MODULE *PaxosEPR*

EXTENDS *TLC*, *Integers*, *FiniteSets*

CONSTANTS *Node*, *Ballot*, *Value*

ASSUME $0 \in Ballot$

CONSTANT *Quorum*

CONSTANT *None*

VARIABLES *ballotStart*,
*prepareMsg*,
*proposeMsg*,
*voteMsg*,
*leftBallot*,
*joinedBallot*,
*decision*

$vars \triangleq \langle ballotStart, prepareMsg, proposeMsg, voteMsg, leftBallot, joinedBallot, decision \rangle$

$$
\begin{aligned}
Init \triangleq\ & \land ballotStart = [b \in Ballot \mapsto \text{FALSE}] \\
& \land prepareMsg = [n \in Node \mapsto [b \in Ballot \mapsto None]] \\
& \land proposeMsg = [b \in Ballot \mapsto None] \\
& \land voteMsg = [n \in Node \mapsto [b \in Ballot \mapsto None]] \\
& \land leftBallot = [n \in Node \mapsto [b \in Ballot \mapsto \text{FALSE}]] \\
& \land joinedBallot = [n \in Node \mapsto [b \in Ballot \mapsto \text{FALSE}]] \\
& \land decision = [n \in Node \mapsto [b \in Ballot \mapsto \{\}]]
\end{aligned}
$$

$$
\begin{aligned}
max(S) \triangleq\ & \text{IF } S = \{\} \text{ THEN } 0 \\
& \text{ELSE CHOOSE } x \in S : \forall\, y \in S : x \geq y
\end{aligned}
$$

$$
\begin{aligned}
Phase1a(b) \triangleq\ & \land ballotStart' = [ballotStart \text{ EXCEPT } ![b] = \text{TRUE}] \\
& \land \text{UNCHANGED } \langle prepareMsg, proposeMsg, voteMsg, leftBallot, joinedBallot, decision \rangle
\end{aligned}
$$

$$
\begin{aligned}
Phase1b(n,\, b) \triangleq\ & \land ballotStart[b] = \text{TRUE} \\
& \land leftBallot[n][b] = \text{FALSE} \\
& \land \text{LET } maxBal \triangleq max(\{t \in Ballot : t < b \land voteMsg[n][t] \neq None\}) \\
& \qquad\ maxVal \triangleq \text{IF } maxBal \neq 0 \text{ THEN } voteMsg[n][maxBal] \\
& \qquad\qquad\qquad \text{ELSE } None
\end{aligned}
$$

$$
\begin{array}{l}
\quad \text{IN} \\
\qquad prepareMsg = [prepareMsg \text{ EXCEPT } ![n][b] = \langle maxBal,\ maxVal\rangle] \\
\land\ \ leftBallot = [leftBallot \text{ EXCEPT } ![n] = \\
\qquad\qquad [t \in Ballot \mapsto \text{IF } \lor\, t < b \\
\qquad\qquad\qquad\qquad\qquad\qquad \lor\, leftBallot[n][t] = \text{TRUE} \\
\qquad\qquad\qquad\qquad\quad \text{THEN TRUE} \\
\qquad\qquad\qquad\qquad\quad \text{ELSE FALSE}]] \\
\land\, joinedBallot' = [joinedBallot \text{ EXCEPT } ![n][b] = \text{TRUE}] \\
\land \text{ UNCHANGED } \langle ballotStart,\ proposeMsg,\ voteMsg,\ decision\rangle
\end{array}
$$

$$
\begin{array}{l}
Phase2a(b,\ Q) \triangleq\ \land\, proposeMsg[b] = None \\
\qquad\qquad \land\, \forall\, nn \in Q : joinedBallot[nn][b] = \text{TRUE} \\
\qquad\qquad \land \text{ LET } maxVotedBallot \triangleq [n \in Q \mapsto max(\{t \in Ballot :\ \land\, t < b \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \land\, voteMsg[n][t] \neq None\})] \\
\qquad\qquad\qquad maxNode \triangleq \text{ CHOOSE } n \in Q : \forall\, m \in Q : maxVotedBallot[n] \geq maxVotedBallot[m] \\
\qquad\qquad\qquad maxBallot \triangleq maxVotedBallot[maxNode] \\
\qquad\qquad\qquad maxValue \triangleq \text{ IF } maxBallot \neq 0 \text{ THEN } voteMsg[maxNode][maxBallot] \\
\qquad\qquad\qquad\qquad\qquad \text{ELSE CHOOSE } v \in Value : \text{TRUE} \\
\qquad\qquad \text{IN} \\
\qquad\qquad\quad proposeMsg' = [proposeMsg \text{ EXCEPT } ![b] = maxValue] \\
\qquad\qquad \land \text{ UNCHANGED } \langle ballotStart,\ prepareMsg,\ voteMsg,\ leftBallot,\ joinedBallot,\ decision\rangle
\end{array}
$$

$$
\begin{array}{l}
Phase2b(n,\ b) \triangleq\ \land\, proposeMsg[b] \neq None \\
\qquad\qquad \land\, leftBallot[n][b] = \text{FALSE} \\
\qquad\qquad \land\, voteMsg' = [voteMsg \text{ EXCEPT } ![n][b] = proposeMsg[b]] \\
\qquad\qquad \land \text{ UNCHANGED } \langle ballotStart,\ prepareMsg,\ proposeMsg,\ leftBallot,\ joinedBallot,\ decision\rangle
\end{array}
$$

