Soundness

Meanings for types:

τ ::= int | $bool$

θ ::= $intloc$ | τexp | $comm$

$\mathcal{T}$: $\theta \to$ a domain

$\mathcal{T}[\![int]\!]$ = Int

$\mathcal{T}[\![bool]\!]$ = Bool

$\mathcal{T}[\![intloc]\!]$ = Loc

$\mathcal{T}[\![\tau exp]\!]$ = Store $\to [\![\tau]\!]$

$\mathcal{T}[\![comm]\!]$ = $\text{Store}_\perp \to \text{Store}_\perp$

Soundness Theorem:

For all well-typed phrases P:θ, $\mathcal{S}[\![P{:}\theta]\!] \in \mathcal{T}[\![\theta]\!]$

(where $\mathcal{S}$ is one of $\mathcal{N}$, $\mathcal{L}$, $\mathcal{E}$, or $\mathcal{C}$)

Proof: by structural induction over typing rules

Natural semantics for IMP, part 1

For `Numeral`:

$$\langle n{:}int, s\rangle \Rightarrow n$$

For `Location`:

$$\langle loc_i{:}intloc, s\rangle \Rightarrow loc_i$$

For `Expression`:

$$\frac{\langle N{:}int, s\rangle \Rightarrow n}{\langle N{:}intexp, s\rangle \Rightarrow n} \qquad \frac{\langle L{:}intloc, s\rangle \Rightarrow loc_i}{\langle @L{:}intexp, s\rangle \Rightarrow \text{lookup}(loc_i, s)}$$

$$\frac{\langle E_1{:}intexp, s\rangle \Rightarrow n_1 \qquad \langle E_2{:}intexp, s\rangle \Rightarrow n_2}{\langle E_1 + E_2{:}intexp, s\rangle \Rightarrow \text{plus}(n_1, n_2)}$$

$$\frac{\langle E{:}boolexp, s\rangle \Rightarrow b}{\langle \text{not } E{:}boolexp, s\rangle \Rightarrow \text{not}(b)}$$

$$\frac{\langle E_1{:}\tau exp, s\rangle \Rightarrow n_1 \qquad \langle E_2{:}\tau exp, s\rangle \Rightarrow n_2}{\langle E_1 = E_2{:}boolexp, s\rangle \Rightarrow \text{equal}\tau(n_1, n_2)} \text{ for } \tau \in \{int, bool\}$$

Natural semantics for IMP, part 2

For `Command`:

$$\frac{\langle L{:}intloc, s\rangle \Rightarrow loc_i \qquad \langle E{:}intexp, s\rangle \Rightarrow n}{\langle L := E{:}comm, s\rangle \Rightarrow \text{update}\,(loc_i, n, s)}$$

$$\frac{\langle C_1{:}comm, s\rangle \Rightarrow s' \qquad \langle C_2{:}comm, s'\rangle \Rightarrow s''}{\langle C_1;C_2{:}comm, s\rangle \Rightarrow s''}$$

$$\frac{\langle E{:}boolexp, s\rangle \Rightarrow \text{true} \qquad \langle C_1{:}comm, s\rangle \Rightarrow s'}{\langle \text{if } E \text{ then } C_1 \text{ else } C_2{:}comm, s\rangle \Rightarrow s'}$$

$$\frac{\langle E{:}boolexp, s\rangle \Rightarrow \text{false} \qquad \langle C_2{:}comm, s\rangle \Rightarrow s'}{\langle \text{if } E \text{ then } C_1 \text{ else } C_2{:}comm, s\rangle \Rightarrow s'}$$

$$\frac{\begin{array}{c}\langle E{:}boolexp, s\rangle \Rightarrow \text{true} \qquad \langle C{:}comm, s\rangle \Rightarrow s' \\ \langle \text{while } E \text{ do } C{:}comm, s'\rangle \Rightarrow s''\end{array}}{\langle \text{while } E \text{ do } C{:}comm, s\rangle \Rightarrow s''}$$

$$\frac{\langle E{:}boolexp, s\rangle \Rightarrow \text{false}}{\langle \text{while } E \text{ do } C{:}comm, s\rangle \Rightarrow s}$$

$$\langle \text{skip}{:}comm, s\rangle \Rightarrow s$$

Partial transition semantics for IMP

For `Numeral`: $\langle n{:}int, s\rangle \to n$

For `Location`: $\langle loc_i{:}intloc, s\rangle \to loc_i$

For `Expression`:

$$\frac{\langle N{:}int, s\rangle \to n}{\langle N{:}intexp, s\rangle \to n} \qquad \frac{\langle L{:}intloc, s\rangle \to loc_i}{\langle @L{:}intexp, s\rangle \to \text{lookup}\,(loc_i, s)}$$

$$\frac{\langle E_1{:}intexp, s\rangle \to \langle E_1'{:}intexp, s\rangle}{\langle E_1 + E_2{:}intexp, s\rangle \to \langle E_1' + E_2{:}intexp, s\rangle}$$

$$\frac{\langle E_1{:}intexp, s\rangle \to n_1}{\langle E_1 + E_2{:}intexp, s\rangle \to \langle n_1 + E_2{:}intexp, s\rangle}$$

$$\frac{\langle E_2{:}intexp, s\rangle \to \langle E_2'{:}intexp, s\rangle}{\langle n_1 + E_2{:}intexp, s\rangle \to \langle n_1 + E_2'{:}intexp, s\rangle}$$

$$\frac{\langle E_2{:}intexp, s\rangle \to n_2}{\langle n_1 + E_2{:}intexp, s\rangle \to \langle n_1 + n_2{:}intexp, s\rangle}$$

$$\langle n_1 + n_2{:}intexp, s\rangle \to \text{plus}\,(n_1, n_2)$$

$(E_1 = E_2{:}boolexp$ is similar$)$

$$\frac{\langle E{:}boolexp, s\rangle \to \langle E'{:}boolexp, s\rangle}{\langle \text{not } E{:}boolexp, s\rangle \to \langle \text{not } E'{:}boolexp, s\rangle}$$

$$\frac{\langle E{:}boolexp, s\rangle \to b}{\langle \text{not } E{:}boolexp, s\rangle \to \langle \text{not } b{:}boolexp, s\rangle}$$

$$\langle \text{not } b{:}boolexp, s\rangle \to \text{not}\,(b)$$

Axiomatic semantics for IMP commands

For `Command`:

$$\{A\,[E/@L]\}\ L := E\ \{A\} \qquad \frac{\{A\}\ C_1\ \{B\} \qquad \{B\}\ C_2\ \{C\}}{\{A\}\ C_1;\ C_2\ \{C\}}$$

$$\frac{\{A \wedge E\}\ C_1\ \{B_1\} \qquad \{A \wedge \neg E\}\ C_2\ \{B_2\}}{\{A\}\ \text{if } E \text{ then } C_1 \text{ else } C_2\ \{B_1 \vee B_2\}}$$

$$\frac{\{A \wedge E\}\ C\ \{A\}}{\{A\}\ \text{while } E \text{ do } C\ \{A \wedge \neg E\}}$$

General consequence rule:

$$\frac{A \Rightarrow A' \qquad \{A'\}\ C\ \{B'\} \qquad B' \Rightarrow B}{\{A\}\ C\ \{B\}}$$