MODULE *MultiPaxos*

Heavily inspired by (https://*github.com*/nano-o/*MultiPaxos*/blob/master/*MultiPaxos.tla*)

EXTENDS *Integers*, *FiniteSets*, *Sequences*

CONSTANTS *Acceptors*, *Values*, *Ballots*

$Maximum(S) \triangleq$ IF $S = \{\}$ THEN -1
ELSE CHOOSE $n \in S : \forall\, m \in S : n \geq m$

$Max(S,\, LessEq(\_,\, \_)) \triangleq$ IF $S = \{\}$ THEN -1
ELSE CHOOSE $n \in S : \forall\, m \in S : LessEq(m,\, n)$

$Instances \triangleq \{1,\, 2,\, 3\}$

$Quorums \triangleq \{Q \in \text{SUBSET } Acceptors : Cardinality(Q) * 2 > Cardinality(Acceptors)\}$

$None \triangleq$ CHOOSE $v : v \notin Values$

$Messages \triangleq [type : \{\text{“prepare”}\},\, bal : Ballots]$
$\cup$
$[type : \{\text{“promise”}\},\, bal : Ballots,\, maxVBal : Ballots \cup \{-1\},\, maxVVal : Values \cup \{None\},\, acc :$
$\cup$
$[type : \{\text{“accept”}\},\quad bal : Ballots,\, val : Values]$
$\cup$
$[type : \{\text{“accepted”}\},\, maxVBal : Ballots,\, maxVVal : Values,\, acc : Acceptors]$

VARIABLES $ballot$, $1amsgs$, $1bmsgs$, $2amsgs$, $vote$, $leaderVote$

$vars \triangleq \langle leaderVote,\, ballot,\, vote,\, 1amsgs,\, 1bmsgs,\, 2amsgs\rangle$

$TypeOK \triangleq \land\, ballot \in [Acceptors \to Ballots \cup \{-1\}]$
$\land\, 1amsgs \subseteq \{\langle b\rangle : b \in Ballots\}$
$\land\, vote \in [Acceptors \to [Instances \to [Ballots \to Values \cup \{None\}]]]$

$allEntries \triangleq \{\langle i,\, \langle b,\, v\rangle\rangle : i \in Instances,\, b \in Ballots \cup \{-1\},\, v \in Values \cup \{None\}\}$

$MaxVotedBallot(i,\, a,\, max) \triangleq Max(\{b \in Ballots : b \leq max \land vote[a][i][b] \neq None\} \cup \{-1\},\ \leq)$

$MaxVotedBallots(i,\, Q,\, max) \triangleq \{MaxVotedBallot(i,\, a,\, max) : a \in Q\}$

$HighestVote(i,\, max,\, Q) \triangleq$ IF $\exists\, a \in Q : MaxVotedBallot(i,\, a,\, max) \neq -1$
THEN LET $MaxVoter \triangleq$ CHOOSE $a \in Q : MaxVotedBallot(i,\, a,\, max) = Max(M$
IN $vote[MaxVoter][i][MaxVotedBallot(i,\, MaxVoter,\, max)]$
ELSE $None$

$$
\begin{aligned}
\mathit{Init} \triangleq\ & \land\ \mathit{ballot} = [a \in \mathit{Acceptors} \mapsto 0] \\
& \land\ 1\mathit{amsgs} = \{\} \\
& \land\ 1\mathit{bmsgs} = \{\} \\
& \land\ 2\mathit{amsgs} = \{\} \\
& \land\ \mathit{vote} = [a \in \mathit{Acceptors} \mapsto [i \in \mathit{Instances} \mapsto [b \in \mathit{Ballots} \mapsto \mathit{None}]]] \\
& \land\ \mathit{leaderVote} = [b \in \mathit{Ballots} \mapsto [i \in \mathit{Instances} \mapsto \langle -1,\ \mathit{None} \rangle]]
\end{aligned}
$$

