/

p8q12
MJCG

Specification & Verification I

2003

SV2: Solution Notes

This question pertains to the "Program refinement" part of the syllabus.

(a) Define the specification $[P, Q]$ as used in program refinement.

$[P, Q]$ specifies the set of cammands that when run in a state satisfying P terminate in a state satisfying Q, thus:
$[P,Q] \ = \ \{C \mid \ \vdash \ [P]C[Q]\}$

(b) Devise refinement rules for FOR-commands.

A Hoare Logic rule for FOR-commands is

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

with the side condition that neither V, nor any variable in E_1 or E_2, is assigned to in C.
Thus a suitable refinement law based on this would be

$$\begin{array}{l} [P[E_1/V] \wedge E_1 \leq E_2, P[E_2+1/V]] \\ \supseteq \\ \texttt{FOR}\ V\texttt{:=}E_1\ \texttt{UNTIL}\ E_2\ \texttt{DO}\ [P \wedge E_1 \leq V \wedge V \leq E_2, P[V+1/V]] \end{array}$$

provided the FOR-rule side condition holds.
There is also the FOR-axiom

$$\vdash [P \wedge E_2 < E_1]\ \texttt{FOR}\ V\texttt{:=}E_1\ \texttt{UNTIL}\ E_2\ \texttt{DO}\ C\ [P]$$

Which suggests the refinement rule

$$\vdash [P \wedge E_2 < E_1,\ P] \supseteq \texttt{FOR}\ V\texttt{:=}E_1\ \texttt{UNTIL}\ E_2\ \texttt{DO}\ C$$

The model answer here is the obvious convertion of the Hoare rules from the lectures into refinement laws. There may be other good answers (e.g. combining the rule and axiom into a single law).

(c) Show how your rule can can be justified using Floyd-Hoare logic.

In detail, the justification of the law for FOR-commands is:

$C \in$ FOR $V := E_1$ UNTIL E_2 DO $[P \wedge E_1 \leq V \wedge V \leq E_2, P[V+1/V]]$
$\Rightarrow$ (definition of $[\_,\_]$)
$\exists C'.C =$ FOR $V := E_1$ UNTIL E_2 DO $C' \wedge$
    $C' \in [P \wedge E_1 \leq V \wedge V \leq E_2, P[V+1/V]]$
$\Rightarrow$ (definition of $[\_,\_]$)
$\exists C'.C =$ FOR $V := E_1$ UNTIL E_2 DO $C' \wedge$
    $\vdash [P \wedge E_1 \leq V \wedge V \leq E_2] C' [P[V+1/V]]$
$\Rightarrow$ (Hoare rule for FOR-commands, assuming conditions on V)
$\exists C'.C =$ FOR $V := E_1$ UNTIL E_2 DO $C' \wedge$
    $\vdash [P[E_1/V] \wedge E_1 \leq E_2]$ FOR $V := E_1$ UNTIL E_2 DO $C'[P[E_2+1/V]]$
$\Rightarrow$
$\vdash [P[E_1/V] \wedge E_1 \leq E_2] C [P[E_2+1/V]]$
$\Rightarrow$
$C \in [P[E_1/V] \wedge E_1 \leq E_2, P[E_2+1/V]]$

The justification of refinement rule corresponding to the FOR-axiom is immediate from the definition of $[\_,\_]$ and the axiom.

No treatment of refinment for FOR-coomands was discussed during the course, so this part of the question is not bookwork.

(d) Use your rule to show that

`[SUM=0 ∧ 1≤M, SUM = M×N] ⊇ FOR I := 1 UNTIL M DO SUM := SUM+N`

Take $P(V) = \mathtt{SUM} = \mathtt{N} \times (V-1)$, then by my FOR-command refinement rule:

$[\mathtt{SUM} = 0 \wedge 1 \leq \mathtt{M}, \mathtt{SUM} = \mathtt{N} \times \mathtt{M}]$
$\supseteq$
FOR I:=1 UNTIL M DO $[\mathtt{SUM} = \mathtt{N} \times (\mathtt{I}-1) \wedge 1 \leq \mathtt{I} \wedge \mathtt{I} \leq \mathtt{M}, \mathtt{SUM} = \mathtt{N} \times \mathtt{I}]$

It is easy to show:
$\vdash [\mathtt{SUM} = \mathtt{N} \times (\mathtt{I}-1) \wedge 1 \leq \mathtt{I} \wedge \mathtt{I} \leq \mathtt{M}]$
    $\mathtt{SUM} := \mathtt{SUM} + \mathtt{N}$
    $[\mathtt{SUM} = \mathtt{N} \times \mathtt{I}]$
hence by the refinement rule for assignments
$[\mathtt{SUM} = \mathtt{N} \times (\mathtt{I}-1) \wedge 1 \leq \mathtt{I} \wedge \mathtt{I} \leq \mathtt{M}, \mathtt{SUM} = \mathtt{N} \times \mathtt{I}]$
$\supseteq$
$\mathtt{SUM} := \mathtt{SUM} + \mathtt{N}$
Hence desired result by monotonicity of refinement.

The precondition 1≤M makes the question easier (as one doesn't need the FOR-axiom). A harder question would have 0≤M.