Floyd – Hoare logic (deterministic sequential programs)

The Assignment Axiom

$$\vdash \{P[E/V]\}\ V{:=}E\ \{P\}$$

V – any variable, *E* – any expression, *P* – any statement, *P*[*E*/*V*] – result of substituting *E* for all occurrences of the variables V in the statement *P*

The derived Assignment Rule

$$\frac{\vdash P \Rightarrow Q[E/V]}{\vdash \{P\}\ V{:=}E\ \{Q\}}$$

Precondition strengthening

$$\frac{\vdash P \Rightarrow P', \qquad \vdash \{P'\}\ C\ \{Q\}}{\vdash \{P\}\ C\ \{Q\}}$$

Postcondition weakening

$$\frac{\vdash \{P\}\ C\ \{Q'\} \qquad \vdash Q' \Rightarrow Q,}{\vdash \{P\}\ C\ \{Q\}}$$

Specification conjunction

$$\frac{\vdash \{P_1\}\ C\ \{Q_1\}, \qquad \vdash \{P_2\}\ C\ \{Q_2\},}{\vdash \{P_1 \wedge P_2\}\ C\ \{Q_2 \wedge Q_2\}}$$

Specification disjunction

$$\frac{\vdash \{P_1\}\ C\ \{Q_1\}, \qquad \vdash \{P_2\}\ C\ \{Q_2\},}{\vdash \{P_1 \vee P_2\}\ C\ \{Q_2 \vee Q_2\}}$$

The sequencing rule

$$\frac{\vdash \{P\}\ C_1\ \{R\}, \qquad \vdash \{R\}\ C_2\ \{Q\},}{\vdash \{P\}\ C_1;\ C_2\ \{Q\}}$$

The derived sequencing rule

$$\frac{\begin{array}{ll} & \vdash P \Rightarrow P_1 \\ \vdash \{P_1\}\ C_1\ \{Q_1\}, & \vdash Q_1 \Rightarrow P_2 \\ \vdash \{P_2\}\ C_2\ \{Q_2\}, & \vdash Q_2 \Rightarrow P_3 \\ \quad . & \quad . \\ \quad . & \quad . \\ \vdash \{P_n\}\ C_n\ \{Q_n\}, & \vdash Q_n \Rightarrow Q \end{array}}{\vdash \{P\}\ C_1;\ \ldots;\ C_n\{Q\},}$$

The derived `SKIP` rule

$$\frac{\vdash P \Rightarrow Q}{\vdash \{P\}\ \texttt{SKIP}\ \{Q\}}$$

The block rule

$$\frac{\vdash \{P\}\ C\ \{Q\}}{\vdash \{P\}\ \texttt{BEGIN VAR}\ V_1;\ \ldots\ ;V_n\ ;\ C\ \texttt{END}\ \{Q\}}$$

where none of the variables $V_1;\ \ldots\ ;V_n$ occur in *P* or *Q*

The derived block rule

$$\frac{\begin{array}{ll} & \vdash P \Rightarrow P_1 \\ \vdash \{P_1\}\ C_1\ \{Q_1\}, & \vdash Q_1 \Rightarrow P_2 \\ \vdash \{P_2\}\ C_2\ \{Q_2\}, & \vdash Q_2 \Rightarrow P_3 \\ . & . \\ \vdash \{P_n\}\ C_n\ \{Q_n\}, & \vdash Q_n \Rightarrow Q \end{array}}{\vdash \{P\}\ \texttt{BEGIN VAR}\ V_1; \ldots ;\texttt{VAR}\ V_n; C_1; \ldots ; C_n\ \texttt{END}\ \{Q\}}$$

where none of the variables $V_1; \ldots ;V_n$ occur in P or Q

The conditional (IF) rules

$$\frac{\vdash \{P \wedge S\}\ C\ \{Q\} \qquad \vdash P \wedge \neg S \Rightarrow Q}{\vdash \{P\}\ \mathbf{IF}\ S\ \mathbf{THEN}\ C\ \{Q\}}$$

$$\frac{\vdash \{P \wedge S\}\ C_1\ \{Q\}, \qquad \vdash \{P \wedge \neg S\}\ C_2\ \{Q\}}{\vdash \{P\}\ \mathbf{IF}\ S\ \mathbf{THEN}\ C_1\ \mathbf{ELSE}\ C_2 \{Q\}}$$

