MODULE *TestRWLLSC*

EXTENDS *Integers*, *FiniteSets*, *TLAPS*
CONSTANT N
VARIABLES pc, ll, X, x, v, S, ret
ASSUME $NPosInt \triangleq N \in Nat \setminus \{0\}$

$vars \triangleq \langle pc, ll, X, x, v, S, ret \rangle$
$Bot \triangleq -15$
$Ack \triangleq -20$
$ProcSet \triangleq 1 \,..\, N$

$Init \triangleq \land pc \in [ProcSet \to \{1, 3\}]$
$\land ll = [p \in ProcSet \mapsto \text{FALSE}]$
$\land X = 0$
$\land X \in Nat$
$\land x = [p \in ProcSet \mapsto 0]$
$\land x \in [ProcSet \to Nat]$
$\land v \in [ProcSet \to Nat]$
$\land S = X$
$\land ret = [p \in ProcSet \mapsto Bot]$
$\land ret \in [ProcSet \to Nat]$???

$\text{x}_p \leftarrow X$
$L1(p) \triangleq \land pc[p] = 1$
$\land pc' = [pc \text{ EXCEPT } ![p] = 2]$
$\land x' = [x \text{ EXCEPT } ![p] = X]$
$\land ret' = [ret \text{ EXCEPT } ![p] = X]$
$\land \text{UNCHANGED } \langle ll, X, v, S \rangle$

return x_p
$L2(p) \triangleq \land pc[p] = 2$
$\land \exists Line \in \{1, 3\} : pc' = [pc \text{ EXCEPT } ![p] = Line]$
$\land ret' = [ret \text{ EXCEPT } ![p] = Bot]$
$\land \text{UNCHANGED } \langle ll, X, x, v, S \rangle$

$\text{X.LL}_p()$
$L3(p) \triangleq \land pc[p] = 3$
$\land pc' = [pc \text{ EXCEPT } ![p] = 4]$
$\land ll' = [ll \text{ EXCEPT } ![p] = \text{TRUE}]$
$\land \text{UNCHANGED } \langle X, x, v, S, ret \rangle$

$\text{X.SC}_p(v_p)$
$L4(p) \triangleq \lor (\land pc[p] = 4$
$\land ll[p] = \text{TRUE}$
$\land pc' = [pc \text{ EXCEPT } ![p] = 5]$
$\land ll' = [q \in ProcSet \mapsto \text{FALSE}]$

$$
\begin{array}{l}
\quad \land X' = v[p] \\
\quad \land S' = v[p] \\
\quad \land ret' = [q \in ProcSet \mapsto \text{IF } (\land pc[q] = 4 \\
\qquad\qquad\qquad\qquad\qquad\qquad \land ll[q] = \text{TRUE}) \text{ THEN } Ack \text{ ELSE } ret[q]] \\
\quad \land \text{UNCHANGED } \langle x, v \rangle) \\
\lor (\land pc[p] = 4 \\
\quad \land ll[p] = \text{FALSE} \\
\quad \land pc' = [pc \text{ EXCEPT } ![p] = 5] \\
\quad \land \text{UNCHANGED } \langle ll, X, x, v, S, ret \rangle)
\end{array}
$$

return ack

$$
\begin{array}{lll}
L5(p) & \triangleq & \land pc[p] = 5 \\
& & \land \exists Line \in \{1, 3\} : pc' = [pc \text{ EXCEPT } ![p] = Line] \\
& & \land ret' = [ret \text{ EXCEPT } ![p] = Bot] \\
& & \land \exists v\_pr \in Nat : v' = [v \text{ EXCEPT } ![p] = v\_pr] \\
& & \land \text{UNCHANGED } \langle ll, X, x, S \rangle
\end{array}
$$

$$
\begin{array}{lll}
Step(p) & \triangleq & \lor L1(p) \\
& & \lor L2(p) \\
& & \lor L3(p) \\
& & \lor L4(p) \\
& & \lor L5(p)
\end{array}
$$

$$Next \triangleq (\exists p \in ProcSet : Step(p))$$

$$
\begin{array}{lll}
Spec & \triangleq & \land Init \\
& & \land \Box[Next]_{vars}
\end{array}
$$

