MODULE $RL - Paxos$

EXTENDS *Integers*, *FiniteSets*

CONSTANTS *Acceptors*, *Nil*, *Value*, *BMax*, *W*, *CongestedSet*

$Ballots \triangleq 0 \,..\, BMax$

$Instances \triangleq \{0, 1, 2, 3, 4, 5, 6\}$

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

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

VARIABLES

ballot,
vote,
leaderVote,
$1a$*msgs*,
$1b$*msgs*,
$2a$*msgs*,
status, *[$i \in Instances \to \{Init, Accepted, Committed, Executed\}$]
commitQ, *[$i \in Instances \to$ SUBSET *Acceptors*]
execute, **Nat*
Commute, *[$i \in Instances \to$ BOOLEAN]
$p2b$*msgs*, *SUBSET (Instances × *Acceptors*)
commitMsgs, *SUBSET *Instances*
$p2b2c$ *SUBSET (*Instances* × *Acceptors*): P2b → coordinator

---

$Init \triangleq$
$\wedge\ ReqOf = [i \in Instances \mapsto Nil]$
$\wedge\ ballot = [a \in Acceptors \mapsto 0]$
$\wedge\ vote = [a \in Acceptors \mapsto$
$\quad [i \in Instances \mapsto$
$\quad\quad [b \in Ballots \mapsto Nil]]]$
$\wedge\ 1amsgs = \{\}$
$\wedge\ 1bmsgs = \{\}$
$\wedge\ 2amsgs = \{\}$
$\wedge\ leaderVote = [b \in Ballots \mapsto [i \in Instances \mapsto \langle -1, Nil\rangle]]$
$\wedge\ status = [i \in Instances \mapsto$ "Init"$]$
$\wedge\ commitQ = [i \in Instances \mapsto \{\}]$
$\wedge\ execute = 0$
$\wedge\ Commute = [i \in Instances \mapsto$ FALSE$]$
$\wedge\ p2bmsgs = \{\}$
$\wedge\ commitMsgs = \{\}$
$\wedge\ p2b2c = \{\}$

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

$TypeInv \triangleq$
$\wedge\ ballot \in [Acceptors \to \{-1\} \cup Ballots]$
$\wedge\ leaderVote \in [Ballots \to [Instances \to (\{-1\} \cup Ballots) \times (\{Nil\} \cup Value)]]$
$\wedge\ vote \in [Acceptors \to [Instances \to\ [Ballots \to (\{Nil\} \cup Value)]]]$

$\land\ 1amsgs \subseteq \{\langle b \rangle : b \in Ballots\}$
$\land\ 2amsgs \subseteq \{\langle b,\ i,\ \langle bb,\ v \rangle \rangle : i \in Instances,\ b \in Ballots,\ bb \in Ballots,\ v \in Value \cup \{Nil\}\}$

$\land\ leaderVote \in [Ballots \to [Instances \to ((Ballots \cup \{-1\}) \times (\{Nil\} \cup Value))]]$
$\land\ status \in [Instances \to \{\text{"Init"},\ \text{"Accepted"},\ \text{"Committed"},\ \text{"Executed"}\}]$
$\land\ commitQ\ \in [Instances \to \text{SUBSET}\ Acceptors]$
$\land\ execute\ \ \in Nat$
$\land\ Commute \in [Instances \to \text{BOOLEAN}\ ]$
$\land\ p2bmsgs \subseteq (Instances \times Acceptors)$
$\land\ commitMsgs \subseteq Instances$
$\land\ p2b2c \subseteq (Instances \times Acceptors)$

$IncreaseBallot(a,\ b)\ \triangleq$
$\land\ ballot[a] < b$
$\land\ ballot' = [ballot\ \text{EXCEPT}\ ![a] = b]$
$\land\ \text{UNCHANGED}\ \langle vote,\ leaderVote,\ 1amsgs,\ 1bmsgs,\ 2amsgs,$
$status,\ commitQ,\ execute,\ Commute,\ p2bmsgs,\ commitMsgs,\ p2b2c\rangle$

