```
┌──────────────────────── MODULE EagerVoting ────────────────────────┐
EXTENDS Sets
├────────────────────────────────────────────────────────────────────┤
CONSTANT Value, Acceptor, Quorum
ASSUME QuorumAssumption ≜
    ∧   ∀ Q ∈ Quorum : Q ⊆ Acceptor
    ∧   ∀ Q1, Q2 ∈ Quorum : Q1 ∩ Q2 ≠ {}
THEOREM QuorumNonEmpty ≜ ∀ Q ∈ Quorum : Q ≠ {}
BY QuorumAssumption
Ballot ≜ Nat
├────────────────────────────────────────────────────────────────────┤
VARIABLES votes, maxBal
TypeOK ≜ ∧ votes ∈ [Acceptor → SUBSET (Ballot × Value)]
         ∧ maxBal ∈ [Acceptor → Ballot ∪ { − 1}]
├────────────────────────────────────────────────────────────────────┤
VotedFor(a, b, v) ≜ ⟨b, v⟩ ∈ votes[a]
DidNotVoteAt(a, b) ≜ ∀ v ∈ Value : ¬VotedFor(a, b, v)
ShowsSafeAt(Q, b, v) ≜
  ∧ ∀ a ∈ Q : maxBal[a] ≥ b  have promised
  ∧ ∃ c ∈    − 1 . . (b − 1) :
      ∧ (c ≠ − 1) ⇒ ∃ a ∈ Q : VotedFor(a, c, v)
      ∧ ∀ d ∈ (c + 1) . . (b − 1), a ∈ Q : DidNotVoteAt(a, d)
├────────────────────────────────────────────────────────────────────┤
Init ≜
    ∧ votes = [a ∈ Acceptor ↦ {}]
    ∧ maxBal = [a ∈ Acceptor ↦ − 1]
IncreaseMaxBal(a, b) ≜
  ∧ maxBal[a] < b
  ∧ maxBal′ = [maxBal EXCEPT ![a] = b]  make promise
  ∧ UNCHANGED votes

The only difference between EagerVoting and Voting is:

In Voting, we have maxBal′ = [maxBal EXCEPT ![a] = b].

VoteFor(a, b, v) ≜
    ∧   maxBal[a] ≤ b  keep promise
    ∧   ∀ vt ∈ votes[a] : vt[1] ≠ b
    ∧   ∀ c ∈ Acceptor \ {a} :
          ∀ vt ∈ votes[c] : (vt[1] = b) ⇒ (vt[2] = v)
    ∧   ∃ Q ∈ Quorum : ShowsSafeAt(Q, b, v)  safe to vote
    ∧   votes′ = [votes EXCEPT ![a] = votes[a] ∪ {⟨b, v⟩}]  vote
    ∧   ∃ c ∈ Ballot :
          ∧ c ≥ b
          ∧ maxBal′ = [maxBal EXCEPT ![a] = c]  make promise
```

```
├──────────────────────────────────────────────────────────────────┤
Next ≜
    ∃ a ∈ Acceptor, b ∈ Ballot :
        ∨ IncreaseMaxBal(a, b)
        ∨ ∃ v ∈ Value : VoteFor(a, b, v)
Spec ≜ Init ∧ □[Next]_⟨votes, maxBal⟩
├──────────────────────────────────────────────────────────────────┤
ChosenAt(b, v) ≜
    ∃ Q ∈ Quorum : ∀ a ∈ Q : VotedFor(a, b, v)
chosen ≜ {v ∈ Value : ∃ b ∈ Ballot : ChosenAt(b, v)}
Consistency ≜ chosen = {} ∨ ∃ v ∈ Value : chosen = {v}  Cardinality(chosen) ≤ 1
├──────────────────────────────────────────────────────────────────┤
CannotVoteAt(a, b) ≜
     ∧ maxBal[a] > b
     ∧ DidNotVoteAt(a, b)
NoneOtherChoosableAt(b, v) ≜
    ∃ Q ∈ Quorum :
       ∀ a ∈ Q : VotedFor(a, b, v) ∨ CannotVoteAt(a, b)
SafeAt(b, v) ≜
    ∀ c ∈ 0 . . (b − 1) : NoneOtherChoosableAt(c, v)
VotesSafe ≜
    ∀ a ∈ Acceptor, b ∈ Ballot, v ∈ Value :
        VotedFor(a, b, v) ⇒ SafeAt(b, v)
OneVote ≜
    ∀ a ∈ Acceptor, b ∈ Ballot, v, w ∈ Value :
        VotedFor(a, b, v) ∧ VotedFor(a, b, w) ⇒ (v = w)
OneValuePerBallot ≜
    ∀ a1, a2 ∈ Acceptor, b ∈ Ballot, v1, v2 ∈ Value :
        VotedFor(a1, b, v1) ∧ VotedFor(a2, b, v2) ⇒ (v1 = v2)
