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*, *TLC*

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

   $Max(M) \triangleq$   A message with the highest ballot number among the set of messages ms
         CHOOSE $maxM \in M : \forall m \in M : m.mbal \leq maxM.mbal$

   $HighestAcceptedValue(Q1bMessages) \triangleq Max(Q1bMessages).mval$

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

 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 $\land\ sentMsgs(\text{"2a"}, self) = \{\}$
         $\land\ \exists\, Q \in Quorum : ShowsSafeAt(Q, self, v)$ ;
    $msgs := msgs \cup \{[type \mapsto \text{"2a"}, bal \mapsto self, val \mapsto v]\}$ ;
   }

  macro $Phase2b(b)\{$
    when $b \geq maxBal[self]$ ;
    with $(m \in sentMsgs(\text{"2a"}, b))\{$
        $maxBal[self] := b$ ;
        $maxVBal[self] := b$ ;
        $maxVVal[self] := m.val$ ;
        $msgs := msgs \cup \{[type \mapsto \text{"2b"}, acc \mapsto self, bal \mapsto b, val \mapsto m.val]\}$
    }
   }

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

  process $(leader \in Ballot)\{$
    $ldr$: while (TRUE){
           either $Phase1a()$
           or     with $(v \in Value)\{Phase2a(v)\}$
          }
   }
}
$TypeOK \triangleq \land\ maxBal \in [Acceptor \rightarrow Ballot \cup \{-1\}]$
                   $\land\ maxVBal \in [Acceptor \rightarrow Ballot \cup \{-1\}]$
                   $\land\ maxVVal \in [Acceptor \rightarrow Value \cup \{None\}]$
                   $\land\ msgs \subseteq Message$

$ChosenIn(b, v) \triangleq$
    $\exists\, Q \in Quorum : \forall\, a \in Q :$
       $\exists\, m \in sentMsgs(\text{"2b"}, b) :$
           $\land\ m.acc = a$
           $\land\ m.val = v$

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

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

THEOREM $Spec \Rightarrow \Box Correctness$

* Modification History
* Last modified *Fri Aug* 04 16:16:29 *PDT* 2017 by *nano*
* Created *Thu Sep* 03 22:58:03 *EDT* 2015 by *nano*