

```

1  |----- MODULE Voting -----|
2  EXTENDS Sets
3  |-----|
4  CONSTANT Value, Acceptor, Quorum

6  ASSUME QuorumAssumption  $\triangleq$ 
7       $\wedge \quad \forall Q \in \textit{Quorum} : Q \subseteq \textit{Acceptor}$ 
8       $\wedge \quad \forall Q1, Q2 \in \textit{Quorum} : Q1 \cap Q2 \neq \{\}$ 

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

13 Ballot  $\triangleq \textit{Nat}$ 
14 |-----|
15 VARIABLES votes, maxBal

17 TypeOK  $\triangleq$ 
18      $\wedge \quad \textit{votes} \in [\textit{Acceptor} \rightarrow \text{SUBSET } (\textit{Ballot} \times \textit{Value})]$ 
19      $\wedge \quad \textit{maxBal} \in [\textit{Acceptor} \rightarrow \textit{Ballot} \cup \{-1\}]$ 
20 |-----|
21 VotedFor(a, b, v)  $\triangleq \langle b, v \rangle \in \textit{votes}[a]$ 

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

25 ShowsSafeAt(Q, b, v)  $\triangleq$ 
26      $\wedge \forall a \in Q : \textit{maxBal}[a] \geq b$ 
27      $\wedge \exists c \in -1 \dots (b-1) :$ 
28          $\wedge (c \neq -1) \Rightarrow \exists a \in Q : \textit{VotedFor}(a, c, v)$ 
29          $\wedge \forall d \in (c+1) \dots (b-1), a \in Q : \textit{DidNotVoteAt}(a, d)$ 
30 |-----|
31 Init  $\triangleq$ 
32      $\wedge \textit{votes} = [a \in \textit{Acceptor} \mapsto \{\}]$ 
33      $\wedge \textit{maxBal} = [a \in \textit{Acceptor} \mapsto -1]$ 

35 IncreaseMaxBal(a, b)  $\triangleq$ 
36      $\wedge b > \textit{maxBal}[a]$ 
37      $\wedge \textit{maxBal}' = [\textit{maxBal} \text{ EXCEPT } ![a] = b]$ 
38      $\wedge \text{UNCHANGED } \textit{votes}$ 

40 VoteFor(a, b, v)  $\triangleq$ 
41      $\wedge \quad \textit{maxBal}[a] \leq b$ 
42      $\wedge \quad \forall vt \in \textit{votes}[a] : vt[1] \neq b$ 
43      $\wedge \quad \forall c \in \textit{Acceptor} \setminus \{a\} :$ 
44          $\forall vt \in \textit{votes}[c] : (vt[1] = b) \Rightarrow (vt[2] = v)$ 
45      $\wedge \quad \exists Q \in \textit{Quorum} : \textit{ShowsSafeAt}(Q, b, v)$ 
46      $\wedge \quad \textit{votes}' = [\textit{votes} \text{ EXCEPT } ![a] = \textit{votes}[a] \cup \{\langle b, v \rangle\}]$ 
47      $\wedge \quad \textit{maxBal}' = [\textit{maxBal} \text{ EXCEPT } ![a] = b]$ 

```

48 $Next \triangleq$
 49 $\exists a \in Acceptor, b \in Ballot :$
 50 $\quad \vee IncreaseMaxBal(a, b)$
 51 $\quad \vee \exists v \in Value : VoteFor(a, b, v)$
 52
 54 $Spec \triangleq Init \wedge \Box[Next]_{\langle votes, maxBal \rangle}$

56 $ChosenAt(b, v) \triangleq$
 57 $\exists Q \in Quorum : \forall a \in Q : VotedFor(a, b, v)$
 58
 59 $chosen \triangleq \{v \in Value : \exists b \in Ballot : ChosenAt(b, v)\}$