Inv ≜ TypeOK ∧ VotesSafe ∧ OneValuePerBallot
├──────────────────────────────────────────────────────────────────┤
THEOREM AllSafeAtZero ≜ ∀ v ∈ Value : SafeAt(0, v)
  BY DEF SafeAt
THEOREM ChoosableThm ≜
                ∀ b ∈ Ballot, v ∈ Value :
                  ChosenAt(b, v) ⇒ NoneOtherChoosableAt(b, v)
  BY DEF ChosenAt, NoneOtherChoosableAt
THEOREM OneVoteThm ≜ OneValuePerBallot ⇒ OneVote
  BY DEF OneValuePerBallot, OneVote
├──────────────────────────────────────────────────────────────────┤
THEOREM VotesSafeImpliesConsistency ≜
   ASSUME VotesSafe, OneVote, chosen ≠ {}
```

```
    PROVE  $\exists\, v \in Value : chosen = \{v\}$
$\langle 1\rangle 1.$ PICK $v \in Value : v \in chosen$
  BY DEF $chosen$
$\langle 1\rangle 2.$ SUFFICES ASSUME NEW $w \in chosen$
                 PROVE  $w = v$
  BY $\langle 1\rangle 1$, $\langle 1\rangle 2$
$\langle 1\rangle 3.$ ASSUME NEW $b1 \in Ballot$, NEW $b2 \in Ballot$, $b1 < b2$,
               NEW $v1 \in Value$, NEW $v2 \in Value$,
               $ChosenAt(b1, v1) \land ChosenAt(b2, v2)$
      PROVE  $v1 = v2$
  $\langle 2\rangle 1.$ $SafeAt(b2, v2)$
    BY $\langle 1\rangle 3$, $QuorumAssumption$, $SMT$ DEF $ChosenAt$, $VotesSafe$
  $\langle 2\rangle 2.$ QED
    BY $\langle 1\rangle 3$, $\langle 2\rangle 1$, $QuorumAssumption$, $Z3$
    DEFS $CannotVoteAt$, $DidNotVoteAt$, $OneVote$,
         $ChosenAt$, $NoneOtherChoosableAt$, $Ballot$, $SafeAt$
$\langle 1\rangle 4.$ QED
  BY $QuorumAssumption$, $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 3$, $Z3$
  DEFS $Ballot$, $ChosenAt$, $OneVote$, $chosen$
THEOREM $ShowsSafety \triangleq$
             $TypeOK \land VotesSafe \land OneValuePerBallot \Rightarrow$
               $\forall\, Q \in Quorum, b \in Ballot, v \in Value :$
                 $ShowsSafeAt(Q, b, v) \Rightarrow SafeAt(b, v)$
  BY $QuorumAssumption$, $Z3$
  DEFS $Ballot$, $TypeOK$, $VotesSafe$, $OneValuePerBallot$, $SafeAt$,
    $ShowsSafeAt$, $CannotVoteAt$, $NoneOtherChoosableAt$, $DidNotVoteAt$
THEOREM $SafeAtStable \triangleq Inv \land Next \land TypeOK' \Rightarrow$
                              $\forall\, b \in Ballot, v \in Value :$
                                 $SafeAt(b, v) \Rightarrow SafeAt(b, v)'$
  OMITTED
```

```
THEOREM $Invariant \triangleq Spec \Rightarrow \Box Inv$
$\langle 1\rangle$ USE DEF $Inv$
$\langle 1\rangle 1.$ $Init \Rightarrow Inv$
  BY DEF $Init$, $TypeOK$, $VotesSafe$, $OneValuePerBallot$, $VotedFor$
$\langle 1\rangle 2.$ $Inv \land [Next]_{\langle votes,\, maxBal\rangle} \Rightarrow Inv'$
  $\langle 2\rangle$ SUFFICES ASSUME $Inv$, $[Next]_{\langle votes,\, maxBal\rangle}$
               PROVE  $Inv'$
    OBVIOUS
  $\langle 2\rangle 1.$CASE $Next$
    $\langle 3\rangle$ SUFFICES ASSUME NEW $a \in Acceptor$, NEW $b \in Ballot$,
                            $\lor\ IncreaseMaxBal(a, b)$
