

```

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

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

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

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

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

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

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

```

48 $Next \triangleq$
 49 $\exists a \in Acceptor, b \in Ballot :$
 50 $\quad \vee IncreaseMaxBal(a, b)$
 51 $\quad \vee \exists v \in Value : VoteFor(a, b, v)$

53 $Spec \triangleq Init \wedge \Box[Next]_{\langle votes, maxBal \rangle}$
 54 \mid
 55 $ChosenAt(b, v) \triangleq$
 56 $\quad \exists Q \in Quorum : \forall a \in Q : VotedFor(a, b, v)$

58 $chosen \triangleq \{v \in Value : \exists b \in Ballot : ChosenAt(b, v)\}$
 60 $Consistency \triangleq chosen = \{\} \vee \exists v \in Value : chosen = \{v\}$ $Cardinality(chosen) \leq 1$

62 $CannotVoteAt(a, b) \triangleq$
 63 $\quad \wedge maxBal[a] > b$
 64 $\quad \wedge DidNotVoteAt(a, b)$

66 $NoneOtherChoosableAt(b, v) \triangleq$
 67 $\quad \exists Q \in Quorum :$
 68 $\quad \forall a \in Q : VotedFor(a, b, v) \vee CannotVoteAt(a, b)$

70 $SafeAt(b, v) \triangleq$
 71 $\quad \forall c \in 0 \dots (b - 1) : NoneOtherChoosableAt(c, v)$

73 $VotesSafe \triangleq$
 74 $\quad \forall a \in Acceptor, b \in Ballot, v \in Value :$
 75 $\quad VotedFor(a, b, v) \Rightarrow SafeAt(b, v)$

77 $OneVote \triangleq$
 78 $\quad \forall a \in Acceptor, b \in Ballot, v, w \in Value :$
 79 $\quad VotedFor(a, b, v) \wedge VotedFor(a, b, w) \Rightarrow (v = w)$

81 $OneValuePerBallot \triangleq$
 82 $\quad \forall a1, a2 \in Acceptor, b \in Ballot, v1, v2 \in Value :$
 83 $\quad VotedFor(a1, b, v1) \wedge VotedFor(a2, b, v2) \Rightarrow (v1 = v2)$

85 $Inv \triangleq TypeOK \wedge VotesSafe \wedge OneValuePerBallot$
 86 \mid
 87 THEOREM $AllSafeAtZero \triangleq \forall v \in Value : SafeAt(0, v)$
 88 BY DEF $SafeAt$

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

95 THEOREM $OneVoteThm \triangleq OneValuePerBallot \Rightarrow OneVote$

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

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

 128 THEOREM *SafeAtStable* $\triangleq \text{Inv} \wedge \text{Next} \wedge \text{TypeOK}' \Rightarrow$
 129 $\forall b \in \text{Ballot}, v \in \text{Value} :$
 130 $\text{SafeAt}(b, v) \Rightarrow \text{SafeAt}(b, v)'$
 131 OMITTED
 132
 133 THEOREM *Invariant* $\triangleq \text{Spec} \Rightarrow \Box \text{Inv}$
 134 $\langle 1 \rangle$ USE DEF *Inv*
 135 $\langle 1 \rangle 1$. *Init* $\Rightarrow \text{Inv}$
 136 BY DEF *Init*, *TypeOK*, *VotesSafe*, *OneValuePerBallot*, *VotedFor*
 137 $\langle 1 \rangle 2$. $\text{Inv} \wedge [\text{Next}]_{\langle \text{votes}, \text{maxBal} \rangle} \Rightarrow \text{Inv}'$
 138 $\langle 2 \rangle$ SUFFICES ASSUME *Inv*, $[\text{Next}]_{\langle \text{votes}, \text{maxBal} \rangle}$
 139 PROVE Inv'
 140 OBVIOUS

