─────────────────────── MODULE *EagerVoting* ───────────────────────

1

2 EXTENDS *Sets*

3 ├──

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

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

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

13 $Ballot \triangleq Nat$

14 ├──

15 VARIABLES *votes*, *maxBal*

17 $TypeOK \triangleq \land votes \in [Acceptor \rightarrow \text{SUBSET } (Ballot \times Value)]$
18                   $\land maxBal \in [Acceptor \rightarrow Ballot \cup \{-1\}]$

19 ├──

20 $VotedFor(a, b, v) \triangleq \langle b, v \rangle \in votes[a]$

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

24 $ShowsSafeAt(Q, b, v) \triangleq$
25     $\land \forall a \in Q : maxBal[a] \geq b$ `have promised`
26     $\land \exists c \in \quad -1 \dots (b-1) :$
27         $\land (c \neq -1) \Rightarrow \exists a \in Q : VotedFor(a, c, v)$
28         $\land \forall d \in (c+1) \dots (b-1), a \in Q : DidNotVoteAt(a, d)$

29 ├──

30 $Init \triangleq$
31     $\land votes = [a \in Acceptor \mapsto \{\}]$
32     $\land maxBal = [a \in Acceptor \mapsto -1]$

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

The only difference between *EagerVoting* and *Voting* is:

In *Voting*, we have $maxBal' = [maxBal \text{ EXCEPT } ![a] = b]$.

44 $VoteFor(a, b, v) \triangleq$
45     $\land \quad maxBal[a] \leq b$ `keep promise`
46     $\land \quad \forall vt \in votes[a] : vt[1] \neq b$
47     $\land \quad \forall c \in Acceptor \setminus \{a\} :$
48         $\forall vt \in votes[c] : (vt[1] = b) \Rightarrow (vt[2] = v)$
49     $\land \quad \exists Q \in Quorum : ShowsSafeAt(Q, b, v)$ `safe to vote`
50     $\land \quad votes' = [votes \text{ EXCEPT } ![a] = votes[a] \cup \{\langle b, v \rangle\}]$ `vote`