                            $\lor\ \exists\, v \in Value : VoteFor(a, b, v)$
                 PROVE  $Inv'$
  BY $\langle 2\rangle 1$  DEF $Next$
$\langle 3\rangle 1.$CASE $IncreaseMaxBal(a, b)$
  $\langle 4\rangle 1.$ $TypeOK'$
    BY $\langle 3\rangle 1$  DEF $TypeOK$, $IncreaseMaxBal$
  $\langle 4\rangle 2.$ $VotesSafe'$
    $\langle 5\rangle$ SUFFICES ASSUME NEW $a\_1 \in Acceptor'$, NEW $b\_1 \in Ballot'$, NEW $v \in Value'$
                   PROVE  $VotedFor(a\_1, b\_1, v)' \Rightarrow SafeAt(b\_1, v)'$
      BY  DEF $VotesSafe$
    $\langle 5\rangle 1.$ $\forall aa \in Acceptor, bb \in Ballot, vv \in Value :$
            $VotedFor(aa, bb, vv) \equiv VotedFor(aa, bb, vv)'$
      BY $\langle 3\rangle 1$  DEF $IncreaseMaxBal$, $VotedFor$
    $\langle 5\rangle 2.$ $\forall aa \in Acceptor, bb \in Ballot :$
            $maxBal[aa] > bb \Rightarrow maxBal'[aa] > bb$
      BY $\langle 3\rangle 1$  DEF $IncreaseMaxBal$, $TypeOK$, $Ballot$
    $\langle 5\rangle 3.$ $\forall aa \in Acceptor, bb \in Ballot :$
            $DidNotVoteAt(aa, bb) \Rightarrow DidNotVoteAt(aa, bb)'$
      BY $\langle 3\rangle 1$  DEF $IncreaseMaxBal$, $DidNotVoteAt$, $VotedFor$
    $\langle 5\rangle 4.$ $\forall aa \in Acceptor, bb \in Ballot :$
            $CannotVoteAt(aa, bb) \Rightarrow CannotVoteAt(aa, bb)'$
      BY $\langle 3\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$  DEF $IncreaseMaxBal$, $CannotVoteAt$
    $\langle 5\rangle 5.$ $\forall bb \in Ballot, vv \in Value :$
            $NoneOtherChoosableAt(bb, vv) \Rightarrow NoneOtherChoosableAt(bb, vv)'$
      BY $\langle 5\rangle 1$, $\langle 5\rangle 4$, $QuorumAssumption$DEFS $NoneOtherChoosableAt$
    $\langle 5\rangle 6.$ QED
      BY $\langle 5\rangle 1$, $\langle 5\rangle 5$  DEF $TypeOK$, $Ballot$, $VotesSafe$, $SafeAt$
  $\langle 4\rangle 3.$ $OneValuePerBallot'$
    BY $\langle 3\rangle 1$  DEF $IncreaseMaxBal$, $OneValuePerBallot$, $VotedFor$
  $\langle 4\rangle 4.$ QED
    BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$  DEF $Inv$
$\langle 3\rangle 2.$ ASSUME NEW $v \in Value$,
               $VoteFor(a, b, v)$
      PROVE  $Inv'$
  $\langle 4\rangle$ SUFFICES ASSUME NEW $Q \in Quorum$,
                          $ShowsSafeAt(Q, b, v)$
                 PROVE  $Inv'$
    BY $\langle 3\rangle 2$  DEF $VoteFor$
  $\langle 4\rangle 1.$ $TypeOK'$
    BY $\langle 3\rangle 2$  DEF $TypeOK$, $VoteFor$
  $\langle 4\rangle 2.$ $VotesSafe'$ Using $OneValuePerBallot$ in $SafeAtStable$
    $\langle 5\rangle$ SUFFICES ASSUME NEW $aa \in Acceptor'$, NEW $bb \in Ballot'$, NEW $vv \in Value'$,
                          $VotedFor(aa, bb, vv)'$
                   PROVE  $SafeAt(bb, vv)'$
      BY  DEF $VotesSafe$
    $\langle 5\rangle 1.$CASE $VotedFor(aa, bb, vv)$
      $\langle 6\rangle 1.$ $SafeAt(bb, vv)$
```

```
            BY ⟨5⟩1  DEF VotesSafe
          ⟨6⟩ QED
