

Task 1

Name _____

Non-deterministic while program

Annotate and prove the correctness of program **S** provided the following specification is given:

$$\{x = 0 \wedge n > 0\} S \{z = n\}$$

$S \equiv$

$y, x, z := n, 0, 0;$

$* (x = 0 \wedge y > 0 \rightarrow z := z + 1; x := 1$

\square

$x \neq 0 \wedge y > 0 \rightarrow y := y - 1; x := 0)$

Hint: use $z+y-x = n$ as one conjunct of the invariant

Solution

Annotated program:

$$P \equiv \{x = 0 \wedge n > 0\}$$

C		C1	$y, x, z := n, 0, 0;$
		$P_1 \equiv \{x = 0 \wedge n > 0 \wedge y = n \wedge z = 0\}$	
		*	$I \equiv \{z + y - x = n\}$
		C21	$(x = 0 \wedge y > 0 \rightarrow z := z + 1; x := 1$
		C2	\square
		C22	$x \neq 0 \wedge y > 0 \rightarrow y := y - 1; x := 0)$

$$Q \equiv \{z = n\}$$

Partial correctness proof:

$\vdash n > 0 \Rightarrow n > 0$	$(A \Rightarrow A)$
$\vdash x=0 \wedge n > 0 \Rightarrow n > 0$	$(\wedge \Rightarrow)$
$\vdash x=0 \wedge n > 0 \Rightarrow 0=0 \wedge n > 0 \wedge n=n \wedge 0=0$	$(=)$
$\vdash P \Rightarrow P_1 [n/y, 0/x, 0/z]$	(subs)
$\vdash \{P\} C1 \{P_1\}$	$(:=)$
$\vdash P_1 \Rightarrow I$	1
$\vdash (I \wedge \neg b_G) \Rightarrow Q$	2
$\vdash \{I \wedge b_{21}\} C21 \{I\}$	3
$\vdash \{I \wedge b_{22}\} C21 \{I\}$	4
$\vdash \{P_1\} C2 \{Q\}$	$(*)$
$\vdash \{P\} C \{Q\}$	$(;)$

$$\begin{array}{c}
\frac{}{\vdash x=0 \wedge n>0 \wedge y=n \wedge z=0 \Rightarrow n=n} \quad (\Rightarrow \text{true}) \\
\frac{}{\vdash x=0 \wedge n>0 \wedge y=n \wedge z=0 \Rightarrow 0+n-0=n} \\
\frac{}{\vdash x=0 \wedge n>0 \wedge y=n \wedge z=0 \Rightarrow z+y-x=n} \quad (\text{subst}) \\
\hline
1
\end{array}$$

$$\begin{array}{c}
\frac{}{\vdash z+y-x=n \wedge (x \neq 0 \vee y>0) \wedge (x=0 \vee y>0) \Rightarrow z=n} \\
\frac{}{\vdash z+y-x=n \wedge \neg(x=0 \wedge y>0) \wedge \neg(x \neq 0 \wedge y>0) \Rightarrow z=n} \\
\frac{}{\vdash z+y-x=n \wedge \neg(b_{21} \vee b_{22}) \Rightarrow z=n} \quad ([./b_{21}, ./b_{22}]) \\
\frac{}{\vdash z+y-x=n \wedge \neg(b_{21} \vee b_{22}) \Rightarrow z=n} \quad (\text{subst}) \\
\hline
2
\end{array}$$

$$\begin{array}{c}
\frac{}{\vdash I \wedge b_{21} \Rightarrow z+y=n} \\
\frac{}{\vdash I \wedge b_{21} \Rightarrow z+1+y-1=n} \\
\frac{}{\vdash I \wedge b_{22} \Rightarrow I[1/x, z+1/z]} \quad ([./x, ./z]) \\
\hline
3
\end{array}$$

$$\begin{array}{c}
\frac{}{\vdash I \wedge b_{22} \Rightarrow z+y-1=n} \\
\frac{}{\vdash I \wedge b_{22} \Rightarrow z+y-1-0=n} \\
\frac{}{\vdash I \wedge b_{22} \Rightarrow I[0/x, y-1/y]} \quad ([./x, ./y]) \\
\hline
4
\end{array}$$

Task 2

Name _____

Shared variable parallel programs (interference test)

Specify assertions for interference test of the program specification

$$\begin{aligned} P_1 &\equiv \{x \leq 4 \wedge y = 2\} \\ S_1 &: \langle x \geq 2 \rightarrow y := y - 2 \rangle \\ Q_1 &\equiv \{y \leq x \wedge x \geq 0\} \\ &\parallel \\ P_2 &\equiv \{x \geq 0 \wedge y \geq 0\} \\ S_2 &: \langle x = 4 \wedge y = 1 \rightarrow z := x - 3 \rangle \\ Q_2 &\equiv \{y + 2 \leq x\} \end{aligned}$$

S1 body does not interfere P2:

$$\vdash \{P_1 \wedge x \geq 2 \wedge P_2\} y := y - 2 \{P_2\}$$

S1 body does not interfere Q2:

$$\vdash \{P_1 \wedge x \geq 2 \wedge Q_2\} y := y - 2 \{Q_2\}$$

S2 body does not interfere P1:

$$\vdash \{P_2 \wedge x = 4 \wedge y = 1 \wedge P_1\} z := x - 3 \{P_1\}$$

S2 body does not interfere Q1:

$$\vdash \{P_2 \wedge x = 4 \wedge y = 1 \wedge Q_1\} z := x - 3 \{Q_1\}$$

Task 3

Name _____

Parallel programs with message passing (cooperation test).
Specify assertions for cooperation test.

$$\begin{aligned} P_1 &\equiv \{x = 5 \wedge y = 7\} \\ S_1 &: \langle E! y - 2 \rangle; \langle x := y - 1 \rangle \{x = 6 \wedge y = 7\}; \langle C! x + 5 \rangle \\ Q_1 &\equiv \{y < 9 \wedge x > 0\} \\ &\parallel \\ P_2 &\equiv \{u = 0\} \\ S_2 &: \langle E? u \rangle; \{u < 10\} \langle C? u \rangle \\ Q_2 &\equiv \{u > 9\} \end{aligned}$$

Solution:

Test for channel E:

$$\vdash \{P_1 \wedge P_2\} u := y - 2 \{(x = 6 \wedge y = 7) [y - 1/x] \wedge u < 10\}$$

Test for channel C:

$$\vdash \{x = 6 \wedge y = 7\} u := x + 5 \{Q_1 \wedge Q_2\}$$