

```

1  ┌────────────────────────── MODULE EagerVoting ───────────────────┐
2  EXTENDS Sets
3  └──────────────────────────────────────────────────────────────────┘
4  CONSTANT Value, Acceptor, Quorum
5
6  ASSUME QuorumAssumption  $\triangleq$ 
7       $\wedge \forall Q \in \text{Quorum} : Q \subseteq \text{Acceptor}$ 
8       $\wedge \forall Q1, Q2 \in \text{Quorum} : Q1 \cap Q2 \neq \{\}$ 
9
10 THEOREM QuorumNonEmpty  $\triangleq \forall Q \in \text{Quorum} : Q \neq \{\}$ 
11 BY QuorumAssumption
12
13 Ballot  $\triangleq \text{Nat}$ 
14 └──────────────────────────────────────────────────────────────────┘
15 VARIABLES votes, maxBal
16
17 TypeOK  $\triangleq \wedge \text{votes} \in [\text{Acceptor} \rightarrow \text{SUBSET} (\text{Ballot} \times \text{Value})]$ 
18              $\wedge \text{maxBal} \in [\text{Acceptor} \rightarrow \text{Ballot} \cup \{-1\}]$ 
19 └──────────────────────────────────────────────────────────────────┘
20 VotedFor(a, b, v)  $\triangleq \langle b, v \rangle \in \text{votes}[a]$ 
21
22 DidNotVoteAt(a, b)  $\triangleq \forall v \in \text{Value} : \neg \text{VotedFor}(a, b, v)$ 
23
24 ShowsSafeAt(Q, b, v)  $\triangleq$ 
25      $\wedge \forall a \in Q : \text{maxBal}[a] \geq b$  have promised
26      $\wedge \exists c \in -1 \dots (b-1) :$ 
27          $\wedge (c \neq -1) \Rightarrow \exists a \in Q : \text{VotedFor}(a, c, v)$ 
28          $\wedge \forall d \in (c+1) \dots (b-1), a \in Q : \text{DidNotVoteAt}(a, d)$ 
29 └──────────────────────────────────────────────────────────────────┘
30 Init  $\triangleq$ 
31      $\wedge \text{votes} = [a \in \text{Acceptor} \mapsto \{\}]$ 
32      $\wedge \text{maxBal} = [a \in \text{Acceptor} \mapsto -1]$ 
33
34 IncreaseMaxBal(a, b)  $\triangleq$ 
35      $\wedge b > \text{maxBal}[a]$ 
36      $\wedge \text{maxBal}' = [\text{maxBal} \text{ EXCEPT } ![a] = b]$  make promise
37      $\wedge \text{UNCHANGED votes}$ 
38
39 ┌──────────────────────────────────────────────────────────────────┐
40 The only difference between EagerVoting and Voting is:
41 In Voting, we have  $\text{maxBal}' = [\text{maxBal} \text{ EXCEPT } ![a] = b]$ .
42 └──────────────────────────────────────────────────────────────────┘
43
44 VoteFor(a, b, v)  $\triangleq$ 
45      $\wedge \text{maxBal}[a] \leq b$  keep promise
46      $\wedge \forall vt \in \text{votes}[a] : vt[1] \neq b$ 
47      $\wedge \forall c \in \text{Acceptor} \setminus \{a\} :$ 
48          $\forall vt \in \text{votes}[c] : (vt[1] = b) \Rightarrow (vt[2] = v)$ 
49      $\wedge \exists Q \in \text{Quorum} : \text{ShowsSafeAt}(Q, b, v)$  safe to vote
50      $\wedge \text{votes}' = [\text{votes} \text{ EXCEPT } ![a] = @ \cup \{\langle b, v \rangle\}]$  vote