The (simple) WHILE -rule

$$\frac{\vdash \{R \wedge S\}\ C\ \{R\}}{\vdash \{R\}\ \mathbf{WHILE}\ S\ \mathbf{DO}\ C\{ R \wedge \neg S \}}$$

The derived WHILE rule

$$\frac{\vdash P \Rightarrow R \qquad \vdash \{R \wedge S\}\ C\ \{R\} \qquad \vdash R \wedge \neg S \Rightarrow Q}{\vdash \{P\}\ \mathbf{WHILE}\ S\ \mathbf{DO}\ C\ \{Q\}}$$

The (simple) FOR -rule

$$\frac{\vdash \{P \wedge (E_1 \leq V) \wedge (V \leq E_2)\}\ C\ \{P[V+1/V]\}}{\vdash \{P[E_1 / V]\} \wedge (E_1 \leq E_2)\}\ \mathbf{FOR}\ V := E_1\ \mathbf{UNTIL}\ E_2\ \mathbf{DO}\ C\ \{P[E_2 + 1/ V]\}}$$

The FOR -axiom

$$\vdash \{P \wedge (E_2 < E_1)\ \mathbf{FOR}\ V := E_1\ \mathbf{UNTIL}\ E_2\ \mathbf{DO}\ C\ \{P\}$$

The extended FOR –rule (annotated case)

$$\frac{\vdash P \Rightarrow R[E_1/V] \qquad \vdash R[E_2+1/V] \Rightarrow Q \qquad \vdash P \wedge (E_2 < E_1) \Rightarrow Q \qquad \vdash \{R \wedge (E_1 \leq V) \wedge (V \leq E_2)\}\ C\ \{R[V+1/V]\}}{\vdash \{P\}\ \mathbf{FOR}\ V := E_1\ \mathbf{UNTIL}\ E_2\ \mathbf{DO}\ \{R\} C\ \{Q\}}$$

The REPEAT rule (with derivation)

$$\frac{\dfrac{\vdash \{P\}\ C\ \{R\} \qquad \dfrac{\vdash R \Rightarrow inv \qquad \vdash \{inv \wedge \neg S\}\ C\ \{inv\} \qquad \vdash inv \wedge S \Rightarrow Q}{\vdash \{R\}\ \mathbf{WHILE}\ \neg S\ \mathbf{DO}\ C\ \{Q\}}}{\vdash \{P\}\ C;\ \mathbf{WHILE}\ \neg S\ \mathbf{DO}\ C\ \{Q\}}}{\vdash \{P\}\ \mathbf{REPEAT}\ C\ \mathbf{UNTIL}\ S\ \{Q\}}$$

The array axioms

$$\vdash A\{ E_1 \leftarrow E_2\}\ (E_1) = E_2$$

$$E_1 \neq E_3 \ \Rightarrow\ \vdash A\{ E_1 \leftarrow E_2\}\ (E_3) = \mathrm{A}(E_3)$$

The array assignment axiom

$$\vdash \{P[A\{ E_1 \leftarrow E_2\}/A]\}\ A(E_1) := E_2\ \ \{P\}$$

$A\{ E_1 \leftarrow E_2\}$- array identical to A , exept that $A(E_1) = E_2\}$

The array assignment rule

$$\frac{\vdash\ P \Rightarrow \{Q[A\{ E_1 \leftarrow E_2\}/A]\}}{\vdash \{P\}\ \ A(E_1) := E_2\ \ \{Q\}}$$

$A\{ E_1 \leftarrow E_2\}$- array identical to A , exept that $A(E_1) = E_2\}$

Non-deterministic sequential programs

Non-deterministic choice

$$\frac{\vdash \forall i \in \{1,\ldots,n\}: \{P\}\ S_i\ \{Q\},}{\vdash \{P\}\ \mathbf{if}\ \Box^{n}_{i=1} S_i\ \mathbf{fi}\ \{Q\}}$$

Non-deterministic if

$$\frac{\vdash \forall i \in \{1,\ldots,n\}: \{P \wedge b_i\}\ S_i\ \{Q\}}{\vdash\ \{P\}\ \text{if}\ \Box^{n}_{i=1} b_i \rightarrow S_i\ \text{fi}\ \{Q\}}$$

Non-deterministic *do*-cycle with explicit *exit*-condition

$$\frac{\vdash\ \{I\}\ S_B\ \{I\}, \qquad \vdash \{I\} S_E \{Q\}}{\vdash \{I\}\mathbf{do}\ S_B \,\Box\, S_E;\ \text{exit}\ \mathbf{od}\ \{Q\}}$$