Invariants

$$Inv1 \triangleq X = S$$

$$
\begin{array}{l}
Inv2 \triangleq \forall p \in ProcSet : \land pc[p] \in \{1, 3\} \Rightarrow ret[p] = Bot \\
\qquad\qquad\qquad\qquad \land pc[p] \in \{2, 5\} \Rightarrow ret[p] \neq Bot \\
\qquad\qquad\qquad\qquad\qquad\qquad \land pc[p] = 2 \Rightarrow ret[p] \neq Bot \\
\qquad\qquad\qquad\qquad\qquad\qquad \land pc[p] = 5 \Rightarrow ret[p] = Ack
\end{array}
$$

$$
\begin{array}{l}
Inv3 \triangleq \forall p \in ProcSet : ((\land pc[p] = 4 \\
\qquad\qquad\qquad\qquad\qquad\qquad \land ll[p] = \text{TRUE}) \Rightarrow ret[p] = Bot)
\end{array}
$$

$$
\begin{array}{l}
Inv4 \triangleq \forall p \in ProcSet : ((\land pc[p] = 4 \\
\qquad\qquad\qquad\qquad\qquad\qquad \land ll[p] = \text{FALSE}) \Rightarrow ret[p] = Ack)
\end{array}
$$

Inductive invariant

$$Lines \triangleq \{1, 2, 3, 4, 5\}$$

$$
\begin{array}{lll}
TypeOK & \triangleq & \land pc \in [ProcSet \to Lines] \\
& & \land ll \in [ProcSet \to \text{BOOLEAN }]
\end{array}
$$

$\land X \in Nat$
$\land x \in [ProcSet \to Nat]$
$\land v \in [ProcSet \to Nat]$
$\land S \in Nat$
$\land ret \in [ProcSet \to Nat \cup \{Ack, Bot\}]$

$IInv \triangleq \land TypeOK$
$\land Inv1$
$\land Inv2$
$\land Inv3$
$\land Inv4$

$ISpec \triangleq \land IInv$
$\land \Box[Next]_{vars}$

Type correctness

THEOREM $TypeCorrectness \triangleq Spec \Rightarrow \Box TypeOK$
$\langle 1 \rangle$ USE $NPosInt$DEFS $ProcSet$, $Lines$, $TypeOK$
$\langle 1 \rangle 1$. $Init \Rightarrow TypeOK$
PROOF BY DEF $Init$
$\langle 1 \rangle 2$. $TypeOK \land [Next]_{vars} \Rightarrow TypeOK'$
$\langle 2 \rangle$ SUFFICES ASSUME $TypeOK$, $[Next]_{vars}$ PROVE $TypeOK'$
OBVIOUS
$\langle 2 \rangle 1$. ASSUME NEW $p \in ProcSet$, $L1(p)$ PROVE $TypeOK'$
PROOF BY $\langle 2 \rangle 1$ DEF $Next$, $vars$, $Step$, $L1$, $L2$, $L3$, $L4$, $L5$
$\langle 2 \rangle 2$. ASSUME NEW $p \in ProcSet$, $L2(p)$ PROVE $TypeOK'$
PROOF BY $\langle 2 \rangle 2$ DEF $Next$, $vars$, $Step$, $L1$, $L2$, $L3$, $L4$, $L5$
$\langle 2 \rangle 3$. ASSUME NEW $p \in ProcSet$, $L3(p)$ PROVE $TypeOK'$
PROOF BY $\langle 2 \rangle 3$ DEF $Next$, $vars$, $Step$, $L1$, $L2$, $L3$, $L4$, $L5$
$\langle 2 \rangle 4$. ASSUME NEW $p \in ProcSet$, $L4(p)$ PROVE $TypeOK'$
$\langle 3 \rangle 1$.CASE $\land pc[p] = 4$
$\land ll[p] = \text{TRUE}$
$\land pc' = [pc \text{ EXCEPT } ![p] = 5]$
$\land ll' = [q \in ProcSet \mapsto \text{FALSE}]$
$\land X' = v[p]$

$\land\ S' = v[p]$
$\land\ ret' = [q \in ProcSet \mapsto \text{IF } (\land\ pc[q] = 4$
$\land\ ll[q] = \text{TRUE}) \text{ THEN } Ack \text{ ELSE } ret[q]]$
$\land$ UNCHANGED $\langle x, v\rangle$
PROOF BY $\langle 3\rangle 1$, $\langle 2\rangle 4$ DEF *Next*, *vars*, *Step*, *L*1, *L*2, *L*3, *L*4, *L*5
$\langle 3\rangle 2$.CASE $\land\ pc[p] = 4$
$\land\ ll[p] = \text{FALSE}$
$\land\ pc' = [pc \text{ EXCEPT } ![p] = 5]$
$\land$ UNCHANGED $\langle ll, X, x, v, S, ret\rangle$
PROOF BY $\langle 3\rangle 2$, $\langle 2\rangle 4$ DEF *Next*, *vars*, *Step*, *L*1, *L*2, *L*3, *L*4, *L*5
$\langle 3\rangle 3$. QED
BY $\langle 2\rangle 4$, $\langle 3\rangle 1$, $\langle 3\rangle 2$ DEF *L*4

