MODULE *PaxosCommit*

EXTENDS *Integers*

$Maximum(S) \triangleq$

$\quad$ IF $S = \{\}$ THEN -1
$\qquad\qquad$ ELSE CHOOSE $n \in S : \forall\, m \in S : n \geq m$

CONSTANT $RM,\quad$ The set of resource managers.
$\qquad Acceptor,\quad$ The set of acceptors.
$\qquad Majority,\quad$ The set of majorities of acceptors
$\qquad Ballot\quad$ The set of ballot numbers

ASSUME

$\land\ Ballot \subseteq Nat$
$\land\ 0 \in Ballot$
$\land\ Majority \subseteq \textsc{subset}\ Acceptor$
$\land\ \forall\, MS1,\ MS2 \in Majority : MS1 \cap MS2 \neq \{\}$

$Messages \triangleq$

$[type : \{\text{"phase1a"}\},\ ins : RM,\ bal : Ballot \setminus \{0\}]$
$\quad\cup$
$[type : \{\text{"phase1b"}\},\ ins : RM,\ mbal : Ballot,\ bal : Ballot \cup \{-1\},$
$\ val : \{\text{"prepared"},\ \text{"aborted"},\ \text{"none"}\},\ acc : Acceptor]$
$\quad\cup$
$[type : \{\text{"phase2a"}\},\ ins : RM,\ bal : Ballot,\ val : \{\text{"prepared"},\ \text{"aborted"}\}]$
$\quad\cup$
$[type : \{\text{"phase2b"}\},\ acc : Acceptor,\ ins : RM,\ bal : Ballot,$
$\ val : \{\text{"prepared"},\ \text{"aborted"}\}]$
$\quad\cup$
$[type : \{\text{"Commit"},\ \text{"Abort"}\}]$

VARIABLES

$rmState,\quad$ $rmState[r]$ is the state of resource manager r.
$aState,\quad$ $aState[ins][ac]$ is the state of acceptor ac for instance ins of the *Paxos* algorithm.
$msgs\quad$ The set of all messages ever sent.