$$
\begin{aligned}
\mathit{IncreaseBallot}(a,\ b) \triangleq\ & \land\ \mathit{ballot}[a] < b \\
& \land\ \mathit{ballot}' = [\mathit{ballot}\ \text{EXCEPT}\ ![a] = b] \\
& \land\ \text{UNCHANGED}\ \langle \mathit{vote},\ \mathit{leaderVote},\ 1\mathit{amsgs},\ 1\mathit{bmsgs},\ 2\mathit{amsgs} \rangle
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Phase1a}(b) \triangleq\ & \land\ \neg \exists\, \mathit{msg} \in 1\mathit{amsgs} : \mathit{msg}[1] = b \\
& \land\ 1\mathit{amsgs}' = 1\mathit{amsgs} \cup \{\langle b \rangle\} \\
& \land\ \text{UNCHANGED}\ \langle \mathit{ballot},\ 1\mathit{bmsgs},\ 2\mathit{amsgs},\ \mathit{vote},\ \mathit{leaderVote} \rangle
\end{aligned}
$$

$$
\begin{aligned}
\mathit{MaxBallotAndVote}(a,\ i,\ \mathit{max}) \triangleq\ & \text{LET}\ \mathit{maxBallot} \triangleq \mathit{Max}(\{b \in \mathit{Ballots} : b \leq \mathit{max} \land \mathit{vote}[a][i][b] \neq \mathit{None}\} \cup \{ \\
& \phantom{\text{LET}}\ v \triangleq \text{IF}\ \mathit{maxBallot} = -1\ \text{THEN}\ \mathit{None} \\
& \phantom{\text{LET}\ v \triangleq \text{IF}\ \mathit{maxBallot} = -1}\ \text{ELSE}\ \ \mathit{vote}[a][i][\mathit{maxBallot}] \\
& \text{IN}\ \ \langle \mathit{maxBallot},\ v \rangle
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Phase1b}(a,\ b) \triangleq\ & \land\ \mathit{ballot}[a] < b \\
& \land\ \langle b \rangle \in 1\mathit{amsgs} \\
& \land\ \mathit{ballot}' = [\mathit{ballot}\ \text{EXCEPT}\ ![a] = b] \\
& \land\ 1\mathit{bmsgs}' = 1\mathit{bmsgs} \cup \{\langle a,\ b,\ \{\langle i,\ \mathit{MaxBallotAndVote}(a,\ i,\ b-1) \rangle : i \in \mathit{Instances}\} \rangle\} \\
& \land\ \text{UNCHANGED}\ \langle 1\mathit{amsgs},\ 2\mathit{amsgs},\ \mathit{vote},\ \mathit{leaderVote} \rangle
\end{aligned}
$$

$$
1\mathit{bMsgs}(b,\ Q) \triangleq \{m \in 1\mathit{bmsgs} : m[1] \in Q \land m[2] = b\}
$$

$$
\begin{aligned}
\mathit{MaxVote}(b,\ i,\ Q) \triangleq\ & \text{LET}\ \mathit{entries} \triangleq \text{UNION}\ \{m[3] : m \in 1\mathit{bMsgs}(b,\ Q)\} \\
& \phantom{\text{LET}}\ \mathit{ientries} \triangleq \{e \in \mathit{entries} : e[1] = i\} \\
& \phantom{\text{LET}}\ \mathit{maxVBal} \triangleq \mathit{Max}(\{e[2][1] : e \in \mathit{ientries}\},\ \leq) \\
& \text{IN}\ \ \text{CHOOSE}\ v \in \mathit{Values} \cup \{\mathit{None}\} : \exists\, e \in \mathit{ientries} : \land\ e[2][1] = \mathit{maxVBal} \\
& \phantom{\text{IN}\ \ \text{CHOOSE}\ v \in \mathit{Values} \cup \{\mathit{None}\} : \exists\, e \in \mathit{ientries} :}\ \land\ e[2][2] = v
\end{aligned}
$$