$\langle 2\rangle 5$. ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $TypeOK'$
PROOF BY $\langle 2\rangle 5$ DEF *Next*, *vars*, *Step*, *L*1, *L*2, *L*3, *L*4, *L*5
$\langle 2\rangle 6$.CASE UNCHANGED *vars*
PROOF BY $\langle 2\rangle 6$ DEF *Next*, *vars*, *Step*, *L*1, *L*2, *L*3, *L*4, *L*5
$\langle 2\rangle 7$. QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$ DEF *Next*, *Step*
$\langle 1\rangle 3$. QED
PROOF BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, *PTL* DEF *Spec*

THEOREM $Spec \Rightarrow \Box IInv$
$\langle 1\rangle$ USE *NPosInt*DEFS *ProcSet*, *Lines*, *TypeOK*, *IInv*, *Inv*1, *Inv*2, *Inv*3, *Inv*4, *Bot*, *Ack*
$\langle 1\rangle 1$. $Init \Rightarrow IInv$
PROOF BY DEF *Init*
$\langle 1\rangle 2$. $IInv \land [Next]_{vars} \Rightarrow IInv'$
$\langle 2\rangle$ SUFFICES ASSUME $IInv$,
$[Next]_{vars}$
PROVE $IInv'$
OBVIOUS
$\langle 2\rangle 1$. ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $IInv'$
PROOF BY $\langle 2\rangle 1$ DEF *Next*, *vars*, *L*1, *L*2, *L*3, *L*4, *L*5
$\langle 2\rangle 2$. ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $IInv'$
PROOF BY $\langle 2\rangle 2$ DEF *Next*, *vars*, *L*1, *L*2, *L*3, *L*4, *L*5
$\langle 2\rangle 3$. ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $IInv'$
PROOF BY $\langle 2\rangle 3$ DEF *Next*, *vars*, *L*1, *L*2, *L*3, *L*4, *L*5

⟨2⟩4. ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $IInv'$
⟨3⟩1.CASE $\land\ pc[p] = 4$
$\land\ ll[p] = \text{TRUE}$
$\land\ pc' = [pc \text{ EXCEPT } ![p] = 5]$
$\land\ ll' = [q \in ProcSet \mapsto \text{FALSE}]$
$\land\ X' = v[p]$
$\land\ S' = v[p]$
$\land\ ret' = [q \in ProcSet \mapsto \text{IF } (\land\ pc[q] = 4$
$\land\ ll[q] = \text{TRUE}) \text{ THEN } Ack \text{ ELSE } ret[q]]$
$\land$ UNCHANGED $\langle x, v\rangle$
PROOF BY ⟨3⟩1, ⟨2⟩4 DEF $Next$, $vars$, $L1$, $L2$, $L3$, $L4$, $L5$
⟨3⟩2.CASE $\land\ pc[p] = 4$
$\land\ ll[p] = \text{FALSE}$
$\land\ pc' = [pc \text{ EXCEPT } ![p] = 5]$
$\land$ UNCHANGED $\langle ll, X, x, v, S, ret\rangle$
PROOF BY ⟨3⟩2, ⟨2⟩4 DEF $Next$, $vars$, $L1$, $L2$, $L3$, $L4$, $L5$
⟨3⟩3. QED
BY ⟨2⟩4, ⟨3⟩1, ⟨3⟩2 DEF $L4$

⟨2⟩5. ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $IInv'$
PROOF BY ⟨2⟩5 DEF $Next$, $vars$, $L1$, $L2$, $L3$, $L4$, $L5$
⟨2⟩6.CASE UNCHANGED $vars$
PROOF BY ⟨2⟩6 DEF $Next$, $vars$, $L1$, $L2$, $L3$, $L4$, $L5$
⟨2⟩7. QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6 DEF $Next$, $Step$

⟨1⟩3. QED
PROOF BY ⟨1⟩1, ⟨1⟩2, PTL DEF $Spec$

* Modification History
* Last modified *Wed* May 05 00:04:45 *EDT* 2021 by *uguryavuz*
* Created *Tue* May 04 21:45:09 *EDT* 2021 by *uguryavuz*