```

51 $\wedge \exists c \in \text{Ballot} :$
52 $\quad \wedge c \geq b$
53 $\quad \wedge \text{maxBal}' = [\text{maxBal} \text{ EXCEPT } ![a] = c] \text{ make promise}$
54 $\quad \text{Next} \triangleq$
55 $\quad \exists a \in \text{Acceptor}, b \in \text{Ballot} :$
56 $\quad \quad \vee \text{IncreaseMaxBal}(a, b)$
57 $\quad \quad \vee \exists v \in \text{Value} : \text{VoteFor}(a, b, v)$
60 $\text{Spec} \triangleq \text{Init} \wedge \square[\text{Next}]_{\langle \text{votes}, \text{maxBal} \rangle}$
61 $\quad \text{ChosenAt}(b, v) \triangleq$
62 $\quad \quad \exists Q \in \text{Quorum} : \forall a \in Q : \text{VotedFor}(a, b, v)$
65 $\text{chosen} \triangleq \{v \in \text{Value} : \exists b \in \text{Ballot} : \text{ChosenAt}(b, v)\}$
67 $\text{Consistency} \triangleq \text{chosen} = \{\} \vee \exists v \in \text{Value} : \text{chosen} = \{v\} \text{ Cardinality}(\text{chosen}) \leq 1$
68 $\quad \text{CannotVoteAt}(a, b) \triangleq$
69 $\quad \quad \wedge \text{maxBal}[a] > b$
70 $\quad \quad \wedge \text{DidNotVoteAt}(a, b)$
73 $\text{NoneOtherChoosableAt}(b, v) \triangleq$
74 $\quad \exists Q \in \text{Quorum} :$
75 $\quad \quad \forall a \in Q : \text{VotedFor}(a, b, v) \vee \text{CannotVoteAt}(a, b)$
77 $\text{SafeAt}(b, v) \triangleq$
78 $\quad \forall c \in 0 \dots (b - 1) : \text{NoneOtherChoosableAt}(c, v)$
80 $\text{VotesSafe} \triangleq$
81 $\quad \forall a \in \text{Acceptor}, b \in \text{Ballot}, v \in \text{Value} :$
82 $\quad \quad \text{VotedFor}(a, b, v) \Rightarrow \text{SafeAt}(b, v)$
84 $\text{OneVote} \triangleq$
85 $\quad \forall a \in \text{Acceptor}, b \in \text{Ballot}, v, w \in \text{Value} :$
86 $\quad \quad \text{VotedFor}(a, b, v) \wedge \text{VotedFor}(a, b, w) \Rightarrow (v = w)$
88 $\text{OneValuePerBallot} \triangleq$
89 $\quad \forall a1, a2 \in \text{Acceptor}, b \in \text{Ballot}, v1, v2 \in \text{Value} :$
90 $\quad \quad \text{VotedFor}(a1, b, v1) \wedge \text{VotedFor}(a2, b, v2) \Rightarrow (v1 = v2)$
92 $\text{Inv} \triangleq \text{TypeOK} \wedge \text{VotesSafe} \wedge \text{OneValuePerBallot}$
93 $\quad \text{THEOREM } \text{AllSafeAtZero} \triangleq \forall v \in \text{Value} : \text{SafeAt}(0, v)$
94 $\quad \text{BY DEF } \text{SafeAt}$
97 $\text{THEOREM } \text{ChoosableThm} \triangleq$
98 $\quad \forall b \in \text{Ballot}, v \in \text{Value} :$

99 $ChosenAt(b, v) \Rightarrow NoneOtherChoosableAt(b, v)$
 100 BY DEF *ChosenAt*, *NoneOtherChoosableAt*

