MODULE *MultiPaxos*

EXTENDS *Integers*, *FiniteSets*

CONSTANTS *Acceptors*, *Nil*, *Value*

$Ballots \triangleq Nat$
$Instances \triangleq \{0, 1, 2, 3, 4, 5, 6\}$
$Quorums \triangleq \{Q \in \text{SUBSET } Acceptors : Cardinality(Q) > Cardinality(Acceptors)/2\}$
$Max(s) \triangleq \text{CHOOSE } x \in s : \forall\, y \in s : x \geq y$

VARIABLES *ballot*,
vote,
leaderVote,
$1a$*msgs*,
$1b$*msgs*,
$2a$*msgs*

$Init \triangleq$
$\land\ ballot = [a \in Acceptors \mapsto 0]$
$\land\ vote = [a \in Acceptors \mapsto$
$[i \in Instances \mapsto$
$[b \in Ballots \mapsto Nil]]]$
$\land\ 1amsgs = \{\}$
$\land\ 1bmsgs = \{\}$
$\land\ 2amsgs = \{\}$
$\land\ leaderVote = [b \in Ballots \mapsto [i \in Instances \mapsto \langle -1, Nil\rangle]]$

$allEntries \triangleq \{\langle i, \langle b, v\rangle\rangle : i \in Instances, b \in Ballots \cup \{-1\}, v \in Value \cup \{Nil\}\}$

$TypeInv \triangleq$
$\land\ ballot \in [Acceptors \to \{-1\} \cup Ballots]$
$\land\ leaderVote \in [Ballots \to [Instances \to (\{-1\} \cup Ballots) \times (\{Nil\} \cup Value)]]$
$\land\ vote \in [Acceptors \to [Instances \to [Ballots \to (\{Nil\} \cup Value)]]]$
$\land\ 1amsgs \subseteq \{\langle b\rangle : b \in Ballots\}$
$\land\ 1bmsgs \subseteq \{\langle b, e, a\rangle : b \in Ballots, a \in Acceptors, e \in \text{SUBSET } allEntries\}$
$\land\ 2amsgs \subseteq \{\langle b, i, \langle bb, v\rangle\rangle : i \in Instances, b \in Ballots,$
$bb \in Ballots, v \in Value \cup \{Nil\}\}$
$\land\ leaderVote \in [Ballots \to [Instances \to ((Ballots \cup \{-1\}) \times (\{Nil\} \cup Value))]]$

$IncreaseBallot(a, b) \triangleq$
$\land\ ballot[a] < b$
$\land\ ballot' = [ballot \text{ EXCEPT } ![a] = b]$

$\land$ UNCHANGED $\langle vote,\ leaderVote,\ 1amsgs,\ 1bmsgs,\ 2amsgs\rangle$

$Phase1a(b) \triangleq$
$\land\ 1amsgs' = 1amsgs \cup \{\langle b\rangle\}$
$\land$ UNCHANGED $\langle ballot,\ vote,\ leaderVote,\ 1bmsgs,\ 2amsgs\rangle$

$MaxAcceptorVote(a,\ i) \triangleq$
LET $maxBallot \triangleq Max(\{b \in Ballots : vote[a][i][b] \neq Nil\} \cup \{-1\})$
$v \triangleq$ IF $maxBallot > -1$ THEN $vote[a][i][maxBallot]$ ELSE Nil
IN $\langle maxBallot,\ v\rangle$

$Phase1b(a,\ b) \triangleq$
$\land\ ballot[a] < b$
$\land\ \langle b\rangle \in 1amsgs$
$\land\ ballot' = [ballot$ EXCEPT $![a] = b]$
$\land\ 1bmsgs' = 1bmsgs \cup$
$\{\langle b,\ \{\langle i,\ MaxAcceptorVote(a,\ i)\rangle : i \in Instances\},\ a\rangle\}$
$\land$ UNCHANGED $\langle vote,\ leaderVote,\ 1amsgs,\ 2amsgs\rangle$

$1bMsgs(b,\ Q) \triangleq$
$\{m \in 1bmsgs :\ m[3] \in Q\ \land m[1] = b\}$

$MaxVote(b,\ i,\ Q) \triangleq$
LET $entries \triangleq$ UNION $\{m[2] : m \in 1bMsgs(b,\ Q)\}$
$ientries \triangleq \{e \in entries : e[1] = i\}$
$maxBal \triangleq Max(\{e[2][1] : e \in ientries\})$
IN CHOOSE $v \in Value \cup \{Nil\}\ : \exists\, e \in ientries :$
$\land\ e[2][1] = maxBal \land e[2][2] = v$

$lastInstance(b,\ Q) \triangleq$ LET $entries \triangleq$ UNION $\{m[2] : m \in 1bMsgs(b,\ Q)\}$
$valid \triangleq \{e \in entries : e[2][1] \neq -1\}$
IN
IF $valid = \{\}$ THEN -1 ELSE $Max(\{e[1] : e \in valid\})$

