MODULE *multipaxos*

EXTENDS *Integers*, *FiniteSets*

CONSTANTS *Acceptors*, *Nil*

$Value \triangleq Nat$

$Ballots \triangleq Nat$
$Instances \triangleq Nat$

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

$Max(s) \triangleq \text{CHOOSE } x \in s : \forall\, y \in s : x \geq y$

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

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

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

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

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

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

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

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

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

$$
\begin{array}{l}
MaxVote(b,\ i,\ Q)\ \triangleq \\
\quad \text{LET } entries \triangleq \text{UNION } \{m[2] : m \in 1bMsgs(b,\ Q)\} \\
\qquad ientries \triangleq \{e \in entries : e[1] = i\} \\
\qquad maxBal \triangleq Max(\{e[2][1] : e \in ientries\}) \\
\quad \text{ATTENTIION!} \\
\quad \text{IN } \ \text{CHOOSE } v \in Value \cup \{Nil\} \cup 0\,..\,100 : \exists\, e \in ientries : \\
\qquad \land\ \ e[2][1] = maxBal \land e[2][2] = v
\end{array}
$$

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

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

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

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

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

$Next \triangleq$
$\quad \lor\ \exists\, a \in Acceptors,\ b \in Ballots : IncreaseBallot(a,\ b)$
$\quad \lor\ \exists\, b \in Ballots : Phase1a(b)$
$\quad \lor\ \exists\, a \in Acceptors,\ b \in Ballots : Phase1b(a,\ b)$
$\quad \lor\ \exists\, b \in Ballots : Merge(b)$
$\quad \lor\ \exists\, b \in Ballots,\ i \in Instances : Propose(b,\ i)$
$\quad \lor\ \exists\, b \in Ballots,\ i \in Instances : Phase2a(b,\ i)$
$\quad \lor\ \exists\, a \in Acceptors,\ b \in Ballots,\ i \in Instances : Vote(a,\ b,\ i)$

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

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

$ConservativeVoteArray \triangleq$
$\quad \forall\, i \in Instances : \forall\, b \in Ballots :$
$\qquad Conservative(i,\ b)$

$WellFormed \triangleq\ \forall\, a \in Acceptors : \forall\, i \in Instances : \forall\, b \in Ballots :$
$\quad b > ballot[a] \Rightarrow vote[a][i][b] \qquad = Nil$

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

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

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

$Choosable(v,\ i,\ b) \triangleq$

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

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

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

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

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

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

---

* Modification History
* Last modified *Tue Apr* 21 22:27:55 *CST* 2020 by *assstriker*
* Created *Thu Mar* 19 18:02:10 *CST* 2020 by *assstriker*