$$
\begin{aligned}
\mathit{LastInstance}(b,\ Q) \triangleq\ & \text{LET}\ \mathit{entries} \triangleq \text{UNION}\ \{m[3] : m \in 1\mathit{bMsgs}(b,\ Q)\} \\
& \phantom{\text{LET}}\ \mathit{valid} \triangleq \{e \in \mathit{entries} : e[2][1] \neq -1\} \\
& \text{IN}\ \ \text{IF}\ \mathit{valid} = \{\}\ \text{THEN}\ -1 \\
& \phantom{\text{IN}\ \ \text{IF}\ \mathit{valid} = \{\}}\ \text{ELSE}\ \ \mathit{Max}(\{e[1] : e \in \mathit{valid}\},\ \leq)
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Merge}(b) \triangleq\ & \land\ \exists\, Q \in \mathit{Quorums} : \\
& \qquad \land\ \forall\, a \in Q : \exists\, m \in 1\mathit{bMsgs}(b,\ Q) : m[1] = a \\
& \qquad \land\ \exists\, v \in \mathit{Values} : \mathit{leaderVote}' = [\mathit{leaderVote}\ \text{EXCEPT}\ ![b] = [i \in \mathit{Instances} \mapsto \\
& \qquad\qquad \text{IF}\ (i \in 1 \,..\, \mathit{LastInstance}(b,\ Q) \land \mathit{leaderVote}[b][i][1] = - \\
& \qquad\qquad\quad \text{THEN IF}\ \mathit{MaxVote}(i,\ b,\ Q) = \mathit{None}\ \text{THEN}\ \langle b,\ v \rangle \\
& \qquad\qquad\qquad\qquad \text{ELSE}\ \ \langle b,\ \mathit{MaxV} \\
& \qquad\qquad\quad \text{ELSE}\ \ \mathit{leaderVote}[b][i]]] \\
& \land\ \text{UNCHANGED}\ \langle \mathit{vote},\ \mathit{ballot},\ 1\mathit{amsgs},\ 1\mathit{bmsgs},\ 2\mathit{amsgs} \rangle
\end{aligned}
$$

$$
\begin{array}{l}
Propose(b,\ i) \triangleq \ \land\ leaderVote[b][i][1] = -1 \\
\qquad\qquad\ \land \exists\, Q \in Quorums : \\
\qquad\qquad\qquad \land \forall\, a \in Q : \exists\, m \in 1bMsgs(b,\ Q) : m[1] = a \\
\qquad\qquad\qquad \land \exists\, v \in Values : leaderVote' = [leaderVote \text{ EXCEPT } ![b][i] = \text{IF } MaxVote(b,\ i,\ Q) = Nor \\
\\
\qquad\qquad\ \land \text{UNCHANGED } \langle vote,\ ballot,\ 1amsgs,\ 1bmsgs,\ 2amsgs\rangle \\
\\
Phase2a(b,\ i) \triangleq \ \land\ leaderVote[b][i][1] = b \\
\qquad\qquad\ \land\ 2amsgs' = 2amsgs \cup \{\langle b,\ i,\ leaderVote[b][i]\rangle\} \\
\qquad\qquad\ \land \text{UNCHANGED } \langle ballot,\ vote,\ leaderVote,\ 1amsgs,\ 1bmsgs\rangle \\
\\
Phase2b(a,\ b,\ i) \triangleq \ \land\ ballot[a] \leq b \\
\qquad\qquad\ \land\ ballot' = [ballot \text{ EXCEPT } ![a] = b] \\
\qquad\qquad\ \land \exists\, m \in 2amsgs : \ \land\ m[2] = i \\
\qquad\qquad\qquad\qquad\qquad\qquad\ \land\ m[1] = b \\
\qquad\qquad\qquad\qquad\qquad\qquad\ \land\ vote' = [vote \text{ EXCEPT } ![a][i][b] = m[3][2]] \\
\qquad\qquad\ \land \text{UNCHANGED } \langle leaderVote,\ 1amsgs,\ 1bmsgs,\ 2amsgs\rangle \\
\\
Next \triangleq \\
\quad \lor\ \exists\, a \in Acceptors,\ b \in Ballots : IncreaseBallot(a,\ b) \\
\quad \lor\ \exists\, b \in Ballots : Phase1a(b) \\
\quad \lor\ \exists\, a \in Acceptors,\ b \in Ballots : Phase1b(a,\ b) \\
\quad \lor\ \exists\, b \in Ballots : Merge(b) \\
\quad \lor\ \exists\, b \in Ballots,\ i \in Instances : Propose(b,\ i) \\
\quad \lor\ \exists\, b \in Ballots,\ i \in Instances : Phase2a(b,\ i) \\
\quad \lor\ \exists\, a \in Acceptors,\ b \in Ballots,\ i \in Instances : Phase2b(a,\ b,\ i) \\
\\
Spec \triangleq\ Init \land \Box[Next]_{vars}
\end{array}
$$

