```
┌──────────────────────────── MODULE PaxosProof ────────────────────────────┐
EXTENDS TLAPS, PaxosTuple

WellFormedMessages ≜ ∀ m ∈ msgs :
     ∧ m[1] = “1a” ⇒ m[2]     ∈ Ballot
     ∧ m[1] = “1b” ⇒ ∧ m[2] ∈ Acceptor
                       ∧ m[3] ∈ Ballot
                       ∧ m[4] ∈ Ballot ∪ {−1}
                       ∧ m[5] ∈ Value ∪ {None}
     ∧ m[1] = “2a” ⇒ m[2] ∈ Ballot ∧ m[3] ∈ Value
     ∧ m[1] = “2b” ⇒ m[2] ∈ Acceptor ∧ m[3] ∈ Ballot ∧ m[4] ∈ Value
├────────────────────────────────────────────────────────────────────────────┤
THEOREM WFmsgs ≜ TypeOK ⇒ WellFormedMessages
  BY Z3DEFS Ballot, TypeOK, Message, WellFormedMessages

THEOREM typing ≜ Spec ⇒ □TypeOK
⟨1⟩.USE DEFS Ballot, TypeOK
⟨1⟩1. Init ⇒ TypeOK
  BY SMTDEFS Init
⟨1⟩2. TypeOK ∧ [Next]_vars ⇒ TypeOK′
  PROOF OMITTED
⟨1⟩.HIDE DEFS Ballot, TypeOK
⟨1⟩3. QED
  BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec
├────────────────────────────────────────────────────────────────────────────┤
StructOK1 ≜ ∀ a ∈ Acceptor : IF maxVBal[a] = −1
                              THEN maxVal[a] = None
                              ELSE ⟨maxVBal[a], maxVal[a]⟩ ∈ votes[a]

THEOREM Spec ⇒ □StructOK1
⟨1⟩.USE DEFS Ballot, TypeOK, StructOK1
⟨1⟩1. Init ⇒ StructOK1
  BY Z3DEFS Init
⟨1⟩2. TypeOK ∧ StructOK1 ∧ [Next]_vars ⇒ StructOK1′
  BY WFmsgs, Z3DEFS Next, Phase1a, Phase2a, Phase1b, Phase2b, Send, votes,
     WellFormedMessages, vars, Message
⟨1⟩q. QED
  BY ONLY ⟨1⟩1, ⟨1⟩2, typing, PTL DEF Spec
├────────────────────────────────────────────────────────────────────────────┤
StructOK2 ≜ ∀ m ∈ msgs :
    (m[1] = “1b”) ⇒ ∧ maxBal[m[2]] ≥ m[3]
                     ∧ (m[4] ≥ 0) ⇒ ⟨m[4], m[5]⟩   ∈ votes[m[2]]

StructOK3 ≜ ∀ m ∈ msgs : m[1] = “2a” ⇒ ∧ ∃ Q ∈ Quorum : V!ShowsSafeAt(Q, m[2], m[3])
                                        ∧ ∀ mm ∈ msgs : ∧ mm[1]  = “2a”
                                                        ∧ mm[2]  = m[2]
```

```
                                                          ⇒ mm[3] = m[3]

StructOK4 ≜ ∀ m ∈ msgs : m[1] = "2b" ⇒ ∧ ∃ mo ∈ msgs : ∧ mo[1]  = "2a"
                                                      ∧ mo[2]  = m[3]
                                                      ∧ mo[3]  = m[4]
                                       ∧ maxBal[m[2]] ≥ m[3]
                                       ∧ maxVBal[m[2]] ≥ m[3]

StructOK5 ≜ ∀ m ∈ msgs : m[1] = "1b" ⇒ ∀ d ∈ Ballot : m[4] < d ∧ d < m[3] ⇒
                                       ∀ v ∈ Value : ¬⟨d, v⟩ ∈ votes[m[2]]

StructOK ≜  ∧ TypeOK
            ∧ StructOK1
            ∧ StructOK2
     ∧ StructOK3
          ∧ StructOK4
          ∧ StructOK5

THEOREM struct_lemma ≜ Spec ⇒ □StructOK
⟨1⟩.USE DEFS Ballot, StructOK, TypeOK, StructOK1, StructOK2, StructOK4, StructOK5
⟨1⟩1. Init ⇒ StructOK
  BY Z3DEFS Init
⟨1⟩2. StructOK ∧ [Next]_vars ⇒ StructOK′
  PROOF OMITTED
⟨1⟩3. QED
  BY ⟨1⟩1, ⟨1⟩2, PTL DEF Spec

THEOREM Spec ⇒ □StructOK3
⟨1⟩.USE DEFS Ballot, TypeOK, StructOK3
⟨1⟩1. Init ⇒ StructOK3
  BY Z3DEFS Init
⟨1⟩2. TypeOK ∧ StructOK ∧ [Next]_vars ⇒ StructOK3′
  PROOF OMITTED
⟨1⟩3. QED
  BY ONLY ⟨1⟩1, ⟨1⟩2, struct_lemma, PTL DEF Spec, StructOK
├──────────────────────────────────────────────────────────────────────────┤
