Syntax of Assertions

Intvar: a set of variables

Aexpv $\supseteq$ Aexp: arithmetic expressions with variables.

$$a ::= n \mid X \mid i \mid a_1 \; aop \; a_2$$

where $n \in N$, $X \in Loc$ and $i \in Intvar$.

Assn $\supseteq$ Bexp: assertions.

$$\begin{array}{rcl} A & ::= & true \mid false \mid a_1 \; rop \; a_2 \mid A_1 \; bop \; A_2 \mid \neg A \\ & \mid & \forall i.\ A \mid \exists i.\ A \end{array}$$

Interpretation $I : Intvar \to N$
Av: $Aexpv \to (Intvar \to N) \to \Sigma \to N$

$$\begin{array}{rcl} Av[\![n]\!] \; I \; \sigma & = & n \\ Av[\![X]\!] \; I \; \sigma & = & \sigma(X) \\ Av[\![i]\!] \; I \; \sigma & = & I(i) \\ Av[\![a_1 \; aop \; a_2]\!] \; I \; \sigma & = & (Av[\![a_1]\!] \; I \; \sigma)[\![aop]\!] \\ & & (Av[\![a_2]\!] \; I \; \sigma) \end{array}$$

Semantics of Assertions

$$(I[n/i])(j) = \begin{cases} n & \text{if } i = j \\ I(j) & \text{otherwise} \end{cases}$$

$[\![.]\!] : Assn \to (Intvar \to N) \to \Sigma \to T$

$$\begin{array}{rcl}
[\![true]\!]I\sigma & = & true \\
[\![false]\!]I\sigma & = & false \\
[\![a_1 \; rop \; a_2]\!]I\sigma & = & (Av[\![a_1]\!]I\sigma)[\![rop]\!](Av[\![a_2]\!]I\sigma) \\
[\![A_1 \; bop \; A_2]\!]I\sigma & = & ([\![A_1]\!]I\sigma)[\![bop]\!]([\![A_2]\!]I\sigma) \\
[\![\forall i.A]\!]I\sigma & = & \begin{cases} true & \text{if } [\![A]\!](I[n/i])\sigma = true \\ & \text{for all } n \in N \\ false & \text{otherwise} \end{cases} \\
[\![\exists i.A]\!]I\sigma & = & \begin{cases} true & \text{if } [\![A]\!](I[n/i])\sigma = true \\ & \text{for some } n \in N \\ false & \text{otherwise} \end{cases}
\end{array}$$

Validity of Assertions: $\sigma \models^I A$

$$\begin{aligned}
\sigma \models^I A \quad &\Leftrightarrow \quad [\![A]\!] I\sigma = true \\
\models^I A \quad &\Leftrightarrow \quad \text{for all } \sigma : \sigma \models^I A \\
\models A \quad &\Leftrightarrow \quad \text{for all } I : \quad \models^I A
\end{aligned}$$

Validity of Hoare-Triples: $\sigma \models^I \{A\}c\{B\}$

$$\sigma \models^I \{A\}c\{B\} \quad \Leftrightarrow \quad (\sigma \models^I A \ \Rightarrow \ C[\![c]\!]\sigma \models^I B)$$

Convention:

- $\perp$ is a new state representing "nontermination"
- if $C[\![c]\!]\sigma$ is undefined we write $C[\![c]\!]\sigma = \perp$
- $\perp \models^I B$ for all I and B

$$\models \{A\}c\{B\} \ \Leftrightarrow \ \text{for all } \sigma \text{ and } I : \sigma \models^I \{A\}c\{B\}$$