102 THEOREM *OneVoteThm* $\triangleq OneValuePerBallot \Rightarrow OneVote$
 103 BY DEF *OneValuePerBallot*, *OneVote*

104
 105 THEOREM *VotesSafeImpliesConsistency* \triangleq
 106 ASSUME *VotesSafe*, *OneVote*, *chosen* $\neq \{\}$
 107 PROVE $\exists v \in Value : chosen = \{v\}$
 108 <1>1. PICK $v \in Value : v \in chosen$
 109 BY DEF *chosen*
 110 <1>2. SUFFICES ASSUME NEW $w \in chosen$
 111 PROVE $w = v$
 112 BY <1>1, <1>2
 113 <1>3. ASSUME NEW $b1 \in Ballot$, NEW $b2 \in Ballot$, $b1 < b2$,
 114 NEW $v1 \in Value$, NEW $v2 \in Value$,
 115 $ChosenAt(b1, v1) \wedge ChosenAt(b2, v2)$
 116 PROVE $v1 = v2$
 117 <2>1. *SafeAt*($b2, v2$)
 118 BY <1>3, *QuorumAssumption*, SMT DEF *ChosenAt*, *VotesSafe*
 119 <2>2. QED
 120 BY <1>3, <2>1, *QuorumAssumption*, Z3
 121 DEFS *CannotVoteAt*, *DidNotVoteAt*, *OneVote*,
 122 *ChosenAt*, *NoneOtherChoosableAt*, *Ballot*, *SafeAt*
 123 <1>4. QED
 124 BY *QuorumAssumption*, <1>1, <1>2, <1>3, Z3
 125 DEFS *Ballot*, *ChosenAt*, *OneVote*, *chosen*

127 THEOREM *ShowsSafety* \triangleq
 128 $TypeOK \wedge VotesSafe \wedge OneValuePerBallot \Rightarrow$
 129 $\forall Q \in Quorum, b \in Ballot, v \in Value :$
 130 $ShowsSafeAt(Q, b, v) \Rightarrow SafeAt(b, v)$
 131 BY *QuorumAssumption*, Z3
 132 DEFS *Ballot*, *TypeOK*, *VotesSafe*, *OneValuePerBallot*, *SafeAt*,
 133 *ShowsSafeAt*, *CannotVoteAt*, *NoneOtherChoosableAt*, *DidNotVoteAt*

135 THEOREM *SafeAtStable* $\triangleq Inv \wedge Next \wedge TypeOK' \Rightarrow$
 136 $\forall b \in Ballot, v \in Value :$
 137 $SafeAt(b, v) \Rightarrow SafeAt(b, v)'$
 138 OMITTED

139
 140 THEOREM *Invariant* $\triangleq Spec \Rightarrow \Box Inv$
 141 <1> USE DEF *Inv*
 142 <1>1. *Init* $\Rightarrow Inv$
 143 BY DEF *Init*, *TypeOK*, *VotesSafe*, *OneValuePerBallot*, *VotedFor*
 144 <1>2. $Inv \wedge [Next]_{\langle votes, maxBal \rangle} \Rightarrow Inv'$