141 $\langle 2 \rangle 1.$ CASE *Next*
142 $\langle 3 \rangle$ SUFFICES ASSUME NEW $a \in \text{Acceptor}$, NEW $b \in \text{Ballot}$,
143 $\quad \vee \text{IncreaseMaxBal}(a, b)$
144 $\quad \vee \exists v \in \text{Value} : \text{VoteFor}(a, b, v)$
145 PROVE Inv'
146 BY $\langle 2 \rangle 1$ DEF *Next*
147 $\langle 3 \rangle 1.$ CASE *IncreaseMaxBal*(a, b)
148 $\langle 4 \rangle 1.$ *TypeOK'*
149 BY $\langle 3 \rangle 1$ DEF *TypeOK*, *IncreaseMaxBal*
150 $\langle 4 \rangle 2.$ *VotesSafe'*
151 $\langle 5 \rangle$ SUFFICES ASSUME NEW $a_1 \in \text{Acceptor}'$, NEW $b_1 \in \text{Ballot}'$, NEW $v \in \text{Value}'$
152 PROVE $\text{VotedFor}(a_1, b_1, v)' \Rightarrow \text{SafeAt}(b_1, v)'$
153 BY DEF *VotesSafe*
154 $\langle 5 \rangle 1.$ $\forall aa \in \text{Acceptor}, bb \in \text{Ballot}, vv \in \text{Value} :$
155 $\quad \text{VotedFor}(aa, bb, vv) \equiv \text{VotedFor}(aa, bb, vv)'$
156 BY $\langle 3 \rangle 1$ DEF *IncreaseMaxBal*, *VotedFor*
157 $\langle 5 \rangle 2.$ $\forall aa \in \text{Acceptor}, bb \in \text{Ballot} :$
158 $\quad \text{maxBal}[aa] > bb \Rightarrow \text{maxBal}'[aa] > bb$
159 BY $\langle 3 \rangle 1$ DEF *IncreaseMaxBal*, *TypeOK*, *Ballot*
160 $\langle 5 \rangle 3.$ $\forall aa \in \text{Acceptor}, bb \in \text{Ballot} :$
161 $\quad \text{DidNotVoteAt}(aa, bb) \Rightarrow \text{DidNotVoteAt}(aa, bb)'$
162 BY $\langle 3 \rangle 1$ DEF *IncreaseMaxBal*, *DidNotVoteAt*, *VotedFor*
163 $\langle 5 \rangle 4.$ $\forall aa \in \text{Acceptor}, bb \in \text{Ballot} :$
164 $\quad \text{CannotVoteAt}(aa, bb) \Rightarrow \text{CannotVoteAt}(aa, bb)'$
165 BY $\langle 3 \rangle 1, \langle 5 \rangle 2, \langle 5 \rangle 3$ DEF *IncreaseMaxBal*, *CannotVoteAt*
166 $\langle 5 \rangle 5.$ $\forall bb \in \text{Ballot}, vv \in \text{Value} :$
167 $\quad \text{NoneOtherChoosableAt}(bb, vv) \Rightarrow \text{NoneOtherChoosableAt}(bb, vv)'$
168 BY $\langle 5 \rangle 1, \langle 5 \rangle 4$, *QuorumAssumption* DEFS *NoneOtherChoosableAt*
169 $\langle 5 \rangle 6.$ QED
170 BY $\langle 5 \rangle 1, \langle 5 \rangle 5$ DEF *TypeOK*, *Ballot*, *VotesSafe*, *SafeAt*
171 $\langle 4 \rangle 3.$ *OneValuePerBallot'*
172 BY $\langle 3 \rangle 1$ DEF *IncreaseMaxBal*, *OneValuePerBallot*, *VotedFor*
173 $\langle 4 \rangle 4.$ QED
174 BY $\langle 4 \rangle 1, \langle 4 \rangle 2, \langle 4 \rangle 3$ DEF *Inv*
