1 Relative Completeness

In the last lecture, we discussed the issue of completeness—i.e., whether it is possible to derive every valid partial correctness specification using the axioms and rules of Hoare logic. Unfortunately, if treated as a pure deductive system, Hoare logic cannot be complete. To see why, consider the following partial correctness specifications:

$$\{\mathsf{true}\}\ \mathsf{skip}\ \{P\} \qquad\qquad \{\mathsf{true}\}\ c\ \{\mathsf{false}\}$$

The first is valid if and only if the assertion P is valid while the second is valid if and only if the command c does not halt.

It turns out that the culprit is the weakening rule, which includes premises involving the validity of implications between the assertions involved:

$$\text{(weakening)} \qquad \frac{\varphi \Rightarrow \varphi' \quad \{\varphi'\}\,c\,\{\psi'\} \quad \psi' \Rightarrow \psi}{\{\varphi\}\,c\,\{\psi\}}.$$

Although we cannot have a complete proof system for first-order formulas, Hoare logic does enjoy the property stated in the following theorem:

Theorem 1.

$$\forall \varphi, \psi, c.\ \vDash \{\varphi\}\ c\ \{\psi\} \quad \textit{implies} \quad \vdash \{\varphi\}\ c\ \{\psi\}.$$

This result, due to Cook (1974), is known as the *relative completeness* of Hoare logic. It says that Hoare logic is no more incomplete than the language of assertions—i.e., if we had an oracle that could decide the validity of assertions, then we could decide the validity of partial correctness specifications.

2 Weakest Preconditions

Given a program s and a postcondition φ, the weakest property of the input state that guarantees that s halts in a state satisfying φ, if it exists, is called the *weakest precondition* of s and φ and is denoted $\mathsf{wp}\ s\ \varphi$. This says that

- $\mathsf{wp}\ s\ \varphi$ implies that s terminates in a state satisfying φ ($\mathsf{wp}\ s\ \varphi$ is a precondition of s and φ),
- if ψ is any other condition that implies that s terminates in a state satisfying φ, then $\psi \Rightarrow \mathsf{wp}\ s\ \varphi$ ($\mathsf{wp}\ s\ \varphi$ is the *weakest precondition* of s and φ).

As in the λ-calculus, juxtaposition represents function application, so wp can be viewed as a higher-order function that takes a program s and a postcondition φ and returns the weakest precondition of s and φ. The function wp can also be viewed as taking a program and returning a function that maps postconditions to preconditions. For this reason, axiomatic semantics is sometimes known as *predicate transformer semantics*.

3 Weakest Liberal Preconditions

Cook's proof of relative completeness depends on the notion of *weakest liberal preconditions*. Given a command c and a postcondition ψ the weakest liberal precondition is the weakest assertion φ such that

$$\{\varphi\}\ c\ \{\psi\}$$

is a valid triple. Here, "weakest" means that any other valid precondition implies φ. That is, φ most accurately describes input states for which c either does not terminate or ends up in a state satisfying ψ.

Formally, an assertion φ is a weakest liberal precondition of c and ψ if:

$$\forall \sigma, I.\ \sigma \vDash_I \varphi \iff (\mathcal{C}[\![c]\!]\ \sigma) \text{ undefined } \vee (\mathcal{C}[\![c]\!]\sigma) \vDash_I \psi$$

We write $wlp(c, \psi)$ for the weakest liberal precondition of command c and postcondition ψ. From left-to-right, the formula above states that $wlp(c, \psi)$ is a valid precondition: $\vDash \{\varphi\}\ c\ \{\psi\}$. The right-to-left implication says it is the weakest valid precondition: if another assertion R satisfies $\vDash \{R\}\ c\ \{\psi\}$, then R implies φ. It can be shown that weakest liberal preconditions are unique modulo equivalence.

We can calculate the weakest liberal precondition of a command as follows:

$$\begin{array}{rcl}
wlp(\mathsf{skip}, \varphi) & = & \varphi \\
wlp((x := a, \varphi) & = & \varphi[a/x] \\
wlp((c_1; c_2), \varphi) & = & wlp(c_1, wlp(c_2, \varphi)) \\
wlp(\mathsf{if}\ b\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \varphi) & = & (b \implies wlp(c_1, \varphi)) \wedge (\neg b \implies wlp(c_2, \varphi))
\end{array}$$

The definition of $wlp(\mathsf{while}\, b\, \mathsf{do}\, c, \varphi)$ is slightly more complicated—it encodes the weakest liberal precondition for each iteration of the loop. To give the intuition, first define the weakest liberal precondition for a loop that termintes in i steps as follows:

$$\begin{array}{rcl}
F_0(\varphi) & = & \mathsf{true} \\
F_{i+1}(\varphi) & = & (\neg b \implies \varphi) \wedge (b \implies wlp(c, F_i(\varphi)))
\end{array}$$

We can then express the weakest liberal precondition using an infinitary conjunction:

$$wlp(\mathsf{while}\ b\ \mathsf{do}\ c, \varphi) = \bigwedge_i F_i(\varphi)$$

See Winskel Chapter 7 for the details of how to encode the weakest liberal precondition for a while loop as an ordinary assertion.

To check that our definition is correct, we can prove (how?) that it yields a valid partial correctness specification:

Lemma 2.

$$\forall c, \psi.\ \vDash \{wlp(c, \psi)\}\ c\ \{\psi\} \quad \textit{and} \quad \forall \rho.\ \vDash \{\rho\}\ c\ \{\psi\}\ \textit{implies}\ (\rho \implies wlp(c, \psi))$$

It is not hard to prove that it also yields a provable specification:

Lemma 3.

$$\forall c, \psi.\ \vdash \{wlp(c, \psi)\}\ c\ \{\psi\}$$

Relative completeness follows by a simple argument:

Proof Sketch. Let c be a command and let P and ψ be assertions such that the partial correctness specification $\{P\}\ c\ \{\psi\}$ is valid. By Lemma 2 we have $\vDash P \implies wlp(c, \psi)$. By Lemma 3 we have $\vdash \{wlp(c, \psi)\}\ c\ \{\psi\}$. We conclude $\vdash \{P\}\ c\ \{\psi\}$ using weakening. □

References

[1] Glynn Winskel. *The Formal Semantics of Programming Languages.* MIT Press, 1993.