MODULE *PaxosMadeSimple*

A specification of the algorithm described in *Paxos* Made Simple. This specification is a modification of: https://lamport.azurewebsites.net/tla/PConProof.tla Look there for comments.

EXTENDS *Integers*, *FiniteSets*

CONSTANT *Value*, *Acceptor*, *Quorum*

ASSUME $QA \triangleq \land \forall\, Q \in Quorum : Q \subseteq Acceptor$
$\land \forall\, Q1,\, Q2 \in Quorum : Q1 \cap Q2 \neq \{\}$

$Ballot \triangleq Nat$

ASSUME $BallotAssump \triangleq (Ballot \cup \{-1\}) \cap Acceptor = \{\}$

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

$Message \triangleq [type : \{\text{“1a”}\},\, bal : Ballot]$
$\cup\ [type : \{\text{“1b”}\},\, acc : Acceptor,\, bal : Ballot,$
$mbal : Ballot \cup \{-1\},\, mval : Value \cup \{None\}]$
$\cup\ [type : \{\text{“2a”}\},\, bal : Ballot,\, val : Value]$
$\cup\ [type : \{\text{“2b”}\},\, acc : Acceptor,\, bal : Ballot,\, val : Value]$

--algorithm *PCon*{
variables $maxBal = [a \in Acceptor \mapsto -1]$,
$maxVBal = [a \in Acceptor \mapsto -1]$,
$maxVVal = [a \in Acceptor \mapsto None]$,
$msgs = \{\}$
define {
$sentMsgs(t,\, b) \triangleq \{m \in msgs : (m.type = t) \land (m.bal = b)\}$

$ShowsSafeAt(Q,\, b,\, v) \triangleq$
LET $Q1b \triangleq \{m \in sentMsgs(\text{“1b”},\, b) : m.acc \in Q\}$
IN $\land \forall\, a \in Q : \exists\, m \in Q1b : m.acc = a$
$\land \lor \forall\, m \in Q1b : m.mbal = -1$
$\lor \exists\, m \in Q1b :$
$\land\, m.mval = v$
$\land \forall\, m1 \in Q1b : m1.mbal \leq m.mbal$
}

macro $Phase1a()\{msgs := msgs \cup \{[type \mapsto \text{“1a”},\, bal \mapsto self]\}$; }

macro $Phase1b(b)\{$
when $b > maxBal[self] \land sentMsgs(\text{“1a”},\, b) \neq \{\}$;
$maxBal[self] := b$;
$msgs := msgs \cup \{[type \mapsto \text{“1b”},\, acc \mapsto self,\, bal \mapsto b,$
$mbal \mapsto maxVBal[self],\, mval \mapsto maxVVal[self]]\}$;
}

```
  macro Phase2a(v){
    when  ∧ sentMsgs("2a", self) = {}
          ∧ ∃ Q ∈ Quorum : ShowsSafeAt(Q, self, v) ;
    msgs := msgs ∪ {[type ↦ "2a", bal ↦ self, val ↦ v]} ;
   }

  macro Phase2b(b){
    when b ≥ maxBal[self] ;
    with (m ∈ sentMsgs("2a", b)){
        maxBal[self] := b ;
        maxVBal[self] := b ;
        maxVVal[self] := m.val ;
        msgs := msgs ∪ {[type ↦ "2b", acc ↦ self, bal ↦ b, val ↦ m.val]}
    }
   }

  process (acceptor ∈ Acceptor){
    acc: while (TRUE){
           with (b ∈ Ballot){either Phase1b(b)or Phase2b(b) }}
   }

  process (leader ∈ Ballot){
    ldr: while (TRUE){
          either Phase1a()
          or     with (v ∈ Value){Phase2a(v)}
         }
   }
}
```

BEGIN TRANSLATION ($chksum(pcal) =$ "39408c33" $\wedge\ chksum(tla) =$ "ed3338c5")

VARIABLES $maxBal,\ maxVBal,\ maxVVal,\ msgs$

define statement

$$sentMsgs(t,\ b) \triangleq \{m \in msgs : (m.type = t) \wedge (m.bal = b)\}$$

$$\begin{array}{l} ShowsSafeAt(Q,\ b,\ v) \triangleq \\ \quad \text{LET } Q1b \triangleq \{m \in sentMsgs(\text{"1b"},\ b) : m.acc \in Q\} \\ \quad \text{IN } \ \wedge \forall\, a \in Q : \exists\, m \in Q1b : m.acc = a \\ \qquad\quad \wedge\ \vee \forall\, m \in Q1b : m.mbal = -1 \\ \qquad\qquad\ \ \vee \exists\, m \in Q1b : \\ \qquad\qquad\qquad \wedge\, m.mval = v \\ \qquad\qquad\qquad \wedge \forall\, m1 \in Q1b : m1.mbal \leq m.mbal \end{array}$$

