Question II (60%)

Write the total correctness proof tree of the triple $[P]\ S_1 \parallel S_2\ [Q]$ (specified below) where each branch is shown up to the first order formulas. Proving first order formulas is not required.

$P \equiv [x = 5 \wedge y = 7 \wedge v = 0]$

$S_1 : P_1 \equiv [\ x = 5 \wedge y = 7]$

$*\{x+y < 3x\}[3x-y] \quad (y < 15 \rightarrow y := x + y\ ); \qquad [y = 12]$

$\langle\ E!\ y - 2\rangle\ ;\ x := \ y - 1\ ; [y=12 \wedge x=11]\ \langle\ C\ ?\ y\rangle\ ;\ z := x + y$

$Q_1 \equiv [z\text{-}y = 11]$

$\parallel$

$S_2 :\ [u<2 \wedge v=0,\ u=0]$

$\langle v < 1 \rightarrow u := v\ \rangle\ ;\ [u=0 \wedge v<12]\ \langle\ E?\ v\rangle\ ;\ v := v–3;\ [v=7]\ \langle\ C!\ u+v\rangle$

$[v\text{-}u>3]$

$Q \equiv [z < 21\ \ \wedge v > 5]$

Solution

Step 1: Introduce meta-symbols to denote program constructs and annotations. It makes the proof more compact and better readable.

$P\ \equiv x = 5 \wedge y = 7 \wedge v =$ // global precondition
$Q\ \equiv z < 21\ \ \wedge v > 5$ // global post-condition

Process S_1:

$S_{11} : y < 15 \rightarrow y := x + y$ // iterated guarded command
$S_{12} : \langle\ E!\ y - 2\rangle$
$S_{13} : x := \ y - 1$
$S_{14} : \langle\ C\ ?\ y\rangle$
$S_{15} : z := x + y$

$P_1 \equiv x = 5 \wedge y = 7$ // local precondition of process S1
$Q_1 \equiv z\text{-}y = 11$ // local post-condition of process S1
$Inv \equiv x+y < 3x$ // invariant of S11
$V \equiv 3x\text{-}y$ // variant of S11
$P_{11} \equiv y = 12$ // intermediate condition between S11 and S12
$P_{12} \equiv y=12 \wedge x=11$ // intermediate condition between S13 and S14

Process S_2:

$S_{21} : \langle v < 1 \rightarrow u := v\ \rangle$ // guarded command
$S_{22} : \langle\ E?\ v\rangle$
$S_{23} : v := v–3$
$S_{24} : \langle\ C!\ u+v\rangle$

$P_2 \equiv\ u<2 \wedge v=0,\ u=0$ // local precondition of process S_2
$Q_2 \equiv v\text{-}u>3$ // local post-condition of process S_2
$P_{21} \equiv u=0 \wedge v<12$ // intermediate condition between S21 and S_{22}
$P_{22} \equiv v=7$ // intermediate condition between S23 and S_{24}

FOL – first order logic

Step 2: Write the proof tree using meta-symbols as long as they need to be substituted with explicit formulae and program constructs

$$\dfrac{\dfrac{}{A_1 \vdash [P_1]\, S_1 [Q_1]}\,4. \qquad \dfrac{}{A_2 \vdash [P_2]\, S_2\, [Q_2]}\,5. \qquad \dfrac{\dfrac{\vdots}{FOL^1\ proof}\,2.}{\vdash P \Rightarrow P_1 \wedge P_2} \qquad \dfrac{\dfrac{\vdots}{FOL^1\ proof}\,3.}{\vdash Q_1 \wedge Q_2 \Rightarrow Q} \qquad \dfrac{}{Coop(A_1\, A_2)}\,1.}{\vdash [P]\ \ S_1 \,\|\, S_2\, [Q]}$$

<u>Branch 1</u>: Cooperation test

Channel *E*:

$$\begin{array}{c} FOL^1\ proof \\ \hline \vdash (y = 12 \wedge u = 0 \wedge v < 12) \Rightarrow (y = 12 \wedge y - 1 = 11 \wedge (y-2) - 3 = 7) \\ \hline \vdash (y = 12 \wedge u = 0 \wedge v < 12) \Rightarrow (y = 12 \wedge y - 1 = 11 \wedge v - 3 = 7)[\,y - 2/v] \\ \hline \vdash \{y = 12 \wedge u = 0 \wedge v < 12\}\ \ v = y - 2\ \{y = 12 \wedge y - 1 = 11 \wedge v - 3 = 7\} \\ \hline \vdash \{y = 12 \wedge u = 0 \wedge v < 12\}\ \ v := y - 2\ \{(y = 12 \wedge \mathrm{x} = 11)\, [y - 1/x\,] \wedge (v = 7)\, [v - 3/v]\} \end{array}$$

(Substitution in post-condition)
(:= - rule)
(Substitutions in post-condition)

// here post-condition is constructed using assignment axiom

Channel *C*:

$$\begin{array}{c} FOL^1\ proof \\ \hline \vdash (y = 12 \wedge x = 11\ \ \wedge v = 7) \Rightarrow ((\,u+v = 11 \wedge v\text{-}u > 3) \\ \hline \vdash \{y = 12 \wedge x = 11\ \ \wedge v = 7\} \Rightarrow (((x+y) - y = 11) \wedge v\text{-}u > 3)[\,u+v/y] \\ \hline \vdash \{y = 12 \wedge x = 11\ \ \wedge v = 7\}\ y{:=}\ u+v\ \{((x+y) - y = 11) \wedge v\text{-}u > 3\} \\ \hline \vdash \{y = 12 \wedge x = 11\ \ \wedge v = 7\}\ y{:=}\ u+v\ \{((x+y) - y = 11) \wedge v\text{-}u > 3\} \\ \hline \vdash \{y = 12 \wedge x = 11\ \ \wedge v = 7\}\ y{:=}\ u+v\ \{(z - y = 11)[\,x + y\,/\,z] \wedge v\text{-}u > 3\} \end{array}$$

