{n+1}(\perp)\sigma = ((\Gamma^n(\perp))^* \circ \mathcal{C}[\![c]\!])\sigma$. We would like to remove the $*$ from this equation, therefore we consider nontermination separately.

  - if $\mathcal{C}[\![c]\!]\sigma = \perp$ then $\Gamma^{n+1}(\perp) = \perp \models^I \{A \wedge \neg b\}$ trivially, since $\perp$ satisfies everything.
  - if $\mathcal{C}[\![c]\!]\sigma \neq \perp$ then we can remove the $*$, that is $\Gamma^{n+1}(\perp) = \Gamma^n(\perp)(\mathcal{C}[\![c]\!]\sigma)$. Since b evaluates to true, we have $\sigma \models^I \{b\}$. Also, since $\sigma \models^I \{A\}$, we get $\sigma \models^I \{A \wedge b\}$. Now applying the global induction hypothesis (i.e., from structural induction), we obtain $\mathcal{C}[\![c]\!]\sigma \models^I \{A\}$, and applying the

induction hypothesis on n (the local induction hypothesis, i.e. from induction on n) we obtain $\Gamma^n(\bot)(\mathcal{C}[\![c]\!]\sigma) \models^I \{A \wedge \neg b\}$. Finally, observing that $\Gamma^n(\bot)(\mathcal{C}[\![c]\!]\sigma) = \Gamma^{n+1}\sigma$, we conclude the proof of the soundness theorem.

2 Relative Completeness

Gödel's *Incompleteness Theorem* (1931) states that there is no proof system where all valid assertions are theorems. This implies that Hoare logic is not complete either, is because of the consequence rule.

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

Since $A \Rightarrow A'$ and $B' \Rightarrow B$ can be statements from number theory, and number theory is incomplete (as shown by the Incompleteness Theorem), Hoare logic is incomplete.

However, we can show relative completeness of Hoare logic, i.e. relative to number theory. This means that if we assume that we have proofs for the assertions, then Hoare logic is complete. This result is known as *Cook's Theorem* (1974).

2.1 Weakest preconditions

Given $c\ \{B\}$, a command and a postcondition, a weakest precondition $wp(c, B)$ is an assertion such that

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

This definition indeed shows that:

- $wp(c, B)$ is a precondition ("$\Rightarrow$" implication):

$$\models \{wp(c, B)\}\ c\ \{B\}$$

- $wp(c, B)$ is the weakest precondition ("$\Leftarrow$" implication):

$$\models \{A\}\ c\ \{B\} \text{ then } \models A \Rightarrow wp(c, B)$$

2.2 Issues with weakest preconditions

We have defined the weakest preconditions, but before we can use them, some questions have to be answered:

1. *Existence*: Does a weakest precondition exist for any command?
2. *Uniqueness*: Is a weakest precondition for any command unique?
3. *Expressiveness*: Is **Assn** expressive enough to characterize the weakest preconditions if they do exist?
4. $\vdash \{wp(c, B)\}\ c\ \{B\}$? I.e., can we prove using Hoare logic that a weakest precondition is a precondition?

The answers to these questions are:

1. Yes. There exists a constructive proof for this.
2. Yes, up to equivalence of assertions.
3. Yes. Non-trivial proof using Gödel's β function.
4. Yes. See the proof later in this lecture.

First we use these four properties in the proof of relative completeness of Hoare logic, and then we come back to prove them.

2.3 Proof of Cook's Relative Completeness Theorem, assuming (1-4)

We assume that the derivations for **Assn** statements are given to us. Then we need to prove

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

From assumption (4) there is a theorem,

$\vdash \{wp(c, B)\}\ c\ \{B\}$

From the definition of the weakest precondition,

$\models A \Rightarrow wp(c, B)$

By assumption, we have a (free) derivation for

$\vdash A \Rightarrow wp(c, B)$

So from the consequence rule of Hoare logic, we can construct a proof tree for $\{A\}\ c\ \{B\}$:

$$\dfrac{\dfrac{(free)\ \vdots}{A \Rightarrow wp(c, B)} \qquad \dfrac{\vdots}{\{wp(c, B)\}\ c\ \{B\}}}{\{A\}\ c\ \{B\}}$$

This means that any valid assertion of the form $\{A\}\ c\ \{B\}$ can be derived in Hoare logic, given derivations for **Assn**. This concludes the proof of the relative completeness. Now we go back to the above four properties of weakest preconditions.

(1) Existence

Here we give an inductive definition of formulas $wp(c, B)$, based on the structure of **Com**.

$$\begin{array}{rcl}
wp(\textbf{skip}, B) & = & B \\
wp(x := a, B) & = & B[x \mapsto a] \\
wp(c_0; c_1, B) & = & wp(c_0, wp(c_1, B)) \\
wp(\textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1, B) & = & (b \wedge wp(c_0, B)) \vee (\neg b \wedge wp(c_1, B)) \\
wp(\textbf{while}\ b\ \textbf{do}\ c, B) & = & \bigwedge\limits_{k \geq 0} P_k \qquad \text{where: } P_0 = \textbf{true} \\
 & & \qquad\qquad\quad P_{k+1} = (b \wedge wp(c, P_k)) \vee (\neg b \wedge B)
\end{array}$$

Note: The sequence $\{\sigma \mid \sigma \models P_k\}_k$ is an ω-chain in the domain $(\mathcal{P}(\Sigma), \supseteq)$, because $P_{k+1} \Rightarrow P_k$ for all k (proof left as exercise). The join operator in this cpo is set intersection.

