MODULE *TPaxos*

EXTENDS *Integers*, *FiniteSets*, *TLAPS*

$\mathit{Max}(m, n) \triangleq \textsc{if}\ m > n\ \textsc{then}\ m\ \textsc{else}\ n$
$\mathit{Injective}(f) \triangleq \forall a, b \in \textsc{domain}\ f : (a \neq b) \Rightarrow (f[a] \neq f[b])$

CONSTANTS
$\mathit{Participant}$, the set of partipants
Value the set of possible input values for *Participant* to propose

$\mathit{None} \triangleq \textsc{choose}\ b : b \notin \mathit{Value}$

LEMMA $\mathit{NoneNotAValue} \triangleq \mathit{None} \notin \mathit{Value}$
BY $\mathit{NoSetContainsEverything}$ DEF None

$\mathit{NP} \triangleq \mathit{Cardinality}(\mathit{Participant})$ number of $p \in$ Participants

$\mathit{Quorum} \triangleq \{Q \in \textsc{subset}\ \mathit{Participant} : \mathit{Cardinality}(Q) * 2 \geq \mathit{NP} + 1\}$
ASSUME $\mathit{QuorumAssumption} \triangleq$
$\land \forall Q \in \mathit{Quorum} : Q \subseteq \mathit{Participant}$
$\land \forall Q1, Q2 \in \mathit{Quorum} : Q1 \cap Q2 \neq \{\}$

$\mathit{Ballot} \triangleq \mathit{Nat}$
$\mathit{AllBallot} \triangleq \mathit{Ballot} \cup \{-1\}$
$\mathit{AllValue} \triangleq \mathit{Value} \cup \{\mathit{None}\}$
$\mathit{MaxBallot} \triangleq \mathit{Cardinality}(\mathit{Ballot}) - 1$

$\mathit{PIndex} \triangleq \textsc{choose}\ f \in [\mathit{Participant} \to 1 \,..\, \mathit{NP}] : \mathit{Injective}(f)$
$\mathit{Bals}(p) \triangleq \{b \in \mathit{Ballot} : b \% \mathit{NP} = \mathit{PIndex}[p] - 1\}$ allocate ballots for each $p \in \mathit{Participant}$

$\mathit{State} \triangleq [\mathit{maxBal} : \mathit{Ballot} \cup \{-1\},$
$\mathit{maxVBal} : \mathit{Ballot} \cup \{-1\}, \mathit{maxVVal} : \mathit{Value} \cup \{\mathit{None}\}]$

$\mathit{InitState} \triangleq [\mathit{maxBal} \mapsto -1, \mathit{maxVBal} \mapsto -1, \mathit{maxVVal} \mapsto \mathit{None}]$

$Message \triangleq [from : Participant,$
$to : \textsc{subset}\ Participant,$
$state : [Participant \rightarrow [maxBal : Ballot \cup \{-1\},$
$maxVBal : Ballot \cup \{-1\},$
$maxVVal : Value \cup \{None\}]]]$

VARIABLES
$state,$ $state[p][q]$: the state of $q \in Participant$ from the view of $p \in Participant$
$msgs$ the set of messages that have been sent

$vars \triangleq \langle state, msgs \rangle$

$TypeOK \triangleq$
$\land\ state \in [Participant \rightarrow [Participant \rightarrow State]]$

$\land\ msgs \subseteq Message$

$Send(m) \triangleq msgs' = msgs \cup \{m\}$

$Init \triangleq$
$\land\ state = [p \in Participant \mapsto [q \in Participant \mapsto InitState]]$
$\land\ msgs = \{\}$

$Prepare(p, b) \triangleq$
$\land\ b \in Bals(p)$
$\land\ state[p][p].maxBal < b$
$\land\ state' = [state\ \textsc{except}\ ![p][p].maxBal = b]$
$\land\ Send([from \mapsto p, to \mapsto Participant \setminus \{p\}, state \mapsto state'[p]])$

```
$UpdateState(q, p, pp) \triangleq$
LET $maxB \triangleq Max(state[q][q].maxBal, pp.maxBal)$
$maxBV \triangleq$ IF $(maxB \leq pp.maxVBal)$
 THEN $pp.maxVBal$
 ELSE $state[q][q].maxVBal$
$maxVV \triangleq$ IF $(maxB \leq pp.maxVBal)$
 THEN $pp.maxVVal$
 ELSE $state[q][q].maxVVal$
$new\_state\_qq \triangleq [maxBal \mapsto maxB,$
$maxVBal \mapsto maxBV,$
$maxVVal \mapsto maxVV]$
$new\_state\_qp \triangleq [maxBal \mapsto Max(state[q][p].maxBal, pp.maxBal),$
$maxVBal \mapsto Max(state[q][p].maxVBal, pp.maxVBal),$
$maxVVal \mapsto ($IF $(state[q][p].maxVBal \leq pp.maxVBal)$
 THEN $pp.maxVVal$
 ELSE $state[q][p].maxVVal)]$
IN    $state' =$
$[state$ EXCEPT
$![q] = [state[q]$ EXCEPT
$![q] = new\_state\_qq,$
$![p] = new\_state\_qp$
$]$
$]$
```

```
$OnMessage(q) \triangleq$
$\exists m \in msgs :$
 $\land q \in m.to$
 $\land$ LET $p \triangleq m.from$
IN    $UpdateState(q, p, m.state[p])$
 $\land$ LET $qm \triangleq [from \mapsto m.from, to \mapsto m.to \setminus \{q\}, state \mapsto m.state]$ remove $q$ from to
$nm \triangleq [from \mapsto q, to \mapsto \{m.from\}, state \mapsto state'[q]]$ new message to reply
IN    IF $\lor m.state[q].maxBal < state'[q][q].maxBal$
$\lor m.state[q].maxVBal < state'[q][q].maxVBal$
 THEN $msgs' = msgs \cup \{nm\}$
 ELSE UNCHANGED $msgs$
```

```
$Accept(p, b, v) \triangleq$
$\land b \in Bals(p)$
$\land \neg\exists m \in msgs : m.state[m.from].maxBal = b \land m.state[m.from].maxVBal = b$
$\land state[p][p].maxBal = b$ corresponding the first conjunction in Voting
$\land state[p][p].maxVBal \neq b$ correspongding the second conjunction in Voting
$\land \exists Q \in Quorum :$
$\land \forall q \in Q : state[p][q].maxBal = b$
```