Inv ≜ TypeOK ∧ StructOK1 ∧ StructOK2 ∧ StructOK3 ∧ StructOK4 ∧ StructOK5

THEOREM OtherMessage ≜ ∀ m1, m2 ∈ msgs′, a, b ∈ {"1a", "2a", "1b", "2b"} :
                ∧ m1[1] = a ∧ m2[1] = b ∧ a ≠ b
                ∧ msgs′ = msgs ∪ {m2}
                ⇒ m1 ∈ msgs
  BY Z3

THEOREM ∀ b ∈ Ballot, v ∈ Value :
              Phase2a(b, v) ∧ Inv ⇒ ∃ Q ∈ Quorum : V!ShowsSafeAt(Q, b, v)
⟨1⟩1. SUFFICES ASSUME NEW b ∈ Ballot,
                          NEW v ∈ Value,
                          ¬∃ m ∈ msgs : m[1] = "2a" ∧ m[3] = b,
                          NEW Q ∈ Quorum,
                          LET  Q1b  ≜  {m ∈ msgs  :  ∧ m[1] = "1b"
                                                     ∧ m[2] ∈ Q
                                                     ∧ m[3] = b}
                               Q1bv  ≜  {m ∈ Q1b : m[4] ≥ 0}
                          IN   ∧ ∀ a ∈ Q : ∃ m ∈ Q1b : m[2] = a
                               ∧ ∨ Q1bv = {}
                                 ∨ ∃ m   ∈ Q1bv :
                                      ∧ m[5] = v
                                      ∧ ∀ mm ∈ Q1bv : m[4] ≥ mm[4],
                          Send(⟨"2a", b, v⟩),
                          UNCHANGED ⟨maxBal, maxVBal, maxVal⟩,
                          Inv
                  PROVE   V!ShowsSafeAt(Q, b, v)
  BY SMT DEF Phase2a
⟨1⟩.USE ⟨1⟩1  DEF Ballot, Inv, TypeOK
⟨1⟩2. V!ShowsSafeAt(Q, b, v)!1
  BY SMT DEF Ballot, Send, StructOK2
⟨1⟩.DEFINE Q1b  ≜  {m ∈ msgs  :  ∧ m[1] = "1b"
                                 ∧ m[2] ∈ Q
                                 ∧ m[3] = b}
⟨1⟩.DEFINE Q1bv  ≜  {m ∈ Q1b : m[4] ≥ 0}
⟨1⟩3. V!ShowsSafeAt(Q, b, v)!2
  ⟨2⟩1. SUFFICES ASSUME NEW c ∈ −1 .. b − 1
                 PROVE  ∧ c ≠ −1 ⇒ (∃ a ∈ Q : V!VotedFor(a, c, v))
                        ∧ ∀ d ∈ c + 1 .. b − 1, a ∈ Q : V!DidNotVoteAt(a, d)
    BY SMT
  ⟨2⟩2. c ≠ −1 ⇒ (∃ a ∈ Q : V!VotedFor(a, c, v))
  ⟨2⟩3. ∀ d ∈ c + 1 .. b − 1, a ∈ Q : V!DidNotVoteAt(a, d)
  ⟨2⟩q. QED
    BY ⟨2⟩2, ⟨2⟩3, SMT
⟨1⟩q. QED
  BY ⟨1⟩2, ⟨1⟩3, Z3 DEF V!ShowsSafeAt
├──────────────────────────────────────────────────────────────────────┤
THEOREM Next ∧ Inv ⇒ V!Next ∨ UNCHANGED ⟨votes, maxBal⟩
⟨1⟩1. SUFFICES ASSUME Next, InvPROVE  V!Next
  BY ⟨1⟩1, SMT
⟨1⟩.USE  DEF Next, V!Next
⟨1⟩2.CASE ∃ b ∈ Ballot : Phase1a(b)
⟨1⟩3.CASE ∃ b ∈ Ballot : ∃ v ∈ Value : Phase2a(b, v)
⟨1⟩4.CASE ∃ a ∈ Acceptor : Phase1b(a)
  BY ⟨1⟩4, Inv, WFmsgs, Z3T(10)
   DEF Phase1b, Inv, WellFormedMessages, Ballot, V!Ballot, V!IncreaseMaxBal, votes, Send
```

```
⟨1⟩5.CASE ∃ a ∈ Acceptor : Phase2b(a)
  ⟨2⟩1. PICK a ∈ Acceptor, m ∈ msgs :
              ∧ m[1] = "2a"
              ∧ m[2] ≥ maxBal[a]
              ∧ maxBal' = [maxBal EXCEPT ![a] = m[2]]
              ∧ maxVBal' = [maxVBal EXCEPT ![a] = m[2]]
              ∧ maxVal' = [maxVal EXCEPT ![a] = m[3]]
              ∧ Send(⟨"2b", a, m[2], m[3]⟩)
      BY ⟨1⟩5, Z3 DEF Phase2b
  ⟨2⟩2. SUFFICES ASSUME NEW a_1 ∈ Acceptor, NEW b ∈ Nat
                     PROVE   ∨ V!IncreaseMaxBal(a_1, b)
                             ∨ ∃ v ∈ Value : V!VoteFor(a_1, b, v)
      BY Z3 DEF V!Ballot
  ⟨2⟩q. QED
⟨1⟩q. QED
  BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, ⟨1⟩4, ⟨1⟩5, Z3
```