145 $\langle 2 \rangle$ SUFFICES ASSUME $Inv, [Next]_{\langle votes, maxBal \rangle}$
146 PROVE Inv'
147 OBVIOUS
148 $\langle 2 \rangle 1$. CASE $Next$
149 $\langle 3 \rangle$ SUFFICES ASSUME NEW $a \in Acceptor$, NEW $b \in Ballot$,
150 $\vee IncreaseMaxBal(a, b)$
151 $\vee \exists v \in Value : VoteFor(a, b, v)$
152 PROVE Inv'
153 BY $\langle 2 \rangle 1$ DEF $Next$
154 $\langle 3 \rangle 1$. CASE $IncreaseMaxBal(a, b)$
155 $\langle 4 \rangle 1$. $TypeOK'$
156 BY $\langle 3 \rangle 1$ DEF $TypeOK, IncreaseMaxBal$
157 $\langle 4 \rangle 2$. $VotesSafe'$
158 $\langle 5 \rangle$ SUFFICES ASSUME NEW $a_{-1} \in Acceptor'$, NEW $b_{-1} \in Ballot'$, NEW $v \in Value'$
159 PROVE $VotedFor(a_{-1}, b_{-1}, v)' \Rightarrow SafeAt(b_{-1}, v)'$
160 BY DEF $VotesSafe$
161 $\langle 5 \rangle 1$. $\forall aa \in Acceptor, bb \in Ballot, vv \in Value :$
162 $VotedFor(aa, bb, vv) \equiv VotedFor(aa, bb, vv)'$
163 BY $\langle 3 \rangle 1$ DEF $IncreaseMaxBal, VotedFor$
164 $\langle 5 \rangle 2$. $\forall aa \in Acceptor, bb \in Ballot :$
165 $maxBal[aa] > bb \Rightarrow maxBal'[aa] > bb$
166 BY $\langle 3 \rangle 1$ DEF $IncreaseMaxBal, TypeOK, Ballot$
167 $\langle 5 \rangle 3$. $\forall aa \in Acceptor, bb \in Ballot :$
168 $DidNotVoteAt(aa, bb) \Rightarrow DidNotVoteAt(aa, bb)'$
169 BY $\langle 3 \rangle 1$ DEF $IncreaseMaxBal, DidNotVoteAt, VotedFor$
170 $\langle 5 \rangle 4$. $\forall aa \in Acceptor, bb \in Ballot :$
171 $CannotVoteAt(aa, bb) \Rightarrow CannotVoteAt(aa, bb)'$
172 BY $\langle 3 \rangle 1, \langle 5 \rangle 2, \langle 5 \rangle 3$ DEF $IncreaseMaxBal, CannotVoteAt$
173 $\langle 5 \rangle 5$. $\forall bb \in Ballot, vv \in Value :$
174 $NoneOtherChoosableAt(bb, vv) \Rightarrow NoneOtherChoosableAt(bb, vv)'$
175 BY $\langle 5 \rangle 1, \langle 5 \rangle 4, QuorumAssumption$ DEFS $NoneOtherChoosableAt$
176 $\langle 5 \rangle 6$. QED
177 BY $\langle 5 \rangle 1, \langle 5 \rangle 5$ DEF $TypeOK, Ballot, VotesSafe, SafeAt$
178 $\langle 4 \rangle 3$. $OneValuePerBallot'$
179 BY $\langle 3 \rangle 1$ DEF $IncreaseMaxBal, OneValuePerBallot, VotedFor$
180 $\langle 4 \rangle 4$. QED
181 BY $\langle 4 \rangle 1, \langle 4 \rangle 2, \langle 4 \rangle 3$ DEF Inv
182 $\langle 3 \rangle 2$. ASSUME NEW $v \in Value$,
183 $VoteFor(a, b, v)$
184 PROVE Inv'
185 $\langle 4 \rangle$ SUFFICES ASSUME NEW $Q \in Quorum$,
186 $ShowsSafeAt(Q, b, v)$
187 PROVE Inv'
188 BY $\langle 3 \rangle 2$ DEF $VoteFor$
189 $\langle 4 \rangle 1$. $TypeOK'$

190 BY $\langle 3 \rangle 2$ DEF *TypeOK*, *VoteFor*
 191 $\langle 4 \rangle 2$. *VotesSafe'* Using *OneValuePerBallot* in *SafeAtStable*
 192 $\langle 5 \rangle$ SUFFICES ASSUME NEW *aa* \in *Acceptor'*, NEW *bb* \in *Ballot'*, NEW *vv* \in *Value'*,
 193 *VotedFor*(*aa*, *bb*, *vv*)'
 194 PROVE *SafeAt*(*bb*, *vv*)'
 195 BY DEF *VotesSafe*
 196 $\langle 5 \rangle 1$. CASE *VotedFor*(*aa*, *bb*, *vv*)
 197 $\langle 6 \rangle 1$. *SafeAt*(*bb*, *vv*)
 198 BY $\langle 5 \rangle 1$ DEF *VotesSafe*
 199 $\langle 6 \rangle$ QED
 200 BY $\langle 4 \rangle 1$, $\langle 6 \rangle 1$, *SafeAtStable* DEF *Next*
 201 $\langle 5 \rangle 2$. CASE \neg *VotedFor*(*aa*, *bb*, *vv*)
 202 $\langle 6 \rangle 1$. *aa* = *a* \wedge *bb* = *b* \wedge *vv* = *v* \wedge *VotedFor*(*a*, *b*, *v*)'
 203 BY $\langle 3 \rangle 2$, $\langle 4 \rangle 1$, $\langle 5 \rangle 2$ DEF *VoteFor*, *VotedFor*, *TypeOK*
 204 $\langle 6 \rangle$ QED
 205 BY $\langle 4 \rangle 1$, $\langle 6 \rangle 1$, *ShowsSafety*, *SafeAtStable* DEF *VoteFor*, *Next*
 206 $\langle 5 \rangle$ QED
 207 BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$
 208 $\langle 4 \rangle 3$. *OneValuePerBallot'*
 209 BY $\langle 3 \rangle 2$ DEF *VoteFor*, *OneValuePerBallot*, *VotedFor*, *TypeOK*
 210 $\langle 4 \rangle 4$. QED
 211 BY $\langle 3 \rangle 2$, $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEF *Inv*
 212 $\langle 3 \rangle 3$. QED
 213 BY $\langle 2 \rangle 1$, $\langle 3 \rangle 1$, $\langle 3 \rangle 2$
 214 $\langle 2 \rangle 2$. CASE UNCHANGED \langle votes, *maxBal* \rangle
 215 BY $\langle 2 \rangle 2$
 216 DEFS *TypeOK*, *Next*, *VotesSafe*, *OneValuePerBallot*,
 217 *VotedFor*, *SafeAt*, *NoneOtherChoosableAt*, *CannotVoteAt*, *DidNotVoteAt*,
 218 *IncreaseMaxBal*, *VoteFor*
 219 $\langle 2 \rangle 3$. QED
 220 BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$
 221 $\langle 1 \rangle 3$. QED
 222 BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, *PTL* DEF *Spec*
 223 |-----|
 224 THEOREM *Consistent* \triangleq *Spec* \Rightarrow \square *Consistency*
 225 $\langle 1 \rangle$ USE DEF *Ballot*
 226 $\langle 1 \rangle 1$. *Inv* \Rightarrow *Consistency*
 227 $\langle 2 \rangle$ SUFFICES ASSUME *Inv*
 228 PROVE *Consistency*
 229 OBVIOUS
 230 $\langle 2 \rangle$ QED
 231 BY *VotesSafeImpliesConsistency*, *OneVoteThm* DEF *Inv*, *Consistency*
 232 $\langle 1 \rangle 2$. QED
 233 BY *Invariant*, $\langle 1 \rangle 1$, *PTL*
 234 |-----|

