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

6  ASSUME QuorumAssumption ≜
7      ∧  ∀ Q ∈ Quorum : Q ⊆ Acceptor
8      ∧  ∀ Q1, Q2 ∈ Quorum : Q1 ∩ Q2 ≠ {}

10 THEOREM QuorumNonEmpty ≜ ∀ Q ∈ Quorum : Q ≠ {}
11 BY QuorumAssumption

13 Ballot ≜ Nat
14 ----------------------------------
15 VARIABLES votes, maxBal

17 TypeOK ≜
18     ∧  votes ∈ [Acceptor → SUBSET (Ballot × Value)]
19     ∧  maxBal ∈ [Acceptor → Ballot ∪ {-1}]
20 ----------------------------------
21 VotedFor(a, b, v) ≜ ⟨b, v⟩ ∈ votes[a]

23 DidNotVoteAt(a, b) ≜ ∀ v ∈ Value : ¬VotedFor(a, b, v)

25 ShowsSafeAt(Q, b, v) ≜
26   ∧ ∀ a ∈ Q : maxBal[a] ≥ b
27   ∧ ∃ c ∈ -1 .. (b-1) :
28       ∧ (c ≠ -1) ⇒ ∃ a ∈ Q : VotedFor(a, c, v)
29       ∧ ∀ d ∈ (c+1) .. (b-1), a ∈ Q : DidNotVoteAt(a, d)
30 ----------------------------------
31 Init ≜
32     ∧ votes = [a ∈ Acceptor ↦ {}]
33     ∧ maxBal = [a ∈ Acceptor ↦ -1]

35 IncreaseMaxBal(a, b) ≜
36   ∧ b > maxBal[a]
37   ∧ maxBal' = [maxBal EXCEPT ![a] = b]
38   ∧ UNCHANGED votes

40 VoteFor(a, b, v) ≜
41     ∧  maxBal[a] ≤ b
42     ∧  ∀ vt ∈ votes[a] : vt[1] ≠ b
43     ∧  ∀ c ∈ Acceptor \ {a} :
44          ∀ vt ∈ votes[c] : (vt[1] = b) ⇒ (vt[2] = v)
45     ∧  ∃ Q ∈ Quorum : ShowsSafeAt(Q, b, v)
46     ∧  votes' = [votes EXCEPT ![a] = votes[a] ∪ {⟨b, v⟩}]
47     ∧  maxBal' = [maxBal EXCEPT ![a] = b]
```

48 ⊢———⊣
49 $Next \triangleq$
50 $\quad \exists\, a \in Acceptor,\ b \in Ballot :$
51 $\quad\quad \lor\ IncreaseMaxBal(a,\ b)$
52 $\quad\quad \lor \exists\, v \in Value : VoteFor(a,\ b,\ v)$

54 $Spec \triangleq Init \land \Box[Next]_{\langle votes,\ maxBal\rangle}$
55 ⊢———⊣
56 $ChosenAt(b,\ v) \triangleq$
57 $\quad \exists\, Q \in Quorum : \forall\, a \in Q : VotedFor(a,\ b,\ v)$

59 $chosen \triangleq \{v \in Value : \exists\, b \in Ballot : ChosenAt(b,\ v)\}$
60 ⊢———⊣
61 $CannotVoteAt(a,\ b) \triangleq$
62 $\quad \land\ maxBal[a] > b$
63 $\quad \land\ DidNotVoteAt(a,\ b)$

65 $NoneOtherChoosableAt(b,\ v) \triangleq$
66 $\quad \exists\, Q \in Quorum :$
67 $\quad\quad \forall\, a \in Q : VotedFor(a,\ b,\ v) \lor CannotVoteAt(a,\ b)$

69 $SafeAt(b,\ v) \triangleq$
70 $\quad \forall\, c \in 0\,..\,(b-1) : NoneOtherChoosableAt(c,\ v)$

72 $VotesSafe \triangleq$
73 $\quad \forall\, a \in Acceptor,\ b \in Ballot,\ v \in Value :$
74 $\quad\quad VotedFor(a,\ b,\ v) \Rightarrow SafeAt(b,\ v)$

76 $OneVote \triangleq$
77 $\quad \forall\, a \in Acceptor,\ b \in Ballot,\ v,\ w \in Value :$
78 $\quad\quad VotedFor(a,\ b,\ v) \land VotedFor(a,\ b,\ w) \Rightarrow (v = w)$

80 $OneValuePerBallot \triangleq$
81 $\quad \forall\, a1,\ a2 \in Acceptor,\ b \in Ballot,\ v1,\ v2 \in Value :$
82 $\quad\quad VotedFor(a1,\ b,\ v1) \land VotedFor(a2,\ b,\ v2) \Rightarrow (v1 = v2)$

84 $Inv \triangleq TypeOK \land VotesSafe \land OneValuePerBallot$
85 ⊢———⊣
86 THEOREM $AllSafeAtZero \triangleq \forall\, v \in Value : SafeAt(0,\ v)$
87 BY DEF $SafeAt$

89 THEOREM $ChoosableThm \triangleq$
90 $\quad\quad \forall\, b \in Ballot,\ v \in Value :$
91 $\quad\quad\quad ChosenAt(b,\ v) \Rightarrow NoneOtherChoosableAt(b,\ v)$
92 BY DEF $ChosenAt,\ NoneOtherChoosableAt$

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