1

```
51          ∧  ∃ c ∈ Value :
52                ∧ c ≥ b
53                ∧ maxBal′ = [maxBal EXCEPT ![a] = c]  make promise
```

```
55   Next  ≜
56        ∃ a ∈ Acceptor, b ∈ Ballot :
57           ∨ IncreaseMaxBal(a, b)
58           ∨ ∃ v ∈ Value : VoteFor(a, b, v)
```

```
60   Spec  ≜  Init ∧ □[Next]⟨votes, maxBal⟩
```

```
62   ChosenAt(b, v)  ≜
63        ∃ Q ∈ Quorum : ∀ a ∈ Q : VotedFor(a, b, v)
```

```
65   chosen  ≜  {v ∈ Value : ∃ b ∈ Ballot : ChosenAt(b, v)}
```

```
67   Consistency  ≜  chosen = {} ∨ ∃ v ∈ Value : chosen = {v}  Cardinality(chosen) ≤ 1
```

```
69   CannotVoteAt(a, b)  ≜
70        ∧ maxBal[a] > b
71        ∧ DidNotVoteAt(a, b)
```

```
73   NoneOtherChoosableAt(b, v)  ≜
74        ∃ Q ∈ Quorum :
75           ∀ a ∈ Q : VotedFor(a, b, v) ∨ CannotVoteAt(a, b)
```

```
77   SafeAt(b, v)  ≜
78        ∀ c ∈ 0 .. (b − 1) : NoneOtherChoosableAt(c, v)
```

```
80   VotesSafe  ≜
81        ∀ a ∈ Acceptor, b ∈ Ballot, v ∈ Value :
82           VotedFor(a, b, v) ⇒ SafeAt(b, v)
```

```
84   OneVote  ≜
85        ∀ a ∈ Acceptor, b ∈ Ballot, v, w ∈ Value :
86           VotedFor(a, b, v) ∧ VotedFor(a, b, w) ⇒ (v = w)
```

```
88   OneValuePerBallot  ≜
89        ∀ a1, a2 ∈ Acceptor, b ∈ Ballot, v1, v2 ∈ Value :
90           VotedFor(a1, b, v1) ∧ VotedFor(a2, b, v2) ⇒ (v1 = v2)
```

```
92   Inv  ≜  TypeOK ∧ VotesSafe ∧ OneValuePerBallot
```

```
94   THEOREM AllSafeAtZero  ≜  ∀ v ∈ Value : SafeAt(0, v)
95      BY  DEF SafeAt
```

```
97   THEOREM ChoosableThm  ≜
98                ∀ b ∈ Ballot, v ∈ Value :
```

```
 99              ChosenAt(b, v) ⇒ NoneOtherChoosableAt(b, v)
100    BY  DEF ChosenAt, NoneOtherChoosableAt

102  THEOREM OneVoteThm  ≜  OneValuePerBallot ⇒ OneVote
103    BY  DEF OneValuePerBallot, OneVote
104 ⊢─────────────────────────────────────────────────────────────────
105  THEOREM VotesSafeImpliesConsistency  ≜
106     ASSUME VotesSafe, OneVote, chosen ≠ {}
107     PROVE  ∃ v ∈ Value : chosen = {v}
108  ⟨1⟩1. PICK v ∈ Value : v ∈ chosen
109    BY  DEF chosen
110  ⟨1⟩2. SUFFICES ASSUME NEW w ∈ chosen
111               PROVE   w = v
112    BY ⟨1⟩1, ⟨1⟩2
113  ⟨1⟩3. ASSUME NEW b1 ∈ Ballot, NEW b2 ∈ Ballot, b1 < b2,
114               NEW v1 ∈ Value, NEW v2 ∈ Value,
115               ChosenAt(b1, v1) ∧ 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  ≜
128             TypeOK ∧ VotesSafe ∧ OneValuePerBallot ⇒
129               ∀ Q ∈ Quorum, b ∈ Ballot, v ∈ Value :
130                 ShowsSafeAt(Q, b, v) ⇒ SafeAt(b, v)
131    BY QuorumAssumption, Z3
132    DEFS Ballot, TypeOK, VotesSafe, OneValuePerBallot, SafeAt,
133      ShowsSafeAt, CannotVoteAt, NoneOtherChoosableAt, DidNotVoteAt

135  THEOREM SafeAtStable  ≜  Inv ∧ Next ∧ TypeOK' ⇒
136                            ∀ b ∈ Ballot, v ∈ Value :
137                              SafeAt(b, v) ⇒ SafeAt(b, v)'
138    OMITTED
139 ⊢─────────────────────────────────────────────────────────────────
140  THEOREM Invariant  ≜  Spec ⇒ □Inv
141  ⟨1⟩ USE  DEF Inv
142  ⟨1⟩1. Init ⇒ Inv
143    BY  DEF Init, TypeOK, VotesSafe, OneValuePerBallot, VotedFor
144  ⟨1⟩2. Inv ∧ [Next]_{⟨votes, maxBal⟩} ⇒ 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 ⟨3⟩2  DEF TypeOK, VoteFor
191     ⟨4⟩2. VotesSafe′  Using OneValuePerBallot in SafeAtStable
192        ⟨5⟩ SUFFICES ASSUME NEW aa ∈ Acceptor′, NEW bb ∈ Ballot′, NEW vv ∈ Value′,
193                              VotedFor(aa, bb, vv)′
194                     PROVE   SafeAt(bb, vv)′
195          BY  DEF VotesSafe
196        ⟨5⟩1.CASE VotedFor(aa, bb, vv)
197          ⟨6⟩1. SafeAt(bb, vv)
198            BY ⟨5⟩1  DEF VotesSafe
199          ⟨6⟩ QED
200            BY ⟨4⟩1, ⟨6⟩1, SafeAtStable DEF Next
201        ⟨5⟩2.CASE ¬VotedFor(aa, bb, vv)
202          ⟨6⟩1. aa = a ∧ bb = b ∧ vv = v ∧ VotedFor(a, b, v)′
203            BY ⟨3⟩2, ⟨4⟩1, ⟨5⟩2  DEF VoteFor, VotedFor, TypeOK
204          ⟨6⟩ QED
205            BY ⟨4⟩1, ⟨6⟩1, ShowsSafety, SafeAtStable DEF VoteFor, Next
206        ⟨5⟩ QED
207          BY ⟨5⟩1, ⟨5⟩2
208     ⟨4⟩3. OneValuePerBallot′
209        BY ⟨3⟩2  DEF VoteFor, OneValuePerBallot, VotedFor, TypeOK
210     ⟨4⟩4. QED
211        BY ⟨3⟩2, ⟨4⟩1, ⟨4⟩2, ⟨4⟩3  DEF Inv
212   ⟨3⟩3. QED
213     BY ⟨2⟩1, ⟨3⟩1, ⟨3⟩2
214 ⟨2⟩2.CASE UNCHANGED ⟨votes, maxBal⟩
215   BY ⟨2⟩2
216   DEFS TypeOK, Next, VotesSafe, OneValuePerBallot,
217        VotedFor, SafeAt, NoneOtherChoosableAt, CannotVoteAt, DidNotVoteAt,
218        IncreaseMaxBal, VoteFor
219 ⟨2⟩3. QED
220   BY ⟨2⟩1, ⟨2⟩2
221 ⟨1⟩3. QED
222   BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec
223 ⊢──────────────────────────────────────────────────────────────
224 THEOREM Consistent ≜ Spec ⇒ □Consistency
225 ⟨1⟩ USE  DEF Ballot
226 ⟨1⟩1. Inv ⇒ Consistency
227   ⟨2⟩ SUFFICES ASSUME Inv
228               PROVE   Consistency
229   OBVIOUS
230   ⟨2⟩ QED
231     BY VotesSafeImpliesConsistency, OneVoteThm DEF Inv, Consistency
232 ⟨1⟩2. QED
233   BY Invariant, ⟨1⟩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 $QuorumAssumption,\ SetExtensionality,\ IsaM(\text{"force"})$
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