Lecturer: Dexter Kozen

1 Semantics of IMP Revisited

1.1 Syntax of Commands

$$c \quad ::= \quad \mathsf{skip} \ \mid\ x := a \ \mid\ c_0; c_1 \ \mid\ \mathsf{if}\ b\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2 \ \mid\ \mathsf{while}\ b\ \mathsf{do}\ c.$$

1.2 Big-Step Rules

(skip) $\quad \langle \mathsf{skip}, \sigma\rangle \Downarrow \sigma$

(assignment) $$\frac{\langle a, \sigma\rangle \Downarrow n}{\langle x := a, \sigma\rangle \Downarrow \sigma[n/x]}$$

(sequential composition) $$\frac{\langle c_0, \sigma\rangle \Downarrow \tau \quad \langle c_1, \tau\rangle \Downarrow \rho}{\langle c_0; c_1, \sigma\rangle \Downarrow \rho}$$

(conditional) $$\frac{\langle b, \sigma\rangle \Downarrow \mathsf{true} \quad \langle c_1, \sigma\rangle \Downarrow \tau}{\langle \mathsf{if}\ b\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \Downarrow \tau} \qquad \frac{\langle b, \sigma\rangle \Downarrow \mathsf{false} \quad \langle c_2, \sigma\rangle \Downarrow \tau}{\langle \mathsf{if}\ b\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \Downarrow \tau}$$

(while loop) $$\frac{\langle b, \sigma\rangle \Downarrow \mathsf{false}}{\langle \mathsf{while}\ b\ \mathsf{do}\ c, \sigma\rangle \Downarrow \sigma} \qquad \frac{\langle b, \sigma\rangle \Downarrow \mathsf{true} \quad \langle c, \sigma\rangle \Downarrow \tau \quad \langle \mathsf{while}\ b\ \mathsf{do}\ c, \tau\rangle \Downarrow \rho}{\langle \mathsf{while}\ b\ \mathsf{do}\ c, \sigma\rangle \Downarrow \rho}$$

1.3 Binary Relation Semantics

In the semantics of IMP, states $\sigma, \tau, \ldots$ are functions $\mathbf{Var} \to \mathbb{Z}$. Let $\mathbf{St}$ denote the set of all states. For each program c, the big-step rules determine a binary input/output relation on $\mathbf{St}$, namely

$$[\![c]\!] \ \stackrel{\triangle}{=}\ \{(\sigma, \tau) \mid \langle c, \sigma\rangle \Downarrow \tau\} \ \subseteq\ \mathbf{St} \times \mathbf{St}.$$

With this notation, we can express the big-step rules in terms of some basic operations on binary relations, namely *relational composition* ($\circ$) and *reflexive transitive closure* (*):

$$R \circ S \ \stackrel{\triangle}{=}\ \{(\sigma, \rho) \mid \exists \tau\ (\sigma, \tau) \in R,\ (\tau, \rho) \in S\}$$
$$R^* \ \stackrel{\triangle}{=}\ \bigcup_{n \geq 0} R^n \ =\ \{(\sigma, \tau) \mid \exists \sigma_0, \ldots, \sigma_n\ \sigma = \sigma_0,\ \tau = \sigma_n,\ \text{and}\ (\sigma_i, \sigma_{i+1}) \in R,\ 0 \leq i \leq n-1\},$$

where $R^0 \stackrel{\triangle}{=} \{(\sigma, \sigma) \mid \sigma \in \mathbf{St}\}$ and $R^{n+1} \stackrel{\triangle}{=} R \circ R^n$. The big-step rules are equivalent to the following:

(skip)	$[\![\mathsf{skip}]\!]$	$=$	$\{(\sigma, \sigma) \mid \sigma \in \mathbf{St}\}$
(assignment)	$[\![x := a]\!]$	$=$	$\{(\sigma, \sigma[n/x]) \mid \langle a, \sigma\rangle \Downarrow n\}$
(sequential composition)	$[\![c_0; c_1]\!]$	$=$	$[\![c_0]\!] \circ [\![c_1]\!]$
(conditional)	$[\![\mathsf{if}\ b\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2]\!]$	$=$	$[\![b]\!] \circ [\![c_1]\!] \ \cup\ [\![\neg b]\!] \circ [\![c_2]\!]$
(while loop)	$[\![\mathsf{while}\ b\ \mathsf{do}\ c]\!]$	$=$	$([\![b]\!] \circ [\![c]\!])^* \circ [\![\neg b]\!]$,

where in the conditional and while loop,

$$[\![b]\!] \ \stackrel{\triangle}{=}\ \{(\sigma, \sigma) \mid \langle b, \sigma\rangle \Downarrow \mathsf{true}\}$$
$$[\![\neg b]\!] \ \stackrel{\triangle}{=}\ \{(\sigma, \sigma) \mid \langle b, \sigma\rangle \Downarrow \mathsf{false}\} \ =\ [\![\mathsf{skip}]\!] - [\![b]\!].$$

In fact, this would have been a much more compact way to define them originally.

1.4 Semantics of Weakest Liberal Preconditions and Partial Correctness Assertions

We can now give a formal semantics for weakest liberal preconditions and Hoare partial correctness assertions. Let L denote the underlying logic (typically first-order logic). Write $\sigma \vDash \varphi$ if the formula φ of L is true in state σ, and write $\vDash \varphi$ if φ is true in all states. We wish to define what it means for a weakest liberal precondition assertion $\mathsf{wlp}\ c\ \psi$ to be true in a state σ, written $\sigma \vDash \mathsf{wlp}\ c\ \psi$, and for a partial correctness assertion $\{\varphi\}\,c\,\{\psi\}$ to be true, written $\vDash \{\varphi\}\,c\,\{\psi\}$.

$$\begin{aligned}
\sigma \vDash \mathsf{wlp}\ c\ \psi \quad &\overset{\triangle}{\iff} \quad \forall\tau \ \ (\sigma,\tau) \in [\![c]\!] \ \Rightarrow\ \tau \vDash \psi \\
\vDash \{\varphi\}\,c\,\{\psi\} \quad &\overset{\triangle}{\iff} \quad \forall\sigma \ \ \sigma \vDash \varphi \ \Rightarrow\ \sigma \vDash \mathsf{wlp}\ c\ \psi \\
&\iff \quad \forall\sigma,\tau \ \ \sigma \vDash \varphi \wedge (\sigma,\tau) \in [\![c]\!] \ \Rightarrow\ \tau \vDash \psi.
\end{aligned}$$

1.5 Soundness and Relative Completeness of Hoare Logic

Let us write $\vdash \{\varphi\}\,c\,\{\psi\}$ to assert that $\{\varphi\}\,c\,\{\psi\}$ is provable in Hoare logic. Then soundness and relative completeness of Hoare logic are captured in the following theorems. The relative completeness result is due to Cook.

Theorem (soundness) $\vdash \{\varphi\}\,c\,\{\psi\} \ \Rightarrow\ \vDash \{\varphi\}\,c\,\{\psi\}$.

Theorem (relative completeness) Assume that the underlying logic L is *expressive* in the sense that all weakest liberal preconditions are expressible in L; that is, for each program c and formula ψ of L, there is a formula ψ' of L such that for all σ, $\sigma \vDash \psi'$ iff $\sigma \vDash \mathsf{wlp}\ c\ \psi$. Then $\vDash \{\varphi\}\,c\,\{\psi\} \ \Rightarrow\ \vdash \{\varphi\}\,c\,\{\psi\}$, provided we are allowed to assume all true formulas of L as axioms.

Proof sketch. The proof is by structural induction on c. We will just sketch the proof for two cases, assignments and the while loop.