I- invariant

Non-deterministic do-cycle

$$\frac{\vdash\ P \Rightarrow I \qquad \vdash \forall i=1,n: \{I \wedge b_i\}\ S_i\ \{I\} \qquad \vdash\ (I \wedge_{i=1,n} \neg b_i) \Rightarrow Q}{\vdash\ \{P\}\text{do}\ \{I\}\ *\ [\Box^{n}_{i=1} b_i \rightarrow S_i\ ]\ \{Q\}}$$

I -invariant

Paralle programs with shared variables

SVL parallel composition

$$\frac{A_1 \vdash \{P_1\}\ S_1\ \{Q_1\} \quad A_2 \vdash \{P_2\}\ S_2\ \{Q_2\} \quad \vdash P \Rightarrow P_1 \wedge P_2 \quad \vdash Q_1 \wedge Q_2 \Rightarrow Q \quad IFPO(S_1 \| S_2)}{\vdash \{P\}[\{P_1\}\ S_1\ \{Q_1\} \parallel \{P_2\}\ S_2\ \{Q_2\}]\ \{Q\}}$$

Interference free proof outline (*IFPO*)

Let $S_1 \parallel S_2$.
For each pair of annotated assignments $\{P_1\}\ V_1{:=}E_1\ \{Q_1\}$ and $\{P_1\}\ V_2{:=}E_2\ \{Q_2\}$ where $\{P_1\}\ V_1{:=}E_1\ \{Q_1\} \in \mathrm{A}(S_1)$ and $\{P_2\}\ V_2{:=}E_2\ \{Q_2\} \in \mathrm{A}(S_2)$, interference test consists of 4 proof obligations (where A(S) denotes annotated program S):

1. **S_1 does not violate the local precondition P_2 of S_2:**
$$\{P_1 \wedge P_2\}\ V_1 := E_1\ \{P_2\}$$
2. **S_1 does not violate the local postcondition Q_2 of S_2:**
$$\{P_1 \wedge Q_2\}\ V_1 := E_1\ \{Q_2\}$$
3. **S_2 does not violate the local precondition P_1 of S_1:**
$$\{P_2 \wedge P_1\}\ V_1 := E_1\ \{P_1\}$$
4. **S_2 does not violate the local postcondition Q_1 of S_1:**
$$\{P_2 \wedge Q_1\}\ V_1 := E_1\ \{Q_1\}$$

Parallel programs with message passing

DML parallel composition

$$\frac{A_1 \mid\!- \{P_1\}S_1\{Q_1\} \quad A_2 \mid\!- \{P_2\}\, S_2\, \{Q_2\} \quad P \Rightarrow P_1 \wedge P_2 \quad Q_1 \wedge Q_2 \Rightarrow Q \quad Coop(A_1\, A_2)}{\mid\!- \{P\}[\{P_1\}\, S_1\, \{Q_1\} \parallel \{P_2\}S_2\, \{Q_2\}]\{Q\}}$$

DML non-deterministic choice

$$\frac{\forall i = 1, l:\ A_i \mid\!- \{P\}\, S_i\, \{Q\},}{A \mid\!- \{P\}\ [\square^{l}_{i=1} S_i]\ \{Q\}} \qquad A =_{def} \cup^{l}_{i=1} A_i$$

Cooperation test $Coop(A_1\ A_2)$: establishes the validity of sets of axioms A_1 and A_2 about the communication correctness:
Assuming

- there is a matching pair of communication operations over channel C, i.e. $C!\ E$ and $C?v$ where E is an expression and v is a variable,
- the matching pair has local pre- and post-conditions
  S_i: ... $\{P'\}\ C!E\ \{Q'\}$.... and
  S_j: ... $\{P''\}\ C?v\ \{Q''\}$...
  respectively,

then the test $Coop()$ for this pair means proving the validity of tripple

$$\mid\!- \{P' \wedge P''\}\ v := E\ \{Q' \wedge Q''\}. \qquad (*)$$

When the tripple (*) is proved correct then $\{P'\}\ C!E\ \{Q'\}$ and $\{P''\}\ C?v\ \{Q''\}$ are treated respectively as axioms $a^i_k \in A_i$ and $a^j_k \in A_j$ in the local proofs of processes S_i and S_j where these tripples occur.