Verification/Construction Rules

Note Title 03/10/2006

- Pre- and postconditions, triples.
- Assignment axiom.
- Sequential Composition
- Conditionals
- Loops

Hoare triple

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

means if statement S is executed beginning in a state satisfying (*precondition*) P, on termination of S the state will satisfy (*postcondition*) Q.

Note: a Hoare triple expresses *conditional* ("partial") *correctness* of S with respect to precondition P and postcondition Q. "Conditional" means "assuming termination".

Skip

$$\{P\}\ \text{skip}\ \{Q\} \quad = \quad [P \Rightarrow Q]$$

verification condition

Assignment Axiom

$$\{\, Q[xs := es] \,\}\ xs := es\ \{Q\}$$

Sequential Composition

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

if $S = S_1 ; S_2$

and, for some intermediate condition R,

$\{P\}\ S_1\ \{R\}$ and $\{R\}\ S_2\ \{Q\}$.

Conditional Statements

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

if $S = \textbf{if}\ b_1 \to S_1 \ \square\ b_2 \to S_2\ \textbf{fi}$

and $[P \Rightarrow b_1 \vee b_2]$

$\{P \wedge b_1\}\ S_1\ \{Q\}$

$\{P \wedge b_2\}\ S_2\ \{Q\}$.

(Note: rule is extended to more than two branches in the obvious way.)

Iteration

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

if $S = \textbf{do}\ b \to T\ \textbf{od}$

$[P \wedge \neg b \Rightarrow Q]$

$\{P \wedge b\}\ T\ \{P\}$

Note: rule expresses conditional correctness only.

Termination of Loops

Introduce a "bound function" bf. This is an integer-valued function of the program variables.

Termination of **do** $b \to T$ **od** is guaranteed if,

for some P, P is an invariant of the loop body

(i.e. $\{P \wedge b\}\ T\ \{P\}$)

$$\{P \wedge b \wedge bf = C\}\ T\ \{0 \leqslant bf < C \ \vee\ \neg b\}$$

initialisation of the loop guarantees $0 \leqslant b$.