MODULE *Voting*

EXTENDS *Integers*, *FiniteSets*, *TLAPS*

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

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

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

$Ballot \triangleq Nat$

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
$\land \exists\, c \in -1 \,..\, (b-1) :$
$\land (c \neq -1) \Rightarrow \exists\, a \in Q : VotedFor(a,\, c,\, v)$
$\land \forall\, d \in (c+1) \,..\, (b-1),\, a \in Q : DidNotVoteAt(a,\, d)$

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

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

$VoteFor(a,\, b,\, v) \triangleq$
$\land \quad maxBal[a] \leq b$ 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
$\land \quad maxBal' = [maxBal \text{ EXCEPT } ![a] = b]$ make promise

---

$$
\begin{array}{l}
\mathit{Next} \triangleq \\
\quad \exists\, a \in \mathit{Acceptor},\, b \in \mathit{Ballot} : \\
\qquad \lor\, \mathit{IncreaseMaxBal}(a,\, b) \\
\qquad \lor \exists\, v \in \mathit{Value} : \mathit{VoteFor}(a,\, b,\, v) \\
\\
\mathit{Spec} \triangleq \mathit{Init} \land \Box[\mathit{Next}]_{\langle \mathit{votes},\, \mathit{maxBal} \rangle}
\end{array}
$$

$$
\begin{array}{l}
\mathit{ChosenAt}(b,\, v) \triangleq \\
\quad \exists\, Q \in \mathit{Quorum} : \forall\, a \in Q : \mathit{VotedFor}(a,\, b,\, v) \\
\\
\mathit{chosen} \triangleq \{v \in \mathit{Value} : \exists\, b \in \mathit{Ballot} : \mathit{ChosenAt}(b,\, v)\} \\
\\
\mathit{Consistency} \triangleq \mathit{chosen} = \{\} \lor \exists\, v \in \mathit{Value} : \mathit{chosen} = \{v\} \quad \mathit{Cardinality}(\mathit{chosen}) \leq 1
\end{array}
$$

$$
\begin{array}{l}
\mathit{CannotVoteAt}(a,\, b) \triangleq \\
\quad \land\, \mathit{maxBal}[a] > b \\
\quad \land\, \mathit{DidNotVoteAt}(a,\, b) \\
\\
\mathit{NoneOtherChoosableAt}(b,\, v) \triangleq \\
\quad \exists\, Q \in \mathit{Quorum} : \\
\qquad \forall\, a \in Q : \mathit{VotedFor}(a,\, b,\, v) \lor \mathit{CannotVoteAt}(a,\, b) \\
\\
\mathit{SafeAt}(b,\, v) \triangleq \\
\quad \forall\, c \in 0 \,..\, (b-1) : \mathit{NoneOtherChoosableAt}(c,\, v) \\
\\
\mathit{VotesSafe} \triangleq \\
\quad \forall\, a \in \mathit{Acceptor},\, b \in \mathit{Ballot},\, v \in \mathit{Value} : \\
\qquad \mathit{VotedFor}(a,\, b,\, v) \Rightarrow \mathit{SafeAt}(b,\, v) \\
\\
\mathit{OneVote} \triangleq \\
\quad \forall\, a \in \mathit{Acceptor},\, b \in \mathit{Ballot},\, v,\, w \in \mathit{Value} : \\
\qquad \mathit{VotedFor}(a,\, b,\, v) \land \mathit{VotedFor}(a,\, b,\, w) \Rightarrow (v = w) \\
\\
\mathit{OneValuePerBallot} \triangleq \\
\quad \forall\, a1,\, a2 \in \mathit{Acceptor},\, b \in \mathit{Ballot},\, v1,\, v2 \in \mathit{Value} : \\
\qquad \mathit{VotedFor}(a1,\, b,\, v1) \land \mathit{VotedFor}(a2,\, b,\, v2) \Rightarrow (v1 = v2) \\
\\
\mathit{Inv} \triangleq \mathit{TypeOK} \land \mathit{VotesSafe} \land \mathit{OneValuePerBallot}
\end{array}
$$

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

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

THEOREM $\mathit{OneVoteThm} \triangleq \mathit{OneValuePerBallot} \Rightarrow \mathit{OneVote}$