$PCTypeOK \triangleq$

$\land\ rmState \in [RM \rightarrow \{\text{"working"},\ \text{"prepared"},\ \text{"committed"},\ \text{"aborted"}\}]$
$\land\ aState \quad \in [RM \rightarrow [Acceptor \rightarrow [mbal : Ballot,$
$\qquad\qquad\qquad\qquad\qquad\qquad bal \quad : Ballot \cup \{-1\},$
$\qquad\qquad\qquad\qquad\qquad\qquad val \quad : \{\text{"prepared"},\ \text{"aborted"},\ \text{"none"}\}]]]$
$\land\ msgs \subseteq Messages$

```
PCInit ≜    The initial predicate.
  ∧ rmState = [r ∈ RM ↦ "working"]
  ∧ aState  = [r ∈ RM ↦
                 [ac ∈ Acceptor
                     ↦ [mbal ↦ 0, bal  ↦  − 1, val  ↦ "none"]]]
  ∧ msgs = {}

Send(m) ≜ msgs′ = msgs ∪ {m}

RMPrepare(r) ≜
  ∧ rmState[r] = "working"
  ∧ rmState′ = [rmState EXCEPT ![r] = "prepared"]
  ∧ Send([type ↦ "phase2a", ins ↦ r, bal ↦ 0, val ↦ "prepared"])
  ∧ UNCHANGED aState

RMChooseToAbort(r) ≜
  ∧ rmState[r] = "working"
  ∧ rmState′ = [rmState EXCEPT ![r] = "aborted"]
  ∧ Send([type ↦ "phase2a", ins ↦ r, bal ↦ 0, val ↦ "aborted"])
  ∧ UNCHANGED aState

RMRcvCommitMsg(r) ≜
  ∧ [type ↦ "Commit"] ∈ msgs
  ∧ rmState′ = [rmState EXCEPT ![r] = "committed"]
  ∧ UNCHANGED ⟨aState, msgs⟩

RMRcvAbortMsg(r) ≜
  ∧ [type ↦ "Abort"] ∈ msgs
  ∧ rmState′ = [rmState EXCEPT ![r] = "aborted"]
  ∧ UNCHANGED ⟨aState, msgs⟩

Phase1a(bal, r) ≜
  ∧ Send([type ↦ "phase1a", ins ↦ r, bal ↦ bal])
  ∧ UNCHANGED ⟨rmState, aState⟩

Phase2a(bal, r) ≜
  ∧ ¬∃ m ∈ msgs : ∧ m.type = "phase2a"
                  ∧ m.bal = bal
                  ∧ m.ins = r
  ∧ ∃ MS ∈ Majority :
      LET mset ≜ {m ∈ msgs : ∧ m.type  = "phase1b"
                             ∧ m.ins   = r
                             ∧ m.mbal = bal
                             ∧ m.acc   ∈ MS}
          maxbal ≜ Maximum({m.bal : m ∈ mset})
          val ≜ IF maxbal = − 1
                  THEN "aborted"
```

```
                         $\text{ELSE}\ \ (\text{CHOOSE}\ m \in mset : m.bal = maxbal).val$
          $\text{IN}\quad \land \forall\, ac \in MS : \exists\, m \in mset : m.acc = ac$
                $\land\ Send([type \mapsto \text{“phase2a”},\ ins \mapsto r,\ bal \mapsto bal,\ val \mapsto val])$
    $\land\ \text{UNCHANGED}\ \langle rmState,\ aState \rangle$

$PCDecide\ \triangleq$
    $\land\ \text{LET}\ Decided(r,\ v)\ \triangleq$
              $\exists\, b \in Ballot,\ MS \in Majority :$
                $\forall\, ac \in MS : [type \mapsto \text{“phase2b”},\ ins \mapsto r,$
                                  $bal \mapsto b,\ val \mapsto v,\ acc \mapsto ac] \in msgs$
       $\text{IN}\quad \lor\ \land \forall\, r \in RM : Decided(r,\ \text{“prepared”})$
                $\land\ Send([type \mapsto \text{“Commit”}])$
              $\lor\ \land \exists\, r \in RM : Decided(r,\ \text{“aborted”})$
                $\land\ Send([type \mapsto \text{“Abort”}])$
    $\land\ \text{UNCHANGED}\ \langle rmState,\ aState \rangle$

$Phase1b(acc)\ \triangleq$
    $\exists\, m \in msgs :$
      $\land\ m.type = \text{“phase1a”}$
      $\land\ aState[m.ins][acc].mbal < m.bal$
      $\land\ aState' = [aState\ \text{EXCEPT}\ ![m.ins][acc].mbal = m.bal]$
      $\land\ Send([type\ \ \mapsto \text{“phase1b”},$
                 $ins\ \ \ \mapsto m.ins,$
                 $mbal \mapsto m.bal,$
                 $bal\ \ \ \mapsto aState[m.ins][acc].bal,$
                 $val\ \ \ \mapsto aState[m.ins][acc].val,$
                 $acc\ \ \ \mapsto acc])$
      $\land\ \text{UNCHANGED}\ rmState$

$Phase2b(acc)\ \triangleq$
    $\land\ \exists\, m \in msgs :$
         $\land\ m.type = \text{“phase2a”}$
         $\land\ aState[m.ins][acc].mbal \leq m.bal$
         $\land\ aState' = [aState\ \text{EXCEPT}\ ![m.ins][acc].mbal = m.bal,$
                                        $![m.ins][acc].bal\ \ \ = m.bal,$
                                        $![m.ins][acc].val\ \ \ = m.val]$
         $\land\ Send([type \mapsto \text{“phase2b”},\ ins \mapsto m.ins,\ bal \mapsto m.bal,$
                    $val \mapsto m.val,\ acc \mapsto acc])$
    $\land\ \text{UNCHANGED}\ rmState$

$PCNext\ \triangleq$    The next-state action
    $\lor\ \exists\, r \in RM :\ \lor\ RMPrepare(r)$
                     $\lor\ RMChooseToAbort(r)$
                     $\lor\ RMRcvCommitMsg(r)$
                     $\lor\ RMRcvAbortMsg(r)$
```

$$
\begin{array}{l}
\quad \lor \exists\, bal \in Ballot \setminus \{0\},\ r \in RM : Phase1a(bal,\ r) \lor Phase2a(bal,\ r) \\
\quad \lor PCDecide \\
\quad \lor \exists\, acc \in Acceptor : Phase1b(acc) \lor Phase2b(acc)
\end{array}
$$

$$PCSpec \ \triangleq\ PCInit \land \Box[PCNext]_{\langle rmState,\ aState,\ msgs \rangle}$$

THEOREM $PCSpec \Rightarrow \Box PCTypeOK$

INSTANCE $TCommit$

THEOREM $PCSpec \Rightarrow TCSpec$