$Phase1a(b)\ \triangleq$
$\land\ 1amsgs' = 1amsgs \cup \{\langle b \rangle\}$
$\land\ \text{UNCHANGED}\ \langle ballot,\ vote,\ leaderVote,\ 1bmsgs,\ 2amsgs,$
$status,\ commitQ,\ execute,\ Commute,\ p2bmsgs,\ commitMsgs,\ p2b2c\rangle$

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

$Phase1b(a,\ b)\ \triangleq$
$\land\ ballot[a] < b$
$\land\ \langle b \rangle \in 1amsgs$
$\land\ ballot' = [ballot\ \text{EXCEPT}\ ![a] = b]$
$\land\ 1bmsgs' = 1bmsgs \cup$
$\{\langle b,\ \{\langle i,\ MaxAcceptorVote(a,\ i)\rangle : i \in Instances\},\ a\rangle\}$
$\land\ \text{UNCHANGED}\ \langle vote,\ leaderVote,\ 1amsgs,\ 2amsgs,$
$status,\ commitQ,\ execute,\ Commute,\ p2bmsgs,\ commitMsgs,\ p2b2c\rangle$

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

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

$Merge(b)\ \triangleq\ \land \exists\, Q \in Quorums :$

$\land \forall\, a \in Q : \exists\, m \in 1bMsgs(b,\, Q) : m[3] = a$
$\land \exists\, v \in Value : leaderVote' = [leaderVote \text{ EXCEPT } ![b] = [i \in Instances \mapsto$
IF $(i \in 0\,..\,lastInstance(b,\, Q) \land leaderVote[b][i][1] = -1)$
THEN $\langle b,\, MaxVote(b,\, i,\, Q)\rangle$
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 $\langle vote,\, ballot,\, 1amsgs,\, 1bmsgs,\, 2amsgs,$
$status,\, commitQ,\, execute,\, Commute,\, p2bmsgs,\, commitMsgs,\, p2b2c\rangle$

$Propose(b,\, i) \triangleq \land leaderVote[b][i][1] = -1$
$\land \exists\, Q \in Quorums :$
$\land \forall\, a \in Q : \exists\, m \in 1bMsgs(b,\, Q) : m[3] = a$
$\land \exists\, v \in Value :$
$leaderVote' = [leaderVote \text{ EXCEPT } ![b][i] = \text{IF } MaxVote(b, i, Q) = Nil$
THEN $\langle b, v\rangle$
ELSE $\langle b, MaxVote(b, i, Q)\rangle]$
$\land$ UNCHANGED $\langle vote,\, ballot,\, 1amsgs,\, 1bmsgs,\, 2amsgs,$
$status,\, commitQ,\, execute,\, Commute,\, p2bmsgs,\, commitMsgs,\, p2b2c\rangle$

$SetCommuteFlag(b,\, i,\, r) \triangleq$
$\exists\, flag \in \text{BOOLEAN} :$
$\land Commute' = [Commute \text{ EXCEPT } ![i] = flag]$

$Phase2a(b,\, i) \triangleq$
$\land leaderVote[b][i][1] = b$
$\land$ LET $r \triangleq leaderVote[b][i][2]$
IN $SetCommuteFlag(b,\, i,\, r)$
$\land \quad 2amsgs' = 2amsgs \cup \{\langle b,\, i,\, \langle b,\, r\rangle\rangle\}$
$\land$ UNCHANGED $\langle ballot,\, vote,\, leaderVote,\, 1amsgs,\, 1bmsgs,\, status,\, commitQ,\, execute,\, p2bmsgs,$
$commitMsgs,\, p2b2c\rangle$

