Verification/Construction Rules

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

\[\{P\} S \{Q\}\]

Hoare triple

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 \} = [ P \Rightarrow Q ]

verification condition

Assignment Axiom

\{ Q[xs := es] \} \; xs := es \; \{ Q \}

Sequential Composition

\{ P \} S \{ Q \}

\text{if} \quad S = S_1 \; ; \; S_2

\text{and, for some intermediate condition} \; R,

\{ P \} S_1 \{ R \} \; \text{and} \; \{ R \} S_2 \{ Q \} .
Conditional Statements

\( \{ P \} S \{ Q \} \)

\( \text{if } S = \text{ if } b_1 \rightarrow S_1 \lor b_2 \rightarrow S_2 \text{ fi} \)

and \( [ P \Rightarrow b_1 \lor b_2 ] \)

\( \{ P \land b_1 \} S_1 \{ Q \} \)

\( \{ P \land b_2 \} S_2 \{ Q \} \)

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

Iteration

\( \{ P \} S \{ Q \} \)

\( \text{if } S = \text{ do } b \rightarrow T \text{ od} \)

\( [ P \land \neg b \Rightarrow Q ] \)

\( \{ P \land b \} T \{ P \} \)

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 $\text{do } b \rightarrow T \text{ od}$ is guaranteed if,

for some $P$, $P$ is an invariant of the loop body (i.e. $\{P \land b\} T \{P\}$)

$\{P \land b \land bf=C\} T \{0 \leq bf < C \lor \neg b\}$

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