IMP Syntax

$\mathbb{N}$	natural numbers	$n, m, \ldots$
T	truth values	true, false
Loc	locations	$X, Y, \ldots$
Aexp	arithmetic expressions	$a, a_0, \ldots$
Bexp	boolean expressions	$b, b_0, \ldots$
Com	commands	$c, c_0, \ldots$

$a \quad ::= \quad n \mid X \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 \times a_1$

$b \quad ::= \quad \text{false} \mid a_0 \leq a_1 \mid b_0 \to b_1$

$c \quad ::= \quad \text{skip} \mid X := a \mid c_0; c_1 \mid \text{if } b \text{ then } c_0 \text{ else } c_1 \mid \text{while } b \text{ do } c$

Operational Semantics

$\Sigma = \mathsf{Loc} \to \mathbb{Z}$	states $\sigma, \tau, \ldots$
$\langle a, \sigma \rangle \to n$	evaluation of arithmetic expressions
$\langle b, \sigma \rangle \to \mathsf{T}$	evaluation of boolean expressions
$\langle c, \sigma \rangle \to \sigma'$	execution of commands

Example

$$\frac{\langle a, \sigma \rangle \to m}{\langle X := a, \sigma \rangle \to \sigma[m/X]}$$

where

$$\sigma[m/X](Y) \stackrel{\text{def}}{=} \begin{cases} m, & \text{if } Y = X \\ \sigma(Y), & \text{otherwise.} \end{cases}$$

Denotational Semantics

$\Sigma = \mathsf{Loc} \to \mathbb{Z}$ states $\sigma, \tau, \ldots$

$$\begin{array}{rcl} \mathcal{A} & : & \mathsf{Aexp} \to \Sigma \to \mathbb{Z} \\ \mathcal{B} & : & \mathsf{Bexp} \to \Sigma \to \mathsf{T} \\ \mathcal{C} & : & \mathsf{Com} \to \Sigma \to \Sigma \end{array}$$

Example

$$\mathcal{C}[\![X := a]\!] \quad = \quad \{(\sigma, \sigma[m/X]) \mid \sigma \in \Sigma,\ m = \mathcal{A}[\![a]\!]\sigma\}$$

Assertions

Intvar	integer variables $i, j, \ldots$
Aexpv	extended arithmetic expressions $a, a_0, \ldots$
Assn	extended boolean expressions $A, B, C, \ldots$

$$a \quad ::= \quad n \mid X \mid i \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 \times a_1$$

$$A \quad ::= \quad \mathsf{false} \mid a_0 \leq a_1 \mid A_0 \to A_1 \mid \forall i.A$$

$$\begin{aligned}
\neg A &\stackrel{\text{def}}{=} A \to \mathsf{false} \\
\exists i.A &\stackrel{\text{def}}{=} \neg\forall i.\neg A \\
A_0 \vee A_1 &\stackrel{\text{def}}{=} \neg A_0 \to A_1 \\
A_0 \wedge A_1 &\stackrel{\text{def}}{=} \neg(\neg A_0 \vee \neg A_1) \\
a_0 = a_1 &\stackrel{\text{def}}{=} a_0 \leq a_1 \wedge a_1 \leq a_0
\end{aligned}$$

Semantics of Assertions

interpretations I : Intvar $\to \mathbb{Z}$

$\mathcal{A}v$: Aexpv $\to$ {interpretations} $\to \Sigma \to \mathbb{Z}$

satisfaction relation $\sigma \models^I A$
state σ satisfies A under interpretation I

Example

$$\sigma \models^I \forall i.A \quad \overset{\text{def}}{\iff} \quad \sigma \models^{I[n/i]} A \text{ for all } n \in \mathbb{Z}$$

Partial Correctness Assertions

$$\{A\}\, c\, \{B\}$$

If A is true of the start state, and if c halts, then B is true of the halting state

$$\sigma \models^I \{A\}\, c\, \{B\} \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad (\sigma \models^I A \Rightarrow \mathcal{C}\,[\![c]\!]\,\sigma \models^I B)$$

$$\models \{A\}\, c\, \{B\} \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \sigma \models^I \{A\}\, c\, \{B\} \text{ for all } I \text{ and } \sigma$$