235 $C \triangleq$ INSTANCE *Consensus* WITH *chosen* \leftarrow *chosen*
 237 THEOREM *Refinement* \triangleq *Spec* \Rightarrow *C!Spec*
 238 $\langle 1 \rangle 1$. *Init* \Rightarrow *C!Init*
 239 BY *QuorumAssumption*, *SetExtensionality*, *IsaM*("force")
 240 DEF *Init*, *C!Init*, *chosen*, *ChosenAt*, *VotedFor*
 241 $\langle 1 \rangle 2$. *TypeOK'* \wedge *Consistency'* \wedge [*Next*] _{$\langle votes, maxBal \rangle$} \Rightarrow [*C!Next*]_{*chosen*}
 242 $\langle 2 \rangle 1$. UNCHANGED $\langle votes, maxBal \rangle \Rightarrow$ UNCHANGED *chosen*
 243 BY DEF *chosen*, *ChosenAt*, *VotedFor*
 244 $\langle 2 \rangle 2$. *TypeOK'* \wedge *Consistency'* \wedge *Next* \Rightarrow *C!Next* \vee UNCHANGED *chosen*
 245 $\langle 3 \rangle 1$. SUFFICES ASSUME *TypeOK'*, *Consistency'*, *Next*
 246 PROVE *C!Next* \vee UNCHANGED *chosen*
 247 OBVIOUS
 248 $\langle 3 \rangle 2$. *chosen* \subseteq *chosen'*
 249 BY $\langle 3 \rangle 1$, *QuorumAssumption*, Z3
 250 DEFS *Next*, *IncreaseMaxBal*, *VoteFor*, *Inv*, *TypeOK*, *chosen*, *ChosenAt*, *VotedFor*, *Ballot*
 251 $\langle 3 \rangle 3$. *chosen'* = $\{\}$ $\vee \exists v \in Value : chosen' = \{v\}$
 252 BY $\langle 3 \rangle 1$ DEF *Consistency*
 253 $\langle 3 \rangle 4$. QED
 254 BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$ DEF *C!Next*
 255 $\langle 2 \rangle 3$. QED
 256 BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$
 257 $\langle 1 \rangle 3$. QED
 258 BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, *Invariant*, *Consistent*, *PTL* DEF *Spec*, *Inv*, *C!Spec*
 259