175 $\langle 3 \rangle 2.$ ASSUME NEW $v \in \text{Value}$,
176 $\quad \text{VoteFor}(a, b, v)$
177 PROVE Inv'
178 $\langle 4 \rangle$ SUFFICES ASSUME NEW $Q \in \text{Quorum}$,
179 $\quad \text{ShowsSafeAt}(Q, b, v)$
180 PROVE Inv'
181 BY $\langle 3 \rangle 2$ DEF *VoteFor*
182 $\langle 4 \rangle 1.$ *TypeOK'*
183 BY $\langle 3 \rangle 2$ DEF *TypeOK*, *VoteFor*
184 $\langle 4 \rangle 2.$ *VotesSafe'* Using *OneValuePerBallot* in *SafeAtStable*
185 $\langle 5 \rangle$ SUFFICES ASSUME NEW $aa \in \text{Acceptor}'$, NEW $bb \in \text{Ballot}'$, NEW $vv \in \text{Value}'$,

```

186                                     VotedFor(aa, bb, vv)'
187                               PROVE SafeAt(bb, vv)'
188       BY DEF VotesSafe
189       ⟨5⟩1.CASE VotedFor(aa, bb, vv)
190       ⟨6⟩1. SafeAt(bb, vv)
191       BY ⟨5⟩1 DEF VotesSafe
192       ⟨6⟩ QED
193       BY ⟨4⟩1, ⟨6⟩1, SafeAtStable DEF Next
194       ⟨5⟩2.CASE ¬ VotedFor(aa, bb, vv)
195       ⟨6⟩1. aa = a ∧ bb = b ∧ vv = v ∧ VotedFor(a, b, v)'
196       BY ⟨3⟩2, ⟨4⟩1, ⟨5⟩2 DEF VoteFor, VotedFor, TypeOK
197       ⟨6⟩ QED
198       BY ⟨4⟩1, ⟨6⟩1, ShowsSafety, SafeAtStable DEF VoteFor, Next
199       ⟨5⟩ QED
200       BY ⟨5⟩1, ⟨5⟩2
201       ⟨4⟩3. OneValuePerBallot'
202       BY ⟨3⟩2 DEF VoteFor, OneValuePerBallot, VotedFor, TypeOK
203       ⟨4⟩4. QED
204       BY ⟨3⟩2, ⟨4⟩1, ⟨4⟩2, ⟨4⟩3 DEF Inv
205       ⟨3⟩3. QED
206       BY ⟨2⟩1, ⟨3⟩1, ⟨3⟩2
207       ⟨2⟩2.CASE UNCHANGED ⟨votes, maxBal⟩
208       BY ⟨2⟩2
209       DEFS TypeOK, Next, VotesSafe, OneValuePerBallot,
210           VotedFor, SafeAt, NoneOtherChoosableAt, CannotVoteAt, DidNotVoteAt,
211           IncreaseMaxBal, VoteFor
212       ⟨2⟩3. QED
213       BY ⟨2⟩1, ⟨2⟩2
214       ⟨1⟩3. QED
215       BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec
216 |-----|
217 THEOREM Consistent  $\triangleq$  Spec  $\Rightarrow$  □ Consistency
218 ⟨1⟩ USE DEF Ballot
219 ⟨1⟩1. Inv  $\Rightarrow$  Consistency
220 ⟨2⟩ SUFFICES ASSUME Inv
221       PROVE Consistency
222       OBVIOUS
223       ⟨2⟩ QED
224       BY VotesSafeImpliesConsistency, OneVoteThm DEF Inv, Consistency
225       ⟨1⟩2. QED
226       BY Invariant, ⟨1⟩1, PTL
227 |-----|
228 C  $\triangleq$  INSTANCE Consensus WITH chosen  $\leftarrow$  chosen
229
230 THEOREM Refinement  $\triangleq$  Spec  $\Rightarrow$  C!Spec

```

