p8 q 12
MJCG

Specification & Verification I
2001

SV1.2: Solution Notes

Describe the axioms and rules of Floyd-Hoare logic for reasoning about FOR-commands. Carefully explain any side conditions. [8 marks]

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

where neither V, nor any variable occurring in E_1 or E_2, is assigned to in the command C.

The side condition is a consequence of the semantics of FOR-commands in which the bounds expressions E_1 and E_2 are evaluated once, before the command is executed.

Let $n!$ be the factorial of n ($0! = 1$ and $(n+1)! = (n+1) \times n!$). Give a proof of

$\{N \geq 0\}$ `X := 1; FOR Y := 2 UNTIL N DO X := X` $\times$ `Y` $\{X = N!\}$

[12 marks]

```
|- {X = (Y-1)! /\ 2 <= Y /\ Y <= N} X := X * Y {X = Y!}
(Assignment Axiom + Pre Strength)

i.e.
|- {X = (Y-1)! /\ 2 <= Y /\ Y <= N} X := X * Y {(X = (Y-1)!)[Y+1/Y]}

|- {X = (2-1)! /\ 2 <= N} FOR Y := 2 UNTIL N DO X := X * Y {X = N!}
(FOR-rule)

i.e.
|- {X = 1 /\ 2 <= N} FOR Y := 2 UNTIL N DO X := X * Y {X = N!}

|- {X = 1 /\ N < 2}  FOR Y := 2 UNTIL N DO X := X * Y {X = 1 /\ N < 2}
(FOR-axiom)

hence
|- {X = 1 /\ N = 1}  FOR Y := 2 UNTIL N DO X := X * Y {X = N!}

|- {X = 1 /\ 0 <= N} FOR Y := 2 UNTIL N DO X := X * Y {X = N!}
(Specification Conjunction + Pre Strength)

|- {0 <= N} X := 1 {0 <= N /\ X = 1}
(Assignment Axiom + Pre Strength)

hence
|- {0 <= N} X := 1; FOR Y := 2 UNTIL N DO X := X * Y {X = N!}
(Sequencing)
```