$$
\begin{array}{l}
Conservative(i,\ b) \triangleq\ \forall\, a1,\ a2 \in Acceptors : \text{LET } v1 \triangleq\ vote[a1][i][b] \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ v2 \triangleq\ vote[a2][i][b] \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\ \text{IN}\quad (v1 \neq None \land v2 \neq None) \Rightarrow v1 = v2 \\
\\
ConservativeVoteArray \triangleq\ \forall\, i\ \in Instances : \forall\, b \in Ballots : Conservative(i,\ b) \\
\\
WellFormed \triangleq\ \forall\, a \in Acceptors : \forall\, i \in Instances : \forall\, b \in Ballots : \\
\quad b > ballot[a] \Rightarrow vote[a][i][b] \qquad = None \\
\\
VotedFor(a,\ i,\ b,\ v) \triangleq\ vote[a][i][b] = v \\
\\
ChosenAt(i,\ b,\ v) \triangleq \\
\quad \exists\, Q \in Quorums : \forall\, a \in Q : VotedFor(a,\ i,\ b,\ v) \\
\\
Chosen(i,\ v) \triangleq \\
\quad \exists\, b \in Ballots : ChosenAt(i,\ b,\ v) \\
\\
Choosable(v,\ i,\ b) \triangleq \\
\quad \exists\, Q \in Quorums : \forall\, a \in Q : ballot[a] > b \Rightarrow vote[a][i][b] = v
\end{array}
$$

$SafeAt(v,\ i,\ b) \triangleq$
$\quad \forall\, b2 \in Ballots : \forall\, v2 \in Values :$
$\qquad (b2 < b \land Choosable(v2,\ i,\ b2))$
$\qquad\ \Rightarrow v = v2$

$SafeInstanceVoteArray(i) \triangleq \forall\, b \in Ballots : \forall\, a \in Acceptors :$
$\quad$ LET $v \triangleq vote[a][i][b]$
$\quad$ IN $\quad v \neq None \Rightarrow SafeAt(v,\ i,\ b)$

$SafeVoteArray \triangleq \forall\, i \in Instances : SafeInstanceVoteArray(i)$

$Inv \triangleq TypeOK \land WellFormed \land SafeVoteArray \land ConservativeVoteArray$

$Correctness \triangleq$
$\quad \forall\, i \in Instances : \forall\, v1,\ v2 \in Values :$
$\qquad Chosen(i,\ v1) \land Chosen(i,\ v2) \Rightarrow v1 = v2$

\ * Modification History
\ * Last modified *Fri Jan* 15 16:29:36 *CST* 2021 by Dell
\ * Created *Wed Jan* 13 20:45:35 *CST* 2021 by Dell