$$
\begin{array}{l}
Learn(n,\ b,\ v,\ Q) \triangleq\ \land\, \forall\, t \in Q : voteMsg[t][b] = v \\
\qquad\qquad\qquad\qquad\ \land\ \ decision' = [decision \text{ EXCEPT } ![n][b] = decision[n][b] \cup \{v\}] \\
\qquad\qquad\qquad\qquad\ \land \text{ UNCHANGED } \langle ballotStart,\ prepareMsg,\ proposeMsg,\ voteMsg, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad leftBallot,\ joinedBallot\rangle
\end{array}
$$

$$
\begin{array}{l}
Next \triangleq\ \lor\, \exists\, b \in Ballot : Phase1a(b) \\
\qquad\ \lor\, \exists\, n \in Node,\ b \in Ballot : Phase1b(n,\ b) \\
\qquad\ \lor\, \exists\, b \in Ballot,\ Q \in Quorum : Phase2a(b,\ Q) \\
\qquad\ \lor\, \exists\, n \in Node,\ b \in Ballot : Phase2b(n,\ b)
\end{array}
$$

$$
Spec \triangleq\ Init \land \Box[Next]_{vars}
$$

$$
\begin{array}{l}
Inv \triangleq\ \land\, \forall\, n1,\ n2 \in Node,\ b1,\ b2 \in Ballot,\ v1,\ v2 \in Value : v1 \in decision[n1][b1] \land v2 \in decision[n2][b2] \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Rightarrow v1 = v2 \\
\qquad\ \land\, \forall\, b \in Ballot,\ v1,\ v2 \in Value : proposeMsg[b] = v1 \land proposeMsg[b] = v2 \Rightarrow v1 = v2 \\
\qquad\ \land\, \forall\, n \in Node,\ b \in Ballot,\ v \in Value : voteMsg[n][b] = v\ \ \Rightarrow proposeMsg[b] = v \\
\qquad\ \land\, \forall\, b \in Ballot,\ v \in Value : (\exists\, n \in Node : decision[n][b] = v) \Rightarrow \\
\qquad\qquad\qquad\qquad\qquad\qquad (\exists\, Q \qquad \in Quorum : \forall\, n \in Node : n \in Q \Rightarrow voteMsg[n][b] = v)
\end{array}
$$

$$
\begin{aligned}
&\land \forall\, n \in \mathit{Node},\, b1,\, b2 \in \mathit{Ballot},\, v1,\, v2 \in \mathit{Value} : \mathit{prepareMsg}[n][b1] = \langle 0,\, v1\rangle \land b2 < b1 \\
&\qquad\qquad \Rightarrow \neg(\mathit{voteMsg}[n][b2] = v2) \\
&\land \forall\, n \in \mathit{Node},\, b1,\, b2 \in \mathit{Ballot},\, v \in \mathit{Value} : \mathit{proposeMsg}[n][b1] = \langle b2,\, v\rangle \land b2 \neq 0 \Rightarrow b2 < b1 \\
&\qquad\qquad \land \mathit{voteMsg}[n][b2] = v \\
&\land \forall\, n \in \mathit{Node},\, b1,\, b2,\, b3 \in \mathit{Ballot},\, v1,\, v2 \in \mathit{Value} : \mathit{proposeMsg}[n][b1] = \langle b2,\, v1\rangle \land b2 \neq 0 \\
&\qquad\qquad \land b2 < b3 \land b3 < b1 \Rightarrow \\
&\qquad\qquad \neg(\mathit{voteMsg}[n][b3] = v2) \\
&\land \forall\, n \in \mathit{Node},\, v \in \mathit{Value} : \neg(\mathit{voteMsg}[n][0] = v) \\
&\land \forall\, b1,\, b2 \in \mathit{Ballot},\, v1,\, v2 \in \mathit{Value},\, Q \in \mathit{Quorum} : \mathit{proposeMsg}[b2] = v2 \land b1 < b2 \land v1 \neq v2 \;\Rightarrow \\
&\qquad \exists\, n \in \mathit{Node} : n \in Q \land \neg(\mathit{voteMsg}[n][b1] = v1) \land \mathit{leftBallot}[n][b1] = \text{TRUE} \\
&\land \forall\, n \in \mathit{Node},\, b1,\, b2 \in \mathit{Ballot} : b1 < b2 \land \mathit{joinedBallot}[n][b2] = \text{TRUE} \Rightarrow \\
&\qquad\qquad \mathit{leftBallot}[n][b1] = \text{TRUE} \\
&\land \forall\, n \in \mathit{Node},\, b1,\, b2 \in \mathit{Ballot},\, v \in \mathit{Value} : \mathit{proposeMsg}[n][b1] = \langle b2,\, v\rangle \Rightarrow \\
&\qquad\qquad \mathit{joinedBallot}[n][b1] = \text{TRUE}
\end{aligned}
$$

\ * Modification History
\ * Last modified *Fri Apr* 29 13:37:09 *CST* 2022 by *gxs*
\ * Last modified *Fri Apr* 29 13:32:20 *CST* 2022 by *gxs*
\ * Last modified *Thu Apr* 28 21:41:21 *CST* 2022 by *xiaosong*
\ * Created *Tue Apr* 26 19:47:36 *CST* 2022 by *xiaosong*