```
┌──────────────────────────── MODULE MCPaxos ────────────────────────────┐
EXTENDS Paxos, TLC
├────────────────────────────────────────────────────────────────────────┤
CONSTANTS a1, a2, a3   acceptors
CONSTANTS v1, v2       Values

MCAcceptor ≜ {a1}     {a1, a2, a3}
MCValue    ≜ {v1}     {v1, v2}
MCQuorum ≜ {{a1}}  {{a1, a2}, {a1, a3}, {a2, a3}}
MCMaxBallot ≜ 1
MCBallot ≜ 0 . . MCMaxBallot
MCSymmetry ≜ Permutations(MCAcceptor) ∪ Permutations(MCValue)

VotingSpecBar ≜ V ! Spec
├────────────────────────────────────────────────────────────────────────┤
For checking liveness.
MCLSpec ≜ ∧ Spec
          ∧ WF_vars(Phase1a(MCMaxBallot))
          ∧ ∀ v ∈ Value : WF_vars(Phase2a(MCMaxBallot, v))
          ∧ ∀ a ∈ {a1, a2} : WF_vars(Phase1b(a) ∨ Phase2b(a))
MCLiveness ≜ ◇(V ! chosen ≠ {})
├────────────────────────────────────────────────────────────────────────┤
For checking the inductive invariant.

In an initial predicate, a variable x must appear for the first time in a conjunct of the form x = exp
or x ∈ exp . We must therefore rewrite the inductive invariant Inv for use as an initial predicate
to replace the conjunct msgs ⊆ Message with the equivalent formula msgs ∈ SUBSET Message .
ITypeOK ≜ ∧ maxBal ∈ [Acceptor → Ballot ∪ { − 1}]
          ∧ maxVBal ∈ [Acceptor → Ballot ∪ { − 1}]
          ∧ maxVal ∈ [Acceptor → Value ∪ {None}]
          ∧ msgs ∈ SUBSET Message

IInv ≜ ∧ ITypeOK
       ∧ Inv!2      Inv!2 is the second conjunct of the definition of Inv.
       ∧ Inv!3
       ∧ Inv!4


Inv is an inductive invariant of Spec iff it is an invariant of the following specification.
MCISpec ≜ IInv ∧ □[Next]_vars

TLC only tells you if an invariant is violated, not what part is violated. To help locate an error,
it's useful to give TLC the conjuncts of an invariant as separate invariants to check.
Inv1 ≜ Inv!1
Inv2 ≜ Inv!2
Inv3 ≜ Inv!3
Inv4 ≜ Inv!4
```

To prove that *Spec* implements the specification *Spec* of module *Voting* under the refinement mapping we have defined, we must prove

$$Inv \land\ [Next]\_vars \Rightarrow\ [V\,!\,Next]\_\langle votes,\ maxBal\rangle$$

For an inductive invariant *Inv*, this is true iff the following property is implied by specification *MCISpec*.

$$MCIProp\ \triangleq\ \Box[V\,!\,Next]_{\langle votes,\ maxBal\rangle}$$