MODULE *EagerVoting*

EXTENDS *Sets*

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

$Ballot \triangleq Nat$

VARIABLES *votes*, *maxBal*

$TypeOK \triangleq \land votes \in [Acceptor \to \text{SUBSET } (Ballot \times Value)]$
$\land maxBal \in [Acceptor \to Ballot \cup \{-1\}]$

$VotedFor(a, b, v) \triangleq \langle b, v\rangle \in votes[a]$

$DidNotVoteAt(a, b) \triangleq \forall v \in Value : \neg VotedFor(a, b, v)$

$ShowsSafeAt(Q, b, v) \triangleq$
$\land \forall a \in Q : maxBal[a] \geq b$ have promised
$\land \exists c \in -1 \,..\, (b-1) :$
$\land (c \neq -1) \Rightarrow \exists a \in Q : VotedFor(a, c, v)$
$\land \forall d \in (c+1) \,..\, (b-1), a \in Q : DidNotVoteAt(a, d)$

$Init \triangleq$
$\land votes = [a \in Acceptor \mapsto \{\}]$
$\land maxBal = [a \in Acceptor \mapsto -1]$

$IncreaseMaxBal(a, b) \triangleq$
$\land maxBal[a] < b$
$\land maxBal' = [maxBal \text{ EXCEPT } ![a] = b]$ make promise
$\land$ UNCHANGED *votes*

The only difference between *EagerVoting* and *Voting* is: In *Voting*, we have $maxBal' = [maxBal$ EXCEPT $![a] = b]$.

$VoteFor(a, b, v) \triangleq$
$\land \quad maxBal[a] \leq b$ keep promise
$\land \quad \forall vt \in votes[a] : vt[1] \neq b$
$\land \quad \forall c \in Acceptor \setminus \{a\} :$
$\forall vt \in votes[c] : (vt[1] = b) \Rightarrow (vt[2] = v)$
$\land \quad \exists Q \in Quorum : ShowsSafeAt(Q, b, v)$ safe to vote
$\land \quad votes' = [votes \text{ EXCEPT } ![a] = votes[a] \cup \{\langle b, v\rangle\}]$ vote
$\land \quad \exists c \in Ballot :$
$\land c \geq b$
$\land maxBal' = [maxBal \text{ EXCEPT } ![a] = c]$ make promise

---

$Next \triangleq$
$\exists a \in Acceptor, b \in Ballot :$
$\lor IncreaseMaxBal(a, b)$
$\lor \exists v \in Value : VoteFor(a, b, v)$

$Spec \triangleq Init \land \Box[Next]_{\langle votes, maxBal\rangle}$

THEOREM $QuorumNonEmpty \triangleq \forall Q \in Quorum : Q \neq \{\}$
BY $QuorumAssumption$

$ChosenAt(b, v) \triangleq$
$\quad \exists Q \in Quorum : \forall a \in Q : VotedFor(a, b, v)$

$chosen \triangleq \{v \in Value : \exists b \in Ballot : ChosenAt(b, v)\}$

$Consistency \triangleq chosen = \{\} \lor \exists v \in Value : chosen = \{v\}$ $Cardinality(chosen) \leq 1$

$CannotVoteAt(a, b) \triangleq$
$\quad \land maxBal[a] > b$
$\quad \land DidNotVoteAt(a, b)$

$NoneOtherChoosableAt(b, v) \triangleq$
$\quad \exists Q \in Quorum :$
$\quad\quad \forall a \in Q : VotedFor(a, b, v) \lor CannotVoteAt(a, b)$

$SafeAt(b, v) \triangleq$
$\quad \forall c \in 0 \,..\, (b-1) : NoneOtherChoosableAt(c, v)$

$VotesSafe \triangleq$
$\quad \forall a \in Acceptor, b \in Ballot, v \in Value :$
$\quad\quad VotedFor(a, b, v) \Rightarrow SafeAt(b, v)$

$OneVote \triangleq$
$\quad \forall a \in Acceptor, b \in Ballot, v, w \in Value :$
$\quad\quad VotedFor(a, b, v) \land VotedFor(a, b, w) \Rightarrow (v = w)$