$Merge(b) \triangleq \land \exists\, Q \in Quorums :$
$\land \forall\, a \in Q : \exists\, m \in 1bMsgs(b,\ Q) : m[3] = a$
$\land \exists\, v \in Value : leaderVote' = [leaderVote$ EXCEPT $![b] = [i \in Instances \mapsto$
IF $(i \in 0\,..\,lastInstance(b,\ Q) \land leaderVote[b][i][1] = -1)$
THEN IF $MaxVote(b,\ i,\ Q) = Nil$ THEN $\langle b,\ v\rangle$
ELSE $\langle b,\ MaxVote(b,\ i,\ Q)\rangle$
ELSE $leaderVote[b][i]]]$
$\land$ UNCHANGED $\langle vote,\ ballot,\ 1amsgs,\ 1bmsgs,\ 2amsgs\rangle$

$$
\begin{array}{l}
Propose(b,\, i) \triangleq \; \land\, leaderVote[b][i][1] = -1 \\
\qquad\qquad\qquad\quad \land\, \exists\, Q \in Quorums : \\
\qquad\qquad\qquad\qquad \land\, \forall\, a \in Q : \exists\, m \in 1bMsgs(b,\, Q) : m[3] = a \\
\qquad\qquad\qquad\qquad \land\, \exists\, v \in Value : leaderVote' = [leaderVote \text{ EXCEPT } ![b][i] = \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{IF } MaxVote(b,\, i,\, Q) = Nil \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{THEN } \langle b,\, v\rangle \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{ELSE } \langle b,\, MaxVote(b,\, i,\, Q)\rangle] \\
\qquad\qquad\quad \land \text{UNCHANGED } \langle vote,\, ballot,\, 1amsgs,\, 1bmsgs,\, 2amsgs\rangle
\end{array}
$$

$$
\begin{array}{l}
Phase2a(b,\, i) \triangleq \\
\quad \land \quad leaderVote[b][i][1] = b \\
\quad \land \quad 2amsgs' = 2amsgs \cup \{\langle b,\, i,\, leaderVote[b][i]\rangle\} \\
\quad \land \quad \text{UNCHANGED } \langle ballot,\, vote,\, leaderVote,\, 1amsgs,\, 1bmsgs\rangle
\end{array}
$$

$$
\begin{array}{l}
Vote(a,\, b,\, i) \triangleq \\
\quad \land\, ballot[a] \leq \; b \\
\quad \land\, ballot' = [ballot \text{ EXCEPT } ![a] = b] \\
\quad \land \; \exists\, m \in 2amsgs : \\
\qquad \land\, m[2] = i \land m[1] = b \\
\qquad \land\, vote' = [vote \text{ EXCEPT } ![a][i][b] = m[3][2]] \\
\quad \land \; \text{UNCHANGED } \langle leaderVote,\, 1amsgs,\, 1bmsgs,\, 2amsgs\rangle
\end{array}
$$

$$
\begin{array}{l}
Next \triangleq \\
\quad \lor \; \exists\, a \in Acceptors,\, b \in Ballots : IncreaseBallot(a,\, b) \\
\quad \lor \; \exists\, b \in Ballots : Phase1a(b) \\
\quad \lor \; \exists\, a \in Acceptors,\, b \in Ballots : Phase1b(a,\, b) \\
\quad \lor \; \exists\, b \in Ballots : Merge(b) \\
\quad \lor \; \exists\, b \in Ballots,\, i \in Instances : Propose(b,\, i) \\
\quad \lor \; \exists\, b \in Ballots,\, i \in Instances : Phase2a(b,\, i) \\
\quad \lor \; \exists\, a \in Acceptors,\, b \in Ballots,\, i \in Instances : Vote(a,\, b,\, i)
\end{array}
$$

$$
Spec \triangleq \; Init \land \Box[Next]_{\langle leaderVote,\, ballot,\, vote,\, 1amsgs,\, 1bmsgs,\, 2amsgs\rangle}
$$

$$
\begin{array}{l}
Conservative(i,\, b) \triangleq \\
\quad \forall\, a1,\, a2 \in Acceptors : \\
\qquad \text{LET } v1 \triangleq \; vote[a1][i][b] \\
\qquad\quad\; v2 \triangleq \; vote[a2][i][b] \\
\qquad \text{IN} \quad\; (v1 \neq Nil \land v2 \neq Nil) \Rightarrow v1 = v2
\end{array}
$$

$$
\begin{array}{l}
ConservativeVoteArray \triangleq \\
\quad \forall\, i \in Instances : \forall\, b \in Ballots : \\
\qquad Conservative(i,\, b)
\end{array}
$$

$$
\begin{array}{l}
WellFormed \triangleq \; \forall\, a \in Acceptors : \forall\, i \in Instances : \forall\, b \in Ballots : \\
\quad b > ballot[a] \Rightarrow vote[a][i][b] \qquad = Nil
\end{array}
$$

$$
VotedFor(a,\, i,\, b,\, v) \triangleq \; vote[a][i][b] = v
$$

$ChosenAt(i,\ b,\ v) \triangleq$
$\quad \exists\, Q \in Quorums : \forall\, a \in Q : VotedFor(a,\ i,\ b,\ v)$

$Chosen(i,\ v) \triangleq$
$\quad \exists\, b \in Ballots : ChosenAt(i,\ b,\ v)$

$Choosable(v,\ i,\ b) \triangleq$
$\quad \exists\, Q \in Quorums : \forall\, a \in Q : ballot[a] > b \Rightarrow vote[a][i][b] = v$

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

$SafeInstanceVoteArray(i) \triangleq \forall\, b \in Ballots : \forall\, a \in Acceptors :$
$\quad$ LET $v \triangleq vote[a][i][b]$
$\quad$ IN $\quad v \neq Nil \Rightarrow SafeAt(v,\ i,\ b)$

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

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

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

* Modification History
* Last modified *Fri Sep* 11 15:36:28 *CST* 2020 by 15150