§2.6.2 Hoare Logic

$\{p\}\ S\ \{q\}$ --- a Hoare triple

p: precondition; q: postcondition; 1st-order assertions

$\models \{p\}\ S\ \{q\}$: holds, if,
Whenever exec. of S
starts in a state
satisfying p, and
IF S TERMINATES
then resulting Termination
state ~~satisfies~~
satisfies q

E.g. $\models \{x+y=5 \wedge y=3\}\ x := x+y\ \{x=5 \wedge y=3\}$ — T

$x=2$

$\models \{x=2 \wedge y=3\}\ x := x+y\ \{x=5 \wedge y=3\}$

$\models \{x=2\}\ y := 3;\ x := x+y\ \{x=5 \wedge y=3\}$

AXIOMATIZATION

assignm. rule $\{P[e/x]\}\ x := e\ \{P\}$
holds for atomic assignments, only!

Composition Rule:
$$\frac{\{P\}\ S_1\ \{Q\},\ \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1;\ S_2\ \{R\}}$$

If Statement Rule:
$$\frac{\{P \wedge B\}\ S\ \{Q\},\ (P \wedge \neg B) \Rightarrow Q}{\{P\}\ \text{if}\ (B)\ S;\ \{Q\}}$$

While Statement Rule:
$$\frac{\{I \wedge B\}\ S\ \{I\}}{\{I\}\ \text{while}(B)\ S;\ \{I \wedge \neg B\}}$$

Rule of Consequence:
$$\frac{P' \Rightarrow P,\ \{P\}\ S\ \{Q\},\ Q \Rightarrow Q'}{\{P'\}\ S\ \{Q'\}}$$

Figure 2.3 Inference rules in programming logic *PL*.

Ex of an annotated program with the purpose of verification :

$\{ x \geq 0 \wedge y \geq 0 \}$ ← an assertion from FO PL. over $\mathbb{N}$

$q, r := 0, x ;$

$\{ I : (x = q * y + r) \wedge 0 \leq r \}$ I for INVARIANT

do $\{ I \}$

$y \leq r \rightarrow \{ I \wedge y \leq r \}\ q, r := q+1, r-y \ \{ I \}$

od $\{ I \wedge \neg(y \leq r) \}$

$\{ (x = q * y + r) \wedge 0 \leq r < y \}$

juxtaposition means here IMPLICATION or ... which implies ....

Ex. q.14 (Integer division)

$Div_1 :$ $\quad q, r := 0, x;$

$\underline{do}\ \ y \le r \to q, r := q+1, r-y\ \ \underline{od}$

We prove $\quad \vdash \{0 \le x\}\ Div_1\ \{x = q*y + r \wedge 0 \le r \wedge r < y\}$

By (assignm. ax.)

$\vdash \{x = (q+1)*y + (r-y) \wedge y \le r\}\ q, r := q+1, r-y\ \{x = q*y + r \wedge 0 \le r\}$

By (conseq. rule)

$\vdash \{x = q*y + r \wedge 0 \le r \wedge y \le r\}\ q, r := q+1, r-y\ \{x = q*y + r \wedge 0 \le r\}$

By (do-loop rule) this yields:

$\{x = q*y + r \wedge 0 \le r\}$

$\underline{do}\ \ y \le r \to q, r := q+1, r-y\ \ \underline{od}$

$\{x = q*y + r \wedge 0 \le r \wedge r < y\}$

By (ass. rule): $\vdash \{x = 0*y + x \wedge 0 \le x\}\ q, r := 0, x\ \{x = q*y + r \wedge 0 \le r\}$

$\{x = 0*y + x \wedge 0 \le x\} \leftrightarrow 0 \le x$

$\{x = q*y + r \wedge 0 \le r\} \equiv$ Post div

Finally seq. comp. rule proves the desired result.

Ex. q.30 (Integer div. using proof outlines)

We derived

$$\{x \geq 0 \wedge y > 0\} \; Div \; \{\underbrace{x = q*y + r \wedge 0 \leq r < y}_{\text{post div}}\}$$

with Div :

$q, r := 0, x;$

$\underline{do}\ y \leq r \rightarrow q, r := q+1, r-y\ \underline{od}$

This derivation can also be written down using PROOF OUTLINES. These capture the intermediate steps in a derivation, intuitively: a pfo is an annotation of the program proved correct, in which the intermediate assertions reflect the annotations.

$$\{x \geq 0 \wedge y > 0\}\ q, r := 0, x;\ \{\underbrace{x = q*y + r \wedge 0 \leq r}_{\equiv I}\}$$

$\underline{do}\ \{I\}\ y \leq r \rightarrow \{I \wedge y \leq r\}\ q, r := q+1, r-y\ \{I\}\ \underline{od}$

$\underbrace{\{I \wedge \neg(y \leq r)\}\ \{\text{post div}\}}$

2 ass. juxtaposed express applic. of the conseq. rule