BY DEF *OneValuePerBallot*, *OneVote*

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

⟨2⟩1. CASE $Next$

⟨3⟩ 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 ⟨2⟩1 DEF $Next$

⟨3⟩1. CASE $IncreaseMaxBal(a,\ b)$

⟨4⟩1. $TypeOK'$

BY ⟨3⟩1 DEF $TypeOK$, $IncreaseMaxBal$

⟨4⟩2. $VotesSafe'$

⟨5⟩ 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 $VotesSafe$

⟨5⟩1. $\forall\, aa \in Acceptor,\ bb \in Ballot,\ vv \in Value :$
$VotedFor(aa,\ bb,\ vv) \equiv VotedFor(aa,\ bb,\ vv)'$

BY ⟨3⟩1 DEF $IncreaseMaxBal$, $VotedFor$

⟨5⟩2. $\forall\, aa \in Acceptor,\ bb \in Ballot :$
$maxBal[aa] > bb \Rightarrow maxBal'[aa] > bb$

BY ⟨3⟩1 DEF $IncreaseMaxBal$, $TypeOK$, $Ballot$

⟨5⟩3. $\forall\, aa \in Acceptor,\ bb \in Ballot :$
$DidNotVoteAt(aa,\ bb) \Rightarrow DidNotVoteAt(aa,\ bb)'$

BY ⟨3⟩1 DEF $IncreaseMaxBal$, $DidNotVoteAt$, $VotedFor$

⟨5⟩4. $\forall\, aa \in Acceptor,\ bb \in Ballot :$
$CannotVoteAt(aa,\ bb) \Rightarrow CannotVoteAt(aa,\ bb)'$

BY ⟨3⟩1, ⟨5⟩2, ⟨5⟩3 DEF $IncreaseMaxBal$, $CannotVoteAt$

⟨5⟩5. $\forall\, bb \in Ballot,\ vv \in Value :$
$NoneOtherChoosableAt(bb,\ vv) \Rightarrow NoneOtherChoosableAt(bb,\ vv)'$

BY ⟨5⟩1, ⟨5⟩4, $QuorumAssumption$DEFS $NoneOtherChoosableAt$

⟨5⟩6. QED

BY ⟨5⟩1, ⟨5⟩5 DEF $TypeOK$, $Ballot$, $VotesSafe$, $SafeAt$

⟨4⟩3. $OneValuePerBallot'$

BY ⟨3⟩1 DEF $IncreaseMaxBal$, $OneValuePerBallot$, $VotedFor$

⟨4⟩4. QED

BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3 DEF Inv

⟨3⟩2. ASSUME NEW $v \in Value$,
$VoteFor(a,\ b,\ v)$
PROVE Inv'

⟨4⟩ SUFFICES ASSUME NEW $Q \in Quorum$,
$ShowsSafeAt(Q,\ b,\ v)$
PROVE Inv'

BY ⟨3⟩2 DEF $VoteFor$

⟨4⟩1. $TypeOK'$

BY ⟨3⟩2 DEF $TypeOK$, $VoteFor$

⟨4⟩2. $VotesSafe'$ Using $OneValuePerBallot$ in $SafeAtStable$

⟨5⟩ 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*
⟨5⟩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 $\langle votes, maxBal\rangle \Rightarrow$ UNCHANGED $chosen$
BY DEF $chosen$, $ChosenAt$, $VotedFor$
⟨2⟩2. $TypeOK' \land Consistency' \land Next \Rightarrow C!Next \lor$ UNCHANGED $chosen$
⟨3⟩1. SUFFICES ASSUME $TypeOK'$, $Consistency'$, $Next$
PROVE $C!Next \lor$ UNCHANGED $chosen$
OBVIOUS
⟨3⟩2. $chosen \subseteq chosen'$
BY ⟨3⟩1, $QuorumAssumption$, $Z3$
DEFS $Next$, $IncreaseMaxBal$, $VoteFor$, Inv, $TypeOK$, $chosen$, $ChosenAt$, $VotedFor$, $Ballot$
⟨3⟩3. $chosen' = \{\} \lor \exists\, v \in Value : chosen' = \{v\}$
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, $C!Spec$