```
MODULE UniversalPaxosStoreWithVotes
Extend UniversalPaxosStore with an explicit record of votes that have been accepted by participants. This is used to demonstrate that UniversalPaxosStore refines EagerVoting.
EXTENDS UniversalPaxosStore, TLAPS

VARIABLE votes

TypeOKV ≜
    ∧ TypeOK
    ∧ votes ∈ [Participant → SUBSET (Ballot × Value)]

InitV ≜
    ∧ Init
    ∧ votes = [p ∈ Participant ↦ {}]

PrepareV(p, b) ≜
    ∧ Prepare(p, b)
    ∧ UNCHANGED votes

UpdateStateV(q, p, pp) ≜
    ∧ UpdateState(q, p, pp)
    ∧ IF state[q][q].maxBal ≤ pp.maxVBal ∧ pp.maxVBal ≠ −1 accept
      THEN votes' = [votes EXCEPT ![q] = @ ∪ {⟨pp.maxVBal, pp.maxVVal⟩}]
      ELSE UNCHANGED votes

OnMessageV(q) ≜
  ∃ m ∈ msgs :
    ∧ q ∈ m.to
    ∧ LET p ≜ m.from
        IN  UpdateStateV(q, p, m.state[p]) replacing UpdateState
    ∧ IF ∨ m.state[q].maxBal < state'[q][q].maxBal
         ∨ m.state[q].maxVBal < state'[q][q].maxVBal
      THEN Send([from ↦ q, to ↦ {m.from}, state ↦ state'[q]])
      ELSE UNCHANGED msgs

AcceptV(p, b, v) ≜
    ∧  Accept(p, b, v)
    ∧  votes' = [votes EXCEPT ![p] = @ ∪ {⟨b, v⟩}] accept

NextV ≜ ∃ p ∈ Participant : ∨ OnMessageV(p)
                            ∨ ∃ b ∈ Ballot : ∨ PrepareV(p, b)
                                             ∨ ∃ v ∈ Value : AcceptV(p, b, v)
SpecV ≜ InitV ∧ □[NextV]⟨vars, votes⟩

THEOREM Invariant ≜ SpecV ⇒ □TypeOKV
  OMITTED
```

UniversalPaxosStore refines *EagerVoting*.

54 $maxBal \triangleq [p \in Participant \mapsto state[p][p].maxBal]$

56 $EV \triangleq$ INSTANCE *EagerVoting* WITH $Acceptor \leftarrow Participant$

58 THEOREM $SpecV \Rightarrow EV!Spec$
59 $\langle 1\rangle 1.\ InitV \Rightarrow EV!Init$
60 BY DEF $InitV$, $Init$, $EV!Init$, $InitState$, $maxBal$
61 $\langle 1\rangle 2.\ TypeOKV' \land [NextV]_{\langle vars,\ votes\rangle} \Rightarrow [EV!Next]_{\langle votes,\ maxBal\rangle}$
62 $\langle 2\rangle 1.$ UNCHANGED $\langle state,\ msgs,\ votes\rangle \Rightarrow$ UNCHANGED $\langle votes,\ maxBal\rangle$
63 BY DEF $maxBal$
64 $\langle 2\rangle 2.\ TypeOKV' \land NextV \Rightarrow EV!Next \lor$ UNCHANGED $\langle votes,\ maxBal\rangle$
65 $\langle 3\rangle$ USE DEF $TypeOK$, $EV!Ballot$, $Ballot$
66 $\langle 3\rangle 1.$ ASSUME NEW $q \in Participant$,
67 $OnMessageV(q)$,
68 $\langle votes,\ maxBal\rangle' \neq \langle votes,\ maxBal\rangle$
69 PROVE $EV!Next$
70 $\langle 4\rangle 1.\ \exists\, p \in Participant,\ b \in Ballot,\ v \in Value : EV!VoteFor(p,\ b,\ v)$
71 $\langle 5\rangle$ SUFFICES ASSUME NEW $m \in msgs$,
72 $\land\ q \in m.to$
73 $\land\ UpdateStateV(q,\ m.from,\ m.state[m.from])$
74 PROVE $\exists\, p \in Participant,\ b \in Ballot,\ v \in Value : EV!VoteFor(p,\ b,\ v)$
75 BY $\langle 3\rangle 1$ DEF $OnMessageV$
76 $\langle 5\rangle$ QED
77 $\langle 4\rangle$ QED
78 BY $\langle 3\rangle 1$, $\langle 4\rangle 1$ DEF $EV!Next$
79 $\langle 3\rangle 2.$ ASSUME NEW $p \in Participant$,
80 NEW $b \in Ballot$,
81 $PrepareV(p,\ b)$
82 PROVE $EV!Next$
83 $\langle 4\rangle 1.\ EV!IncreaseMaxBal(p,\ b)$
84 $\langle 5\rangle 1.\ b > maxBal[p]$
85 BY $\langle 3\rangle 2$ DEF $maxBal$, $PrepareV$, $Prepare$
86 $\langle 5\rangle 2.\ maxBal' = [maxBal$ EXCEPT $![p] = b]$
87 BY $\langle 3\rangle 2$ DEF $maxBal$, $PrepareV$, $Prepare$, $Ballot$
88 $\langle 5\rangle 3.$ UNCHANGED $votes$
89 BY $\langle 3\rangle 2$ DEF $PrepareV$
90 $\langle 5\rangle 4.$ QED
91 BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ DEF $EV!IncreaseMaxBal$
92 $\langle 4\rangle 2.$ QED
93 BY $\langle 3\rangle 2$, $\langle 4\rangle 1$ DEF $EV!Next$
BY $\langle 3\rangle 2$ DEF $TypeOKV$, $EV!TypeOK$, $TypeOK$, $EV!Next$, $EV!IncreaseMaxBal$, $EV!Ballot$, $PrepareV$, $Prepare$, $Ballot$, $maxBal$
97 $\langle 3\rangle 3.$ ASSUME NEW $p \in Participant$,
98 NEW $b \in Ballot$,

```
                    NEW v ∈ Value,
                    AcceptV(p, b, v)
          PROVE  EV!Next ∨ UNCHANGED ⟨votes, maxBal⟩
      ⟨4⟩1. EV!VoteFor(p, b, v)
      ⟨4⟩.QED
        BY ⟨3⟩3, ⟨4⟩1  DEF EV!Next
    ⟨3⟩4. QED
      BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3  DEF NextV
  ⟨2⟩3. QED
    BY ⟨2⟩1, ⟨2⟩2  DEF vars
⟨1⟩3. QED
  BY ⟨1⟩1, ⟨1⟩2, Invariant, PTL DEF SpecV, EV!Spec
```

* Modification History
* Last modified *Thu Aug* 15 16:15:18 *CST* 2019 by *hengxin*
* Created *Wed Aug* 14 14:05:06 *CST* 2019 by *hengxin*