$\perp$ included to represent non-halting computation

$\Sigma_\perp \stackrel{\text{def}}{=} \Sigma \cup \perp$

$\mathcal{C}\,[\![c]\!]\,\sigma = \perp$ if c does not halt

$\perp \models^I A$ for all A

Hoare Rules

$$\{A\}\ \mathsf{skip}\ \{B\}$$

$$\{B[a/X]\}\ X := a\ \{B\}$$

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

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

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

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

$$\frac{A \to A',\ \{A'\}\ c\ \{B'\},\ B' \to B}{\{A\}\ c\ \{B\}}$$

$\vdash \{A\}\ c\ \{B\}$ if $\{A\}\ c\ \{B\}$ follows from these rules

Soundness: if $\vdash \{A\}\ c\ \{B\}$ then $\models \{A\}\ c\ \{B\}$

Weakest Preconditions

$$wp^I\,[\![c, B]\!] \quad \stackrel{\text{def}}{=} \quad \{\sigma \in \Sigma_\perp \mid \mathcal{C}\,[\![c]\!]\,\sigma \models^I B\}$$

Expressiveness of the Assertion Language

There is an assertion $w\,[\![c, B]\!]$ such that for any I,

$$w\,[\![c, B]\!]^I \quad \stackrel{\text{def}}{=} \quad wp^I\,[\![c, B]\!]$$

Examples

$$\begin{aligned} w\,[\![X := a, B]\!] &= B[a/X] \\ w\,[\![c; c', B]\!] &= w\,[\![c, w\,[\![c', B]\!]\,]\!] \end{aligned}$$

Lemma

$\models \{w\,[\![c, B]\!]\}\; c\; \{B\}$

if $\models \{A\}\; c\; \{B\}$ then $\models A \to w\,[\![c, B]\!]$

Relative Completeness (Cook 1974)

Hoare logic is *relatively complete*: if $\models \{A\}\, c\, \{B\}$ then $\vdash \{A\}\, c\, \{B\}$.

"Relative" means relative to number theory—you get to assume true statements of number theory for free—use them in the weakening rule

$$\frac{A \to A',\ \{A'\}\, c\, \{B'\},\ B' \to B}{\{A\}\, c\, \{B\}}$$

Proof

Show $\vdash \{w\,[\![c, B]\!]\}\, c\, \{B\}$ by induction

$\models \{A\}\, c\, \{B\}$ $\Rightarrow$ $\vdash \{w\,[\![c, B]\!]\}\, c\, \{B\}$ and $\models A \to w\,[\![c, B]\!]$

$\Rightarrow$ $\vdash \{A\}\, c\, \{B\}$ by weakening

Proving Expressiveness

$$
\begin{array}{rcl}
w\,[\![\mathsf{skip}, B]\!] & = & B \\
w\,[\![X := a, B]\!] & = & B[a/X] \\
w\,[\![c; c', B]\!] & = & w\,[\![c, w\,[\![c', B]\!]\,]\!] \\
w\,[\![\mathsf{if}\ b\ \mathsf{then}\ c\ \mathsf{else}\ c', B]\!] & = & (b \wedge w\,[\![c, B]\!]\,) \vee (\neg b \wedge w\,[\![c', B]\!]\,)
\end{array}
$$

$w\,[\![\mathsf{while}\ b\ \mathsf{do}\ c, B]\!]$ is the hard one—uses coding power of number theory

Gödel's β-function

Allows the coding of arbitrary-length sequences of integers into single integers—based on

Chinese Remainder Theorem

If $m_1, \ldots, m_k$ are relatively prime and $n = m_1 \cdots m_k$, then the rings $\mathbb{Z}_n$ and $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ are isomorphic under the map $i \mapsto (i \bmod m_1, \ldots, i \bmod m_k)$.

For details, see Winskel ch. 7