61 $CannotVoteAt(a, b) \triangleq$
 62 $\quad \wedge maxBal[a] > b$
 63 $\quad \wedge DidNotVoteAt(a, b)$
 64
 65 $NoneOtherChoosableAt(b, v) \triangleq$
 66 $\quad \exists Q \in Quorum :$
 67 $\quad \forall a \in Q : VotedFor(a, b, v) \vee CannotVoteAt(a, b)$
 68
 69 $SafeAt(b, v) \triangleq$
 70 $\quad \forall c \in 0 \dots (b - 1) : NoneOtherChoosableAt(c, v)$
 71
 72 $VotesSafe \triangleq$
 73 $\quad \forall a \in Acceptor, b \in Ballot, v \in Value :$
 74 $\quad VotedFor(a, b, v) \Rightarrow SafeAt(b, v)$
 75
 76 $OneVote \triangleq$
 77 $\quad \forall a \in Acceptor, b \in Ballot, v, w \in Value :$
 78 $\quad VotedFor(a, b, v) \wedge VotedFor(a, b, w) \Rightarrow (v = w)$
 79
 80 $OneValuePerBallot \triangleq$
 81 $\quad \forall a1, a2 \in Acceptor, b \in Ballot, v1, v2 \in Value :$
 82 $\quad VotedFor(a1, b, v1) \wedge VotedFor(a2, b, v2) \Rightarrow (v1 = v2)$
 83
 84 $Inv \triangleq TypeOK \wedge VotesSafe \wedge OneValuePerBallot$

86 THEOREM $AllSafeAtZero \triangleq \forall v \in Value : SafeAt(0, v)$
 87 BY DEF $SafeAt$
 88
 89 THEOREM $ChoosableThm \triangleq$
 90 $\quad \forall b \in Ballot, v \in Value :$
 91 $\quad ChosenAt(b, v) \Rightarrow NoneOtherChoosableAt(b, v)$
 92 BY DEF $ChosenAt, NoneOtherChoosableAt$
 93
 94 THEOREM $OneVoteThm \triangleq OneValuePerBallot \Rightarrow OneVote$
 95 BY DEF $OneValuePerBallot, OneVote$

96 |
 97 THEOREM *VotesSafeImpliesConsistency* \triangleq
 98 ASSUME *VotesSafe*, *OneVote*, *chosen* $\neq \{\}$
 99 PROVE $\exists v \in \text{Value} : \text{chosen} = \{v\}$
 100 $\langle 1 \rangle 1$. PICK $v \in \text{Value} : v \in \text{chosen}$
 101 BY DEF *chosen*
 102 $\langle 1 \rangle 2$. SUFFICES ASSUME NEW $w \in \text{chosen}$
 103 PROVE $w = v$
 104 BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$
 105 $\langle 1 \rangle 3$. ASSUME NEW $b1 \in \text{Ballot}$, NEW $b2 \in \text{Ballot}$, $b1 < b2$,
 106 NEW $v1 \in \text{Value}$, NEW $v2 \in \text{Value}$,
 107 $\text{ChosenAt}(b1, v1) \wedge \text{ChosenAt}(b2, v2)$
 108 PROVE $v1 = v2$
 109 $\langle 2 \rangle 1$. *SafeAt*($b2, v2$)
 110 BY $\langle 1 \rangle 3$, *QuorumAssumption*, SMT DEF *ChosenAt*, *VotesSafe*
 111 $\langle 2 \rangle 2$. QED
 112 BY $\langle 1 \rangle 3$, $\langle 2 \rangle 1$, *QuorumAssumption*, Z3
 113 DEFS *CannotVoteAt*, *DidNotVoteAt*, *OneVote*,
 114 *ChosenAt*, *NoneOtherChoosableAt*, *Ballot*, *SafeAt*
 115 $\langle 1 \rangle 4$. QED
 116 BY *QuorumAssumption*, $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, Z3
 117 DEFS *Ballot*, *ChosenAt*, *OneVote*, *chosen*

 119 THEOREM *ShowsSafety* \triangleq
 120 *TypeOK* \wedge *VotesSafe* \wedge *OneValuePerBallot* \Rightarrow
 121 $\forall Q \in \text{Quorum}, b \in \text{Ballot}, v \in \text{Value} :$
 122 *ShowsSafeAt*(Q, b, v) \Rightarrow *SafeAt*(b, v)
 123 BY *QuorumAssumption*, Z3
 124 DEFS *Ballot*, *TypeOK*, *VotesSafe*, *OneValuePerBallot*, *SafeAt*,
 125 *ShowsSafeAt*, *CannotVoteAt*, *NoneOtherChoosableAt*, *DidNotVoteAt*

