Hoare's Proof System

(draft, May 4, 2001)

1 Hoare Triples

A Hoare triple is of the form $\{P\}s\{Q\}$ where P and Q are predicates and s is a statement. P is often called the precondition and Q the postcondition. Such a Hoare triple should be interpreted as "if P holds before the execution of s and the execution of s terminates, then Q holds afterwards." This is also known as partial correctness[1]. Obviously, based on this interpretation not every Hoare triple is valid. For example,

$$\{\mathit{true}\}v = 0;\{v = 0\}$$

is valid, but

$$\{\mathit{true}\}v = 0;\{v = 1\}$$

is not valid. Note that

$$\{\mathit{true}\}\texttt{while}\,(\mathit{true})v = v + 1;\{\mathit{false}\}$$

is valid because the statement $\texttt{while}\,(\mathit{true})v = v + 1;$ never terminates.

2 The Proof System

To conclude which Hoare triples are valid we introduce a proof system. This proof system consists of one axiom and four rules. A rule consists of a number of premises (the Hoare triples and predicates above the line) and a conclusion (the Hoare below the line). Such a rule should be interpreted as "if all premises are valid then the conclusion is valid". The proof system consists of the following axiom and rules.

1. $\{P[e/v]\}v = e;\{P\}$
2. $\dfrac{\{P\}s_1\{Q\} \quad \{Q\}s_2\{R\}}{\{P\}s_1 s_2\{R\}}$
3. $\dfrac{\{P \wedge b\}s_1\{Q\} \quad \{P \wedge \neg b\}s_2\{Q\}}{\{P\}\texttt{if}\,(b)s_1\,\texttt{else}\,s_2\{Q\}}$
4. $\dfrac{\{I \wedge b\}s\{I\}}{\{I\}\texttt{while}\,(b)s\{I \wedge \neg b\}}$
5. $\dfrac{P_1 \rightarrow P_2 \quad \{P_2\}s\{Q_2\} \quad Q_2 \rightarrow Q_1}{\{P_1\}s\{Q_1\}}$

The validity of

$$\{\mathit{true}\}v = 0;\{v = 0\}$$

can be concluded from the axiom 1 where $e = 0$ and $P = (v = 0)$. The validity of

$$\{\mathit{true}\}\texttt{while}\,(\mathit{true})v = v + 1;\{\mathit{false}\}$$

[1] In contrast, the triple $[P]s[Q]$ is interpreted as "if P holds before the execution of s, then the execution of s terminates and Q holds afterwards." This is known as total correctness.

can be drived from axiom 1 and rule 4 as follows.

$$\frac{\{true \wedge true\} v = v + 1; \{true\}}{\{true\}\texttt{while}\,(true) v = v + 1; \{true \wedge \neg true\}}$$

3 Examples