For an assignment $x := a$, suppose $\vDash \{\varphi\}\,x := a\,\{\psi\}$. Then $\forall\sigma \ \ \sigma \vDash \varphi \ \Rightarrow\ \sigma \vDash \mathsf{wlp}\ (x := a)\ \psi$. But $\mathsf{wlp}\ (x := a)\ \psi = \psi\{a/x\}$, so $\forall\sigma \ \ \sigma \vDash \varphi \ \Rightarrow\ \sigma \vDash \psi\{a/x\}$, therefore $\vDash \varphi \rightarrow \psi\{a/x\}$. We can thus assume $\vdash \varphi \rightarrow \psi\{a/x\}$, since we are allowed to take true formulas of L as axioms. Then $\vdash \{\psi\{a/x\}\}\,x := a\,\{\psi\}$ by the assignment rule of Hoare logic, thus $\vdash \{\varphi\}\,x := a\,\{\psi\}$ by the weakening rule of Hoare logic.

Now for the while loop. Suppose $\vDash \{\varphi\}\,\mathsf{while}\ b\ \mathsf{do}\ c\,\{\psi\}$. Then $\forall\sigma \ \ \sigma \vDash \varphi \ \Rightarrow\ \sigma \vDash \mathsf{wlp}\ (\mathsf{while}\ b\ \mathsf{do}\ c)\ \psi$. Since L is expressive, $\mathsf{wlp}\ (\mathsf{while}\ b\ \mathsf{do}\ c)\ \psi$ is equivalent to a formula ρ of L, and $\vDash \varphi \rightarrow \rho$. Since the programs

$$\mathsf{while}\ b\ \mathsf{do}\ c \qquad\qquad \mathsf{if}\ b\ \mathsf{then}\ (c; \mathsf{while}\ b\ \mathsf{do}\ c)\ \mathsf{else\ skip}$$

are semantically equivalent, we have

$$\begin{aligned}
\rho \quad &\Leftrightarrow \quad \mathsf{wlp}\ (\mathsf{while}\ b\ \mathsf{do}\ c)\ \psi \\
&\Leftrightarrow \quad \mathsf{wlp}\ (\mathsf{if}\ b\ \mathsf{then}\ (c; \mathsf{while}\ b\ \mathsf{do}\ c)\ \mathsf{else\ skip})\ \psi \\
&\Leftrightarrow \quad (b \ \Rightarrow\ \mathsf{wlp}\ c\ (\mathsf{wlp}\ (\mathsf{while}\ b\ \mathsf{do}\ c)\ \psi)) \wedge (\neg b \ \Rightarrow\ \mathsf{wlp\ skip}\ \psi) \\
&\Leftrightarrow \quad (b \ \Rightarrow\ \mathsf{wlp}\ c\ \rho) \wedge (\neg b \ \Rightarrow\ \psi),
\end{aligned}$$

thus $\vDash \rho \wedge \neg b \rightarrow \psi$ and $\vDash \rho \wedge b \rightarrow \mathsf{wlp}\ c\ \rho$. The latter says exactly that $\vDash \{\rho \wedge b\}\,c\,\{\rho\}$. By the induction hypothesis, $\vdash \{\rho \wedge b\}\,c\,\{\rho\}$, and by the fact that we may assume all true formulas of L as axioms, $\vdash \varphi \rightarrow \rho$ and $\vdash \rho \wedge \neg b \rightarrow \psi$. Then

$$\begin{aligned}
\vdash \{\rho \wedge b\}\,c\,\{\rho\} \quad &\Rightarrow \quad \vdash \{\rho\}\,\mathsf{while}\ b\ \mathsf{do}\ c\,\{\rho \wedge \neg b\} && \text{by the Hoare while rule} \\
&\Rightarrow \quad \vdash \{\varphi\}\,\mathsf{while}\ b\ \mathsf{do}\ c\,\{\psi\} && \text{by weakening.}
\end{aligned}$$

□