 127 THEOREM *Invariance* \triangleq *Spec* $\Rightarrow \Box \text{Inv}$
 128 $\langle 1 \rangle 1$. *Init* \Rightarrow *Inv*
 129 BY DEF *Init*, *Inv*, *TypeOK*, *VotesSafe*, *VotedFor*, *OneValuePerBallot*
 130 $\langle 1 \rangle 2$. *Inv* $\wedge [\text{Next}]_{\langle \text{votes}, \text{maxBal} \rangle} \Rightarrow \text{Inv}'$
 131 $\langle 2 \rangle 1$. CASE \wedge *Inv*
 132 \wedge *Next*
 133 $\langle 3 \rangle 1$. ASSUME NEW $a \in \text{Acceptor}$, NEW $b \in \text{Ballot}$,
 134 *IncreaseMaxBal*(a, b)
 135 PROVE *Inv* $\wedge [\text{Next}]_{\langle \text{votes}, \text{maxBal} \rangle} \Rightarrow \text{Inv}'$
 136 BY $\langle 3 \rangle 1$
 137 $\langle 3 \rangle 2$. ASSUME NEW $a \in \text{Acceptor}$, NEW $b \in \text{Ballot}$,
 138 $\exists v \in \text{Value} : \text{VoteFor}(a, b, v)$
 139 PROVE *Inv* $\wedge [\text{Next}]_{\langle \text{votes}, \text{maxBal} \rangle} \Rightarrow \text{Inv}'$
 140 $\langle 3 \rangle 3$. QED

```

141     BY  $\langle 2 \rangle 1, \langle 3 \rangle 1, \langle 3 \rangle 2$  DEF Next
142  $\langle 2 \rangle 2$ .CASE  $\wedge$  Inv
143      $\wedge$  UNCHANGED  $\langle votes, maxBal \rangle$ 
144     BY  $\langle 2 \rangle 2$ 
145     DEFS Inv, TypeOK, VotesSafe, OneValuePerBallot,
146         VotedFor, SafeAt, NoneOtherChoosableAt, CannotVoteAt, DidNotVoteAt
147  $\langle 2 \rangle 3$ . QED
148     BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$ 
149  $\langle 1 \rangle 3$ . QED
150     BY  $\langle 1 \rangle 1, \langle 1 \rangle 2, PTL$  DEF Spec

152  $\langle 2 \rangle$  USE DEF Inv, TypeOK, VotesSafe, OneValuePerBallot, Ballot, VotedFor, VoteFor
153 NoneOtherChoosableAt, CannotVoteAt, DidNotVoteAt
154 ───────────────────────────────────────────────────────────────────────────────────┘
155  $C \triangleq$  INSTANCE Consensus

157 THEOREM Spec  $\wedge$  Inv  $\Rightarrow C!Spec$ 
158  $\langle 1 \rangle 1$ . Init  $\Rightarrow C!Init$ 
159     BY QuorumAssumption, SetExtensionality, IsaM ("force")
160     DEF Init, C!Init, chosen, ChosenAt, VotedFor
161  $\langle 1 \rangle 2$ . Next  $\wedge$  Inv  $\Rightarrow C!Next \vee$  UNCHANGED chosen
162  $\langle 2 \rangle 1$  SUFFICES ASSUME Next, Inv PROVE  $C!Next \vee$  UNCHANGED chosen
163     BY  $\langle 2 \rangle 1$ 
164  $\langle 2 \rangle 2$ . chosen  $\subseteq$  chosen'
165     BY  $\langle 2 \rangle 1, QuorumAssumption, Z3$  SMTT(10) fails
166     DEF Next, Inv, TypeOK, IncreaseMaxBal, chosen, ChosenAt, VotedFor, Ballot, VoteFor
167  $\langle 2 \rangle 3$ . chosen' =  $\{\}$   $\vee \exists v \in Value : chosen' = \{v\}$ 
168  $\langle 3 \rangle 1$ . PICK  $a \in Acceptor, b \in Ballot :$ 
169      $\vee IncreaseMaxBal(a, b)$ 
170      $\vee \exists v \in Value : VoteFor(a, b, v)$ 
171     BY  $\langle 2 \rangle 1$  DEF Next
172  $\langle 3 \rangle 2$ .CASE IncreaseMaxBal(a, b)
173  $\langle 3 \rangle 3$ .CASE  $\exists v \in Value : VoteFor(a, b, v)$ 
174  $\langle 3 \rangle q$ . QED
175     BY  $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3, SMT$ 
176  $\langle 2 \rangle q$ . QED
177     BY  $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3, OneVoteThm, VotesSafeImpliesConsistency, SetExtensionality, SMT$ 
178     DEF Inv, C!Next
179  $\langle 1 \rangle 3$ . QED
180     PROOF OMITTED
181 ───────────────────────────────────────────────────────────────────────────────────┘

```