$Vote(a,\, b,\, i) \triangleq$
$\exists\, m \in 2amsgs :$
$\land m[1] = b$
$\land m[2] = i$
$\land ballot[a] \leq b$
$\land ballot' = [ballot \text{ EXCEPT } ![a] = b]$
$\land vote' = [vote \quad \text{EXCEPT } ![a][i][b] = m[3][2]]$
$\land$ IF $a \in CongestedSet$
THEN $\land p2b2c' = p2b2c \cup \{\langle i,\, a\rangle\} \quad p2b2c$
$\land p2bmsgs' = p2bmsgs$
ELSE $\land p2bmsgs' = p2bmsgs \cup \{\langle i,\, a\rangle\} \; p2bmsgs$
$\land p2b2c' = p2b2c$
$\land$ UNCHANGED $\langle leaderVote,\, 1amsgs,\, 1bmsgs,\, 2amsgs,\, status,\, commitQ,\, execute,$
$Commute,\, commitMsgs\rangle$

$InCCW(i) \triangleq (execute \leq i) \land (i \leq execute + W)$

$CP2bCommon(i,\, a,\, cq) \triangleq$

$\land \langle i,\ a\rangle \in p2bmsgs$
$\land commitQ' = [commitQ \text{ EXCEPT } ![i] = cq]$
$\land$ UNCHANGED $\langle p2bmsgs,\ ballot,\ vote,\ leaderVote,\ 1amsgs,\ 1bmsgs,\ 2amsgs,\ Commute,$
$commitMsgs,\ p2b2c\rangle$

$CP2bCommitOnly(i,\ a) \triangleq$
LET $cq \triangleq commitQ[i] \cup \{a\}$
LET $committed \triangleq \exists\, Q \in Quorums : Q \subseteq cq$
IN $\land committed$
$\land \neg(i = execute) \land \neg((Commute[i] = \text{TRUE}) \land InCCW(i))$
$\land status' = [status \text{ EXCEPT } ![i] = \text{“Committed”}]$
$\land$ UNCHANGED $execute$
$\land CP2bCommon(i,\ a,\ cq)$

$CP2bSeqExec(i,\ a) \triangleq$
LET $cq \triangleq commitQ[i] \cup \{a\}$
LET $committed \triangleq \exists\, Q \in Quorums : Q \subseteq cq$
IN $\land committed$
$\land i = execute$
$\land status' = [status \text{ EXCEPT } ![i] = \text{“Executed”}]$
$\land execute' = execute + 1$
$\land CP2bCommon(i,\ a,\ cq)$

$CP2bOOEExec(i,\ a) \triangleq$
LET $cq \triangleq commitQ[i] \cup \{a\}$
LET $committed \triangleq \exists\, Q \in Quorums : Q \subseteq cq$
IN $\land committed$
$\land (Commute[i] = \text{TRUE}) \land InCCW(i) \land i \neq execute$
$\land status' = [status \text{ EXCEPT } ![i] = \text{“Executed”}]$
$\land$ UNCHANGED $execute$
$\land CP2bCommon(i,\ a,\ cq)$

$CP2bNotCommitted(i,\ a) \triangleq$
LET $cq \triangleq commitQ[i] \cup \{a\}$
LET $committed \triangleq \exists\, Q \in Quorums : Q \subseteq cq$
IN $\land \neg committed$
$\land status' = status$
$\land$ UNCHANGED $execute$
$\land CP2bCommon(i,\ a,\ cq)$

$CollectP2b(i) \triangleq$
$\exists\, a \in Acceptors : CP2bSeqExec(i,\ a) \lor CP2bOOEExec(i,\ a) \lor CP2bCommitOnly(i,\ a)$
$\lor CP2bNotCommitted(i,\ a)$

$CoordGather(i) \triangleq$
$\land$ LET $S \triangleq \{a \in Acceptors : \langle i,\ a\rangle \in p2b2c\}$
IN $\exists\, Q \in Quorums : Q \subseteq S$
$\land commitMsgs' = commitMsgs \cup \{i\}$
$\land$ CASE $status[i] = \text{“Executed”} \to$
$\land$ UNCHANGED $\langle status,\ execute\rangle$
$[\ ]\, i = execute \to$
$\land status' = [status \text{ EXCEPT } ![i] = \text{“Executed”}]$