$OneValuePerBallot \triangleq$
$\quad \forall a1, a2 \in Acceptor, b \in Ballot, v1, v2 \in Value :$
$\quad\quad VotedFor(a1, b, v1) \land VotedFor(a2, b, v2) \Rightarrow (v1 = v2)$

$Inv \triangleq TypeOK \land VotesSafe \land OneValuePerBallot$

THEOREM $AllSafeAtZero \triangleq \forall v \in Value : SafeAt(0, v)$
BY DEF $SafeAt$

THEOREM $ChoosableThm \triangleq$
$\quad\quad \forall b \in Ballot, v \in Value :$
$\quad\quad\quad ChosenAt(b, v) \Rightarrow NoneOtherChoosableAt(b, v)$
BY DEF $ChosenAt$, $NoneOtherChoosableAt$

THEOREM $OneVoteThm \triangleq OneValuePerBallot \Rightarrow OneVote$
BY DEF $OneValuePerBallot$, $OneVote$

THEOREM $VotesSafeImpliesConsistency \triangleq$
ASSUME $VotesSafe$, $OneVote$, $chosen \neq \{\}$

PROVE $\exists\, v \in \mathit{Value} : \mathit{chosen} = \{v\}$

⟨1⟩1. PICK $v \in \mathit{Value} : v \in \mathit{chosen}$
BY DEF chosen

⟨1⟩2. SUFFICES ASSUME NEW $w \in \mathit{chosen}$
PROVE $w = v$
BY ⟨1⟩1, ⟨1⟩2

⟨1⟩3. ASSUME NEW $b1 \in \mathit{Ballot}$, NEW $b2 \in \mathit{Ballot}$, $b1 < b2$,
NEW $v1 \in \mathit{Value}$, NEW $v2 \in \mathit{Value}$,
$\mathit{ChosenAt}(b1,\, v1) \land \mathit{ChosenAt}(b2,\, v2)$
PROVE $v1 = v2$

⟨2⟩1. $\mathit{SafeAt}(b2,\, v2)$
BY ⟨1⟩3, $\mathit{QuorumAssumption}$, SMT DEF $\mathit{ChosenAt}$, $\mathit{VotesSafe}$

⟨2⟩2. QED
BY ⟨1⟩3, ⟨2⟩1, $\mathit{QuorumAssumption}$, $Z3$
DEFS $\mathit{CannotVoteAt}$, $\mathit{DidNotVoteAt}$, $\mathit{OneVote}$,
$\mathit{ChosenAt}$, $\mathit{NoneOtherChoosableAt}$, Ballot, SafeAt

⟨1⟩4. QED
BY $\mathit{QuorumAssumption}$, ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, $Z3$
DEFS Ballot, $\mathit{ChosenAt}$, $\mathit{OneVote}$, chosen

THEOREM $\mathit{ShowsSafety} \triangleq$
$\mathit{TypeOK} \land \mathit{VotesSafe} \land \mathit{OneValuePerBallot} \Rightarrow$
$\forall\, Q \in \mathit{Quorum},\, b \in \mathit{Ballot},\, v \in \mathit{Value} :$
$\mathit{ShowsSafeAt}(Q,\, b,\, v) \Rightarrow \mathit{SafeAt}(b,\, v)$
BY $\mathit{QuorumAssumption}$, $Z3$
DEFS Ballot, TypeOK, $\mathit{VotesSafe}$, $\mathit{OneValuePerBallot}$, SafeAt,
$\mathit{ShowsSafeAt}$, $\mathit{CannotVoteAt}$, $\mathit{NoneOtherChoosableAt}$, $\mathit{DidNotVoteAt}$

THEOREM $\mathit{SafeAtStable} \triangleq \mathit{Inv} \land \mathit{Next} \land \mathit{TypeOK}' \Rightarrow$
$\forall\, b \in \mathit{Ballot},\, v \in \mathit{Value} :$
$\mathit{SafeAt}(b,\, v) \Rightarrow \mathit{SafeAt}(b,\, v)'$
OMITTED

THEOREM $\mathit{Invariant} \triangleq \mathit{Spec} \Rightarrow \Box \mathit{Inv}$