$$vars \triangleq \langle maxBal,\ maxVBal,\ maxVVal,\ msgs\rangle$$

$$ProcSet \triangleq (Acceptor) \cup (Ballot)$$

$$
\begin{array}{l}
Init \triangleq \quad \text{Global variables} \\
\qquad \land\, maxBal = [a \in Acceptor \mapsto -1] \\
\qquad \land\, maxVBal = [a \in Acceptor \mapsto -1] \\
\qquad \land\, maxVVal = [a \in Acceptor \mapsto None] \\
\qquad \land\, msgs = \{\}
\end{array}
$$

$$
\begin{array}{l}
acceptor(self) \triangleq\ \exists\, b \in Ballot : \\
\qquad \lor\ \land\, b > maxBal[self] \land sentMsgs(\text{“1a”},\, b) \neq \{\} \\
\qquad\quad \land\, maxBal' = [maxBal \text{ EXCEPT } ![self] = b] \\
\qquad\quad \land\, msgs' = (msgs \cup \{[type \mapsto \text{“1b”},\, acc \mapsto self,\, bal \mapsto b, \\
\qquad\qquad\qquad\qquad mbal \mapsto maxVBal[self],\, mval \mapsto maxVVal[self]]\}) \\
\qquad\quad \land \text{ UNCHANGED } \langle maxVBal,\, maxVVal\rangle \\
\qquad \lor\ \land\, b \geq maxBal[self] \\
\qquad\quad \land\, \exists\, m \in sentMsgs(\text{“2a”},\, b) : \\
\qquad\qquad \land\, maxBal' = [maxBal \text{ EXCEPT } ![self] = b] \\
\qquad\qquad \land\, maxVBal' = [maxVBal \text{ EXCEPT } ![self] = b] \\
\qquad\qquad \land\, maxVVal' = [maxVVal \text{ EXCEPT } ![self] = m.val] \\
\qquad\qquad \land\, msgs' = (msgs \cup \{[type \mapsto \text{“2b”},\, acc \mapsto self,\, bal \mapsto b,\, val \mapsto m.val]\})
\end{array}
$$

$$
\begin{array}{l}
leader(self) \triangleq\ \land\ \lor\ \land\, msgs' = (msgs \cup \{[type \mapsto \text{“1a”},\, bal \mapsto self]\}) \\
\qquad\qquad\qquad\quad \lor\ \land\, \exists\, v \in Value : \\
\qquad\qquad\qquad\qquad\ \land\ \land\, sentMsgs(\text{“2a”},\, self) = \{\} \\
\qquad\qquad\qquad\qquad\quad\ \land\, \exists\, Q \in Quorum : ShowsSafeAt(Q,\, self,\, v) \\
\qquad\qquad\qquad\qquad\ \land\, msgs' = (msgs \cup \{[type \mapsto \text{“2a”},\, bal \mapsto self,\, val \mapsto v]\}) \\
\qquad\qquad\ \land \text{ UNCHANGED } \langle maxBal,\, maxVBal,\, maxVVal\rangle
\end{array}
$$

$$
\begin{array}{l}
Next \triangleq\ (\exists\, self \in Acceptor : acceptor(self)) \\
\qquad\quad \lor\, (\exists\, self \in Ballot : leader(self))
\end{array}
$$

$$
Spec \triangleq\ Init \land \Box[Next]_{vars}
$$

END TRANSLATION

$$
\begin{array}{l}
TypeOK \triangleq\ \land\, maxBal\ \ \in [Acceptor \to Ballot \cup \{-1\}] \\
\qquad\qquad\ \land\, maxVBal \in [Acceptor \to Ballot \cup \{-1\}] \\
\qquad\qquad\ \land\, maxVVal \in [Acceptor \to Value \cup \{None\}] \\
\qquad\qquad\ \land\, msgs \subseteq Message
\end{array}
$$

$$
\begin{array}{l}
ChosenIn(b,\, v) \triangleq \\
\quad \exists\, Q \in Quorum : \forall\, a \in Q : \\
\qquad \exists\, m \in sentMsgs(\text{“2b”},\, b) : \\
\qquad\quad \land\ m.acc = a \\
\qquad\quad \land\ m.val = v
\end{array}
$$

$$
Chosen(v) \triangleq\ \exists\, b \in Ballot : ChosenIn(b,\, v)
$$

$$
\begin{array}{l}
Correctness \triangleq \\
\quad \forall\, v1,\, v2 \in Value : Chosen(v1) \land Chosen(v2) \Rightarrow v1 = v2
\end{array}
$$

THEOREM $Spec \Rightarrow \Box Correctness$

$Liveness \triangleq \forall\, b \in Ballot :$
$\quad \Box(\forall\, a \in Acceptor : maxBal[a] \leq b) \Rightarrow \Diamond(\exists\, v \in Value : Chosen(v))$

* Modification History
* Last modified *Thu Jul* 18 15:30:44 *PDT* 2024 by *nano*
* Created *Thu Sep* 03 22:58:03 *EDT* 2015 by *nano*