$\land\ execute' = execute + 1$
$[\ ](Commute[i] = \text{TRUE}) \land InCCW(i) \land i \neq execute \rightarrow$
$\land\ status' = [status\ \text{EXCEPT}\ ![i] = \text{“Executed”}]$
$\land\ \text{UNCHANGED}\ execute$
$[\ ]\text{OTHER}\ \rightarrow$
$\land\ status' = [status\ \text{EXCEPT}\ ![i] = \text{“Committed”}]$
$\land\ \text{UNCHANGED}\ execute$
$\land\ \text{UNCHANGED}\ \langle commitQ,\ Commute,\ ballot,\ vote,\ leaderVote,\ 1amsgs,\ 1bmsgs,\ 2amsgs,\ p2bmsgs,\ p2b2c\rangle$

$Phase3Deliver(i)\ \triangleq$
$\land\ i \in commitMsgs$
$\land\ \text{CASE}\ status[i] = \text{“Executed”} \rightarrow$
$\land\ \text{UNCHANGED}\ \langle status,\ execute\rangle$
$[\ ]status[i] = \text{“Committed”} \land i \neq execute \land \neg((Commute[i] = \text{TRUE}) \land InCCW(i)) \rightarrow$
$\land\ \text{UNCHANGED}\ \langle status,\ execute\rangle$
$[\ ]i = execute \rightarrow$
$\land\ status' = [status\ \text{EXCEPT}\ ![i] = \text{“Executed”}]$
$\land\ execute' = execute + 1$
$[\ ](Commute[i] = \text{TRUE}) \land InCCW(i) \land i \neq execute \rightarrow$
$\land\ status' = [status\ \text{EXCEPT}\ ![i] = \text{“Executed”}]$
$\land\ \text{UNCHANGED}\ execute$
$[\ ]\text{OTHER}\ \rightarrow$
$\land\ status' = [status\ \text{EXCEPT}\ ![i] = \text{“Committed”}]$
$\land\ \text{UNCHANGED}\ execute$
$\land\ commitMsgs' = commitMsgs \setminus \{i\}$
$\land\ \text{UNCHANGED}\ \langle commitQ,\ Commute,\ ballot,\ vote,\ leaderVote,\ 1amsgs,\ 1bmsgs,\ 2amsgs,\ p2bmsgs,\ p2b2c\rangle$

$Next\ \triangleq$
$\lor\ \exists\, a \in Acceptors,\ b \in Ballots : IncreaseBallot(a,\ b)$
$\lor\ \exists\, b \in Ballots : Phase1a(b)$
$\lor\ \exists\, a \in Acceptors,\ b \in Ballots : Phase1b(a,\ b)$
$\lor\ \exists\, b \in Ballots : Merge(b)$
$\lor\ \exists\, b \in Ballots,\ i \in Instances : Propose(b,\ i)$
$\lor\ \exists\, b \in Ballots,\ i \in Instances : Phase2a(b,\ i)$
$\lor\ \exists\, a \in Acceptors,\ b \in Ballots,\ i \in Instances : Vote(a,\ b,\ i)$
$\lor\ \exists\, i \in Instances : CollectP2b(i)$ broadcast path
$\lor\ \exists\, i \in Instances : CoordGather(i)$ enhanced commit path
$\lor\ \exists\, i \in Instances : Phase3Deliver(i)$ acceptor receive $P3(i)$ ¡ú *Committed*
$\lor\ \exists\, i \in Instances : InOrderExec(i) \lor OOE(i)$

$Spec\ \triangleq$
$Init \land \Box[Next]\langle leaderVote,\ ballot,\ vote,\ 1amsgs,\ 1bmsgs,\ 2amsgs,\ status,\ commitQ,\ execute,\ Commute,\ p2bmsgs,\ commitMsgs,\ p2b2c\rangle$

$Liveness\ \triangleq$
$\forall\, i \in Instances :$
$\Box(status[i] = \text{“Committed”} \Rightarrow \Diamond(status[i] = \text{“Executed”}))$

$Conservative(i,\ b)\ \triangleq$

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

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

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

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

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

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

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

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

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

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

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

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