```
96 ├──────────────────────────────────────────────────────────────────────┤
97  THEOREM VotesSafeImpliesConsistency ≜
98     ASSUME VotesSafe, OneVote, chosen ≠ {}
99     PROVE  ∃ v ∈ Value : chosen = {v}
100 ⟨1⟩1. PICK v ∈ Value : v ∈ chosen
101   BY  DEF chosen
102 ⟨1⟩2. SUFFICES ASSUME NEW w ∈ chosen
103                  PROVE  w = v
104   BY ⟨1⟩1, ⟨1⟩2
105 ⟨1⟩3. ASSUME NEW b1 ∈ Ballot, NEW b2 ∈ Ballot, b1 < b2,
106                NEW v1 ∈ Value, NEW v2 ∈ Value,
107                ChosenAt(b1, v1) ∧ ChosenAt(b2, v2)
108       PROVE  v1 = v2
109   ⟨2⟩1. SafeAt(b2, v2)
110     BY ⟨1⟩3, QuorumAssumption, SMT DEF ChosenAt, VotesSafe
111   ⟨2⟩2. QED
112     BY ⟨1⟩3, ⟨2⟩1, QuorumAssumption, Z3
113     DEFS CannotVoteAt, DidNotVoteAt, OneVote,
114          ChosenAt, NoneOtherChoosableAt, Ballot, SafeAt
115 ⟨1⟩4. QED
116   BY QuorumAssumption, ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, Z3
117   DEFS Ballot, ChosenAt, OneVote, chosen

119 THEOREM ShowsSafety ≜
120              TypeOK ∧ VotesSafe ∧ OneValuePerBallot ⇒
121                ∀ Q ∈ Quorum, b ∈ Ballot, v ∈ Value :
122                  ShowsSafeAt(Q, b, v) ⇒ SafeAt(b, v)
123   BY QuorumAssumption, Z3
124   DEFS Ballot, TypeOK, VotesSafe, OneValuePerBallot, SafeAt,
125     ShowsSafeAt, CannotVoteAt, NoneOtherChoosableAt, DidNotVoteAt
126 ├──────────────────────────────────────────────────────────────────────┤
127 THEOREM Invariance ≜ Spec ⇒ □Inv
128 ⟨1⟩1. Init ⇒ Inv
129   BY  DEF Init, Inv, TypeOK, VotesSafe, VotedFor, OneValuePerBallot
130 ⟨1⟩2. Inv ∧ [Next]⟨votes, maxBal⟩ ⇒ Inv′
131   ⟨2⟩1.CASE ∧ Inv
132             ∧ Next
133     ⟨3⟩1. ASSUME NEW a ∈ Acceptor, NEW b ∈ Ballot,
134                  IncreaseMaxBal(a, b)
135           PROVE  Inv ∧ [Next]⟨votes, maxBal⟩ ⇒ Inv′
136       BY ⟨3⟩1
137     ⟨3⟩2. ASSUME NEW a ∈ Acceptor, NEW b ∈ Ballot,
138                  ∃ v ∈ Value : VoteFor(a, b, v)
139           PROVE  Inv ∧ [Next]⟨votes, maxBal⟩ ⇒ Inv′
140     ⟨3⟩3. QED
```

```
141         BY ⟨2⟩1, ⟨3⟩1, ⟨3⟩2  DEF Next
142     ⟨2⟩2.CASE  ∧ Inv
143                ∧ UNCHANGED ⟨votes, maxBal⟩
144       BY ⟨2⟩2
145       DEFS Inv, TypeOK, VotesSafe, OneValuePerBallot,
146            VotedFor, SafeAt, NoneOtherChoosableAt, CannotVoteAt, DidNotVoteAt
147     ⟨2⟩3. QED
148       BY ⟨2⟩1, ⟨2⟩2
149   ⟨1⟩3. QED
150     BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec

152     ⟨2⟩ USE  DEF Inv, TypeOK, VotesSafe, OneValuePerBallot, Ballot, VotedFor, VoteFor
153     NoneOtherChoosableAt, CannotVoteAt, DidNotVoteAt
154 ├──────────────────────────────────────────────────────────────────────────┤
155   C ≜ INSTANCE Consensus

157   THEOREM Spec ∧ Inv ⇒ C!Spec
158   ⟨1⟩1. Init ⇒ C!Init
159     BY QuorumAssumption, SetExtensionality, IsaM("force")
160      DEF Init, C!Init, chosen, ChosenAt, VotedFor
161   ⟨1⟩2. Next ∧ Inv ⇒ C!Next ∨ UNCHANGED chosen
162     ⟨2⟩1 SUFFICES ASSUME Next, InvPROVE  C!Next ∨ UNCHANGED chosen
163       BY ⟨2⟩1
164     ⟨2⟩2. chosen ⊆ chosen′
165       BY ⟨2⟩1, QuorumAssumption, Z3   SMTT(10) fails
166        DEF Next, Inv, TypeOK, IncreaseMaxBal, chosen, ChosenAt, VotedFor, Ballot, VoteFor
167     ⟨2⟩3. chosen′ = {} ∨ ∃ v ∈ Value : chosen′ = {v}
168       ⟨3⟩1. PICK a ∈ Acceptor, b ∈ Ballot :
169                  ∨ IncreaseMaxBal(a, b)
170                  ∨ ∃ v ∈ Value : VoteFor(a, b, v)
171         BY ⟨2⟩1  DEF Next
172       ⟨3⟩2.CASE IncreaseMaxBal(a, b)
173       ⟨3⟩3.CASE ∃ v ∈ Value : VoteFor(a, b, v)
174       ⟨3⟩q. QED
175         BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, SMT
176     ⟨2⟩q. QED
177       BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, OneVoteThm, VotesSafeImpliesConsistency, SetExtensionality, SMT
178        DEF Inv, C!Next
179   ⟨1⟩3. QED
180     PROOF OMITTED
181 └──────────────────────────────────────────────────────────────────────────┘
```