            BY ⟨4⟩1, ⟨6⟩1, SafeAtStable DEF Next
        ⟨5⟩2.CASE ¬VotedFor(aa, bb, vv)
          ⟨6⟩1. aa = a ∧ bb = b ∧ vv = v ∧ VotedFor(a, b, v)′
            BY ⟨3⟩2, ⟨4⟩1, ⟨5⟩2  DEF VoteFor, VotedFor, TypeOK
          ⟨6⟩ QED
            BY ⟨4⟩1, ⟨6⟩1, ShowsSafety, SafeAtStable DEF VoteFor, Next
        ⟨5⟩ QED
          BY ⟨5⟩1, ⟨5⟩2
      ⟨4⟩3. OneValuePerBallot′
        BY ⟨3⟩2  DEF VoteFor, OneValuePerBallot, VotedFor, TypeOK
      ⟨4⟩4. QED
        BY ⟨3⟩2, ⟨4⟩1, ⟨4⟩2, ⟨4⟩3  DEF Inv
    ⟨3⟩3. QED
      BY ⟨2⟩1, ⟨3⟩1, ⟨3⟩2
  ⟨2⟩2.CASE UNCHANGED ⟨votes, maxBal⟩
    BY ⟨2⟩2
    DEFS TypeOK, Next, VotesSafe, OneValuePerBallot,
         VotedFor, SafeAt, NoneOtherChoosableAt, CannotVoteAt, DidNotVoteAt,
         IncreaseMaxBal, VoteFor
  ⟨2⟩3. QED
    BY ⟨2⟩1, ⟨2⟩2
⟨1⟩3. QED
  BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec
├──────────────────────────────────────────────────────────────────────┤
THEOREM Consistent ≜ Spec ⇒ □Consistency
⟨1⟩ USE  DEF Ballot
⟨1⟩1. Inv ⇒ Consistency
  ⟨2⟩ SUFFICES ASSUME Inv
               PROVE  Consistency
    OBVIOUS
  ⟨2⟩ QED
    BY VotesSafeImpliesConsistency, OneVoteThm DEF Inv, Consistency
⟨1⟩2. QED
  BY Invariant, ⟨1⟩1, PTL
├──────────────────────────────────────────────────────────────────────┤
C ≜ INSTANCE Consensus  WITH chosen ← chosen
THEOREM Refinement ≜ Spec ⇒ C!Spec
⟨1⟩1. Init ⇒ C!Init
  BY QuorumAssumption, SetExtensionality, IsaM("force")
   DEF Init, C!Init, chosen, ChosenAt, VotedFor
⟨1⟩2. TypeOK′ ∧ Consistency′ ∧ [Next]_⟨votes, maxBal⟩ ⇒ [C!Next]_chosen
  ⟨2⟩1. UNCHANGED ⟨votes, maxBal⟩ ⇒ UNCHANGED chosen
    BY  DEF chosen, ChosenAt, VotedFor
  $\langle 2 \rangle 2.$ $\mathit{TypeOK}' \land \mathit{Consistency}' \land \mathit{Next} \Rightarrow C!\mathit{Next} \lor$ UNCHANGED $\mathit{chosen}$
    $\langle 3 \rangle 1.$ SUFFICES ASSUME $\mathit{TypeOK}', \mathit{Consistency}', \mathit{Next}$
                      PROVE  $C!\mathit{Next} \lor$ UNCHANGED $\mathit{chosen}$
      OBVIOUS
    $\langle 3 \rangle 2.$ $\mathit{chosen} \subseteq \mathit{chosen}'$
      BY $\langle 3 \rangle 1$, $\mathit{QuorumAssumption}$, $Z3$
      DEFS $\mathit{Next}, \mathit{IncreaseMaxBal}, \mathit{VoteFor}, \mathit{Inv}, \mathit{TypeOK}, \mathit{chosen}, \mathit{ChosenAt}, \mathit{VotedFor}, \mathit{Ballot}$
    $\langle 3 \rangle 3.$ $\mathit{chosen}' = \{\} \lor \exists v \in \mathit{Value} : \mathit{chosen}' = \{v\}$
      BY $\langle 3 \rangle 1$  DEF $\mathit{Consistency}$
    $\langle 3 \rangle 4.$ QED
      BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$  DEF $C!\mathit{Next}$
  $\langle 2 \rangle 3.$ QED
    BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$
$\langle 1 \rangle 3.$ QED
  BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\mathit{Invariant}$, $\mathit{Consistent}$, $\mathit{PTL}$ DEF $\mathit{Spec}, \mathit{Inv}, C!\mathit{Spec}$
```