CvP - Cheat sheet

Hoare triples

A Hoare triple is an assertion

$$\{P\}\ S\ \{Q\}$$

with the following meaning: For every terminating execution of statement S from state σ to state σ', we have that $\sigma \models P$ implies $\sigma' \models Q$.

Weakest preconditions

$$\begin{aligned}
wp(x := E, Q) &= Q[E/x] \\
wp(S_1 S_2, Q) &= wp(S_1, wp(S_2, Q)) \\
wp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, Q) &= (B \wedge wp(S_1, Q)) \vee (\neg B \wedge wp(S_2, Q))
\end{aligned}$$

Hoare logic axioms

The axiom of assignment:

$$\{Q[E/x]\}\ x := E;\ \{Q\}$$

The rule of consequence:

$$\frac{P' \implies P \quad Q \implies Q' \quad \{P\}\ S\ \{Q\}}{\{P'\}\ S\ \{Q'\}}$$

The rule of sequences/composition:

$$\frac{\{P\}\ S_1\ \{Q\} \quad \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1 S_2\ \{R\}}$$

The rule of conditionals:

$$\frac{\{B \wedge P\}\ S_1\ \{Q\} \quad \{\neg B \wedge P\}\ S_2\ \{Q\}}{\{P\}\ \textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}\ \{Q\}}$$

The rule of while loops:

$$\frac{\{B \wedge I\}\ S\ \{I\}}{\{I\}\ \textbf{while } B \textbf{ do } S_1 \textbf{ od}\ \{\neg B \wedge I\}}$$

Lambda terms

$$\begin{aligned}\langle var\rangle &\to v \mid \langle var\rangle'\\ \langle term\rangle &\to \langle var\rangle \mid (\langle term\rangle\langle term\rangle) \mid (\lambda\langle var\rangle.\langle term\rangle)\end{aligned}$$

Application is left-associative and abstractions can be contracted:

$$\begin{aligned}FM_1\cdots M_n &= ((\cdots((FM_1)M_2)\cdots)M_n)\\ \lambda x_1\cdots x_n.M &= (\lambda x_1.(\cdots(\lambda x_n.M)\cdots))\end{aligned}$$

Free variables

$$\begin{aligned}\text{free}(x) &= \{x\}\\ \text{free}(M_1M_2) &= \text{free}(M_1)\cup\text{free}(M_2)\\ \text{free}(\lambda x.M) &= \text{free}(M)\setminus\{x\}\end{aligned}$$

Substitution

$$\begin{aligned}x[N/x] &= N\\ y[N/x] &= y, \quad \text{if } x\neq y\\ (M_1M_2)[N/x] &= (M_1[N/x]M_2[N/x])\\ (\lambda x.M)[N/x] &= \lambda x.M\\ (\lambda y.M)[N/x] &= \lambda x.(M[N/x]), \quad \text{if } x\neq y \text{ and } y\notin\text{free}(N)\end{aligned}$$

Conversions and reductions

α-conversion:

$$\frac{y\notin\text{free}(M)}{\lambda x.M \leftrightarrow \lambda y.(M[y/x])}$$

β-reduction:

$$(\lambda x.M)N \to M[N/x]$$

η-conversion:

$$\frac{x\notin\text{free}(F)}{\lambda x.(Fx)\leftrightarrow F}$$

Conversion $\to$ on lambda terms is reflexive ($M\to M$), transitive ($M_1\to M_2$ and $M_2\to M_3$ implies $M_1\to M_3$), and closed under application and abstraction:

$$\frac{M_1\to M_1'}{(M_1M_2)\to(M_1'M_2)} \qquad \frac{M_2\to M_2'}{(M_1M_2)\to(M_1M_2')} \qquad \frac{M\to M'}{\lambda x.M\to\lambda x.M'}$$

A λ-term is in **beta normal form**, if no β-reduction is possible.