(Substitutions in post-condition)
(:= - rule)
(Substitutions in post-condition)

If the cooperation tests pass we can formulate the communication commands with their local pre- and post-conditions as axioms and do not prove them again in the proofs of local processes S_1 and S_2

For process S_1: we get axioms A_{11} and A_{12}

A_{11}: $[y = 12]\ \langle E!\, y - 2\rangle\,;\, x :=\ y - 1\,; [\mathrm{y}{=}12 \wedge \mathrm{x}{=}11]$

A_{12}: $[\mathrm{y}{=}12 \wedge \mathrm{x}{=}11]\,\langle\, C\ ?\ y\rangle\,;\, \mathrm{z}{:=}\ x + y\ \ [z\text{-}\mathrm{y} = 11]$

For process S_2: we get axioms A_{21} and A_{22}

A_{21}: $[u{=}0 \wedge v{<}12]\ \langle\, E?\ v\rangle\,;\, v := v{-}3;\ \ [v{=}7]$

A_{22}: $[v{=}7]\,\langle\, C!\ u{+}v\rangle\ [v\text{-}u{>}3]$

Thus, $A_1 = \{A_{11}, A_{12}\}$ and $A_2 = \{\, A_{21}, A_{22}\}$

FOL – first order logic

Branch 4: **Local proof of process S_1**

$$\dfrac{\dfrac{\dfrac{4.1}{A_1 \vdash [P_1]\, S_{11}\, [P_{11}]} \qquad \dfrac{\dfrac{\overline{\overline{}}}{A_1 \vdash A_{11}}}{A_1 \vdash [P_{11}]\, S_{12}\, ;\, S_{13}\, [P_{12}]} \qquad \dfrac{\dfrac{\overline{\overline{}}}{A_1 \vdash A_{12}}}{A_1 \vdash [P_{12}]\, S_{14}\, ;\, S_{15}\, [Q_1]}}{A_1 \vdash [P_1]\, S_{11}\, ;\, S_{12}\, ;\, S_{13}\, ;\, S_{14}\, ;\, S_{15}\, [Q_1]}}{A_1 \vdash [P_1]\, S_1\, [Q_1]}$$

Branch 4.1:

$$\dfrac{\dfrac{\dfrac{\textit{FOL}^1\ \textit{proof}}{A_1 \vdash P_1 \Rightarrow Inv} \qquad \dfrac{\textit{FOL}^1\ \textit{proof}}{A_1 \vdash Inv \wedge y<15 \Rightarrow V \geq 0} \qquad \dfrac{\dfrac{\textit{FOL}^1\ \textit{proof}}{A_1 \vdash (Inv \wedge V=n \wedge y<15) \Rightarrow (Inv \wedge V<n)[(x+y)/y]}}{A_1 \vdash [Inv \wedge V=n \wedge y<15]\ y := x+y\ [Inv \wedge V<n]} \qquad \dfrac{\textit{FOL}^1\ \textit{proof}}{A_1 \vdash Inv \wedge V \geq n \Rightarrow P_{11}}}{A_1 \vdash\ \ [P_1]\ \ *\, \{Inv\}\ [V]\ \ (y < 15 \rightarrow y := x + y\ \ );\ \ \ \ [P_{11}]}}{A_1 \vdash [P_1]\, S_{11}\, [P_{11}]}$$

(Iterated guarded command)

Iterated guarded command rule for total correctness $$\dfrac{\vdash P \Rightarrow I \qquad \vdash I \wedge \bigwedge^{n}_{i=1} b_i \Rightarrow V \geq 0 \qquad \vdash \forall i=1,n : [I \wedge V=n \wedge b_i]\ S_i\ [I \wedge V<n] \qquad \vdash (I \wedge_{i=1,n} \neg b_i) \Rightarrow Q}{\vdash \{P\}\ \ *\, \{I\}\ [V]\ [\Box^{n}_{i=1}\, b_i \rightarrow S_i\ ]\ \{Q\}}$$ *I* – invariant, *V* - variant

Branch 5: **Local proof of process S_2**

$$\dfrac{\dfrac{\dfrac{5.1}{A_2 \vdash [P_2]\, S_{21}\, [P_{21}]} \qquad \dfrac{\dfrac{\overline{\overline{}}}{A_2 \vdash A_{21}}}{A_2 \vdash [P_{21}]\, S_{22}\, ;\, S_{23}\, [P_{22}]} \qquad \dfrac{\dfrac{\overline{\overline{}}}{A_2 \vdash A_{22}}}{A_2 \vdash [P_{22}]\, S_{24}\, [Q_2]}}{A_2 \vdash [P_2]\, S_{21}\, ;\, S_{22}\, ;\, S_{23}\, ;\, S_{24}\, [Q_2]}}{A_2 \vdash [P_2]\, S_2\, [Q_2]}$$

Branch 5.1:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\textit{FOL}^1\ \textit{proof}}{A_2 \vdash (u<2 \wedge v=0,\ u=0\ \ \wedge v < 1) \Rightarrow (u=0 \wedge v<12)[v/u]}}{A_2 \vdash [u<2 \wedge v=0,\ u=0\ \ \wedge v < 1]\ u := v\ [u=0 \wedge v<12]}}{A_2 \vdash [u<2 \wedge v=0,\ u=0]\ \ \langle v < 1 \rightarrow u := v \,\rangle\ ;\ [u=0 \wedge v<12]}}{A_2 \vdash [P_2]\, S_{21}\, [P_{21}]}}{5.1}$$

(guarded command)

FOL – first order logic