Exercise: prove that the expressions inductively defined above are indeed weakest preconditions.

If $W = wp(\textbf{while}\ b\ \textbf{do}\ c, B)$, one can prove that the following relations hold (proof left as exercise):

$$\begin{array}{rcl}
W \wedge \neg b & \Leftrightarrow & \neg b \wedge B \\
W \wedge b & \Leftrightarrow & b \wedge wp(c, W)
\end{array}$$

Note: The following is also a precondition for the while loop, but it is not the weakest precondition:

$$\begin{array}{rcl}
wp(\textbf{while}\ b\ \textbf{do}\ c, B) & = & \bigvee\limits_{k \geq 0} P'_k \qquad \text{where: } P'_0 = (\neg b \wedge B) \\
 & & \qquad\qquad\quad P'_{k+1} = b \wedge wp(c, P'_k)
\end{array}$$

(2) Uniqueness

Suppose there are two weakest preconditions, w_1 and w_2. Then
$\sigma \models^I \{w_1\}$ iff $\mathcal{C}[\![c]\!]\sigma \models^I \{B\}$
$\sigma \models^I \{w_2\}$ iff $\mathcal{C}[\![c]\!]\sigma \models^I \{B\}$
$\Rightarrow \quad \models (w_1 \Leftrightarrow w_2)$
Therefore weakest preconditions are unique up to equivalence of assertions.

(3) Expressiveness

There is a way to express all the weakest preconditions as assertions. The proof is farily complex and is based on Gödel's β function. We will assume the result, but skip the proof – for details see Winskel.

(4) $\vdash \{wp(c, B)\}\ c\ \{B\}$

We prove this using structural induction on command c.

- $\vdash \{wp(\textbf{skip}, B)\}\textbf{skip}\{B\}$, because we know that $wp(\textbf{skip}, B) = B$ and $\overline{\{B\}\textbf{skip}\{B\}}$ is an axiom.
- $\vdash \{wp(X := a, B)\}X := a\{B\}$, because we know that $wp(X := a, B) = B[X \mapsto a]$ and $\overline{\{B[X \mapsto a]\}c\{B\}}$ is another axiom.
- Sequencing. By Induction Hypothesis, assume $\vdash \{wp(c, D)\}\ c_0\ \{D\}$ and $\vdash \{wp(c, D)\}\ c_1\ \{D\}$ for any assertion D. Then $\vdash \{wp(c_0; c_1, B)\}c_0; c_1\{B\}$ because of the following derivation:

$$\frac{\dfrac{\text{(by I.H.)}}{\{wp(c_0, wp(c_1, B))\}c_0\{wp(c_1, B)\}} \quad \dfrac{\text{(by I.H.)}}{\{wp(c_1, B)\}c_1\{B\}}}{\{wp(c_0; c_1, B)\}c_0; c_1\{B\}}$$

- Conditionals. By Induction Hypothesis, assume $\vdash \{wp(c, D)\}\ c_0\ \{D\}$ and $\vdash \{wp(c, D)\}\ c_1\ \{D\}$. Let:

$$W = wp(\textbf{if}\, b\, \textbf{then}\, c_0\, \textbf{else}\, c_1, B) = (b \wedge wp(c_0, B))\ \vee\ (\neg b \wedge wp(c_1, B))$$

  Hence, $W \wedge b \Rightarrow wp(c_0, B)$ and $W \wedge \neg b \Rightarrow wp(c_1, B)$. Then $\vdash \{W\}\textbf{if}\, b\, \textbf{then}\, c_0\, \textbf{else}\, c_1\{B\}$ because of the following derivation:

$$\frac{\dfrac{\dfrac{\text{(for free)}}{W \wedge b \Rightarrow wp(c_0, B)} \quad \dfrac{\text{(by I.H.)}}{\{wp(c_0, B)\}c_0\{B\}}}{\{W \wedge b\}c_0\{B\}} \quad \dfrac{\dfrac{\text{(for free)}}{W \wedge \neg b \Rightarrow wp(c_1, B)} \quad \dfrac{\text{(by I.H.)}}{\{wp(c_1, B)\}c_1\{B\}}}{\{W \wedge \neg b\}c_1\{B\}}}{\{W\}\textbf{if}\, b\, \textbf{then}\, c_0\, \textbf{else}\, c_1\{B\}}$$

- While loops. By Induction Hypothesis, assume $\vdash \{wp(c, D)\}\ c\ \{D\}$ for any assertion D. Let: $W = wp(\textbf{while}\, b\, \textbf{do}\, c, B)$. We know that:

$$\begin{aligned} W \wedge \neg b &\quad\Leftrightarrow\quad \neg b \wedge B \\ W \wedge b &\quad\Leftrightarrow\quad b \wedge wp(c, W) \end{aligned}$$

  Then $\vdash \{W\}\textbf{while}\, b\, \textbf{do}\, c\{B\}$ because of the following derivation:

$$\frac{\dfrac{\dfrac{\dfrac{\text{(for free)}}{W \wedge b \Rightarrow wp(c, W)} \quad \dfrac{\text{(by I.H.)}}{\{wp(c, W)\}c\{W\}}}{\{W \wedge b\}c\{W\}}}{\{W\}while\ b\ do\ c\ \{W \wedge \neg b\}} \quad \dfrac{\text{(for free)}}{W \wedge \neg b \Rightarrow B}}{\{W\}\textbf{while}\, b\, \textbf{do}\, c\{B\}}$$