⟨1⟩ USE DEF Inv

⟨1⟩1. $\mathit{Init} \Rightarrow \mathit{Inv}$
BY DEF Init, TypeOK, $\mathit{VotesSafe}$, $\mathit{OneValuePerBallot}$, $\mathit{VotedFor}$

⟨1⟩2. $\mathit{Inv} \land [\mathit{Next}]_{\langle \mathit{votes},\, \mathit{maxBal} \rangle} \Rightarrow \mathit{Inv}'$
⟨2⟩ SUFFICES ASSUME Inv, $[\mathit{Next}]_{\langle \mathit{votes},\, \mathit{maxBal} \rangle}$
PROVE Inv'
OBVIOUS

⟨2⟩1.CASE Next
⟨3⟩ SUFFICES ASSUME NEW $a \in \mathit{Acceptor}$, NEW $b \in \mathit{Ballot}$,
$\lor\, \mathit{IncreaseMaxBal}(a,\, b)$
$\lor\, \exists\, v \in \mathit{Value} : \mathit{VoteFor}(a,\, b,\, v)$

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 $VotedFor(aa,\ bb,\ vv)$

⟨6⟩1. $SafeAt(bb,\ vv)$
BY ⟨5⟩1 DEF $VotesSafe$
⟨6⟩ QED
BY ⟨4⟩1, ⟨6⟩1, $SafeAtStable$ DEF $Next$
⟨5⟩2.CASE $\neg VotedFor(aa,\ bb,\ vv)$
⟨6⟩1. $aa = a \land bb = b \land vv = v \land VotedFor(a,\ b,\ v)'$
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 $\langle votes,\ maxBal\rangle$
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 $Consistent \triangleq Spec \Rightarrow \Box Consistency$
⟨1⟩ USE DEF $Ballot$
⟨1⟩1. $Inv \Rightarrow Consistency$
⟨2⟩ SUFFICES ASSUME Inv
PROVE $Consistency$
OBVIOUS
⟨2⟩ QED
BY $VotesSafeImpliesConsistency$, $OneVoteThm$ DEF Inv, $Consistency$
⟨1⟩2. QED
BY $Invariant$, ⟨1⟩1, PTL

$C \triangleq$ INSTANCE $Consensus$ WITH $chosen \leftarrow chosen$

THEOREM $Refinement \triangleq Spec \Rightarrow C!Spec$
⟨1⟩1. $Init \Rightarrow C!Init$
BY $QuorumAssumption$, $SetExtensionality$, $IsaM(\text{“force”})$
DEF $Init$, $C!Init$, $chosen$, $ChosenAt$, $VotedFor$
⟨1⟩2. $TypeOK' \land Consistency' \land [Next]_{\langle votes,\ maxBal\rangle} \Rightarrow [C!Next]_{chosen}$

⟨2⟩1. UNCHANGED ⟨*votes*, *maxBal*⟩ ⇒ UNCHANGED *chosen*
BY DEF *chosen*, *ChosenAt*, *VotedFor*
⟨2⟩2. *TypeOK*′ ∧ *Consistency*′ ∧ *Next* ⇒ *C*!*Next* ∨ UNCHANGED *chosen*
⟨3⟩1. SUFFICES ASSUME *TypeOK*′, *Consistency*′, *Next*
PROVE *C*!*Next* ∨ UNCHANGED *chosen*
OBVIOUS
⟨3⟩2. *chosen* ⊆ *chosen*′
BY ⟨3⟩1, *QuorumAssumption*, *Z*3
DEFS *Next*, *IncreaseMaxBal*, *VoteFor*, *Inv*, *TypeOK*, *chosen*, *ChosenAt*, *VotedFor*, *Ballot*
⟨3⟩3. *chosen*′ = {} ∨ ∃ *v* ∈ *Value* : *chosen*′ = {*v*}
BY ⟨3⟩1 DEF *Consistency*
⟨3⟩4. QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3 DEF *C*!*Next*
⟨2⟩3. QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩3. QED
BY ⟨1⟩1, ⟨1⟩2, *Invariant*, *Consistent*, *PTL* DEF *Spec*, *Inv*, *C*!*Spec*