$\land\ \lor \forall\, q \in Q : state[p][q].maxVBal = -1$ free to pick its own value

$\lor \exists\, c \in 0\,..\,(b-1) :$
$\land \forall\, r \in Q : state[p][r].maxVBal \leq c$
$\land \exists\, r \in Q : \land\ state[p][r].maxVBal = c$
$\land\ state[p][r].maxVVal = v$

$\land\ state' = [state \text{ EXCEPT } ![p] = [state[p] \text{ EXCEPT }$
$![p] = [state[p][p] \text{ EXCEPT } !.maxVBal = b,$
$!.maxVVal = v]]]$
$\land\ Send([from \mapsto p,\ to \mapsto Participant \setminus \{p\},\ state \mapsto state'[p]])$

$Next \triangleq \exists\, p \in Participant : \lor\ OnMessage(p)$
$\lor \exists\, b \in Ballot : \lor\ Prepare(p,\ b)$
$\lor \exists\, v \in Value : Accept(p,\ b,\ v)$
$Spec \triangleq Init \land \Box[Next]_{vars}$

$VotedForIn(a,\ b,\ v) \triangleq \exists\, m \in msgs :$
$\land\ m.from = a$
$\land\ m.state[a].maxBal = b$
$\land\ m.state[a].maxVBal = b$
$\land\ m.state[a].maxVVal = v$

$ChosenIn(b,\ v) \triangleq \exists\, Q \in Quorum :$
$\forall\, a \in Q : VotedForIn(a,\ b,\ v)$

$Chosen(v) \triangleq \exists\, b \in Ballot : ChosenIn(b,\ v)$

$ChosenP(p) \triangleq$ the set of values chosen by $p \in Participant$
$\{v \in Value : \exists\, b \in Ballot :$
$\exists\, Q \in Quorum : \forall\, q \in Q : \land\ state[p][q].maxVBal = b$
$\land\ state[p][q].maxVVal = v\}$

$chosen \triangleq \text{UNION } \{ChosenP(p) : p \in Participant\}$

$Consistency \triangleq$ $Cardinality(chosen) \leq 1$

$\forall v1, v2 \in \mathit{Value} : \mathit{Chosen}(v1) \land \mathit{Chosen}(v2) \Rightarrow (v1 = v2)$

```
$\mathit{WontVoteIn}(a, b) \triangleq \land \forall v \in \mathit{Value} : \neg \mathit{VotedForIn}(a, b, v)$
$\land \mathit{state}[a][a].\mathit{maxBal} > b$

$\mathit{SafeAt}(b, v) \triangleq$
$\forall c \in 0 \,..\, (b - 1) :$
$\exists Q \in \mathit{Quorum} :$
$\forall a \in Q : \mathit{VotedForIn}(a, c, v) \lor \mathit{WontVoteIn}(a, c)$
```

```
$\mathit{MsgInv} \triangleq$
$\forall m \in \mathit{msgs} :$
$\textsc{let}\ p \triangleq m.\mathit{from}$
$\mathit{curState} \triangleq m.\mathit{state}[p]$
$\textsc{in}\quad \land \mathit{curState}.\mathit{maxBal} \geq \mathit{curState}.\mathit{maxVBal}$
$\land \mathit{curState}.\mathit{maxBal} \neq \mathit{curState}.\mathit{maxVBal}$
$\Rightarrow \land \mathit{curState}.\mathit{maxBal} \leq \mathit{state}[p][p].\mathit{maxBal}$
$\land \forall c \in (\mathit{curState}.\mathit{maxVBal} + 1) \,..\, (\mathit{curState}.\mathit{maxBal} - 1) :$
$\neg \exists v \in \mathit{Value} : \mathit{VotedForIn}(p, c, v)$
$\land \mathit{curState}.\mathit{maxBal} = \mathit{curState}.\mathit{maxVBal}$ exclude $(-1, -1, \mathit{None})$
$\Rightarrow \land \mathit{SafeAt}(\mathit{curState}.\mathit{maxVBal}, \mathit{curState}.\mathit{maxVVal})$
$\land \forall \mathit{ma} \in \mathit{msgs} : (\mathit{ma}.\mathit{state}[\mathit{ma}.\mathit{from}].\mathit{maxBal} = \mathit{curState}.\mathit{maxBal}$
$\land \mathit{ma}.\mathit{state}[\mathit{ma}.\mathit{from}].\mathit{maxBal} = \mathit{ma}.\mathit{state}[\mathit{ma}.\mathit{from}].\mathit{maxVBal})$
$\Rightarrow \mathit{ma}.\mathit{state}[\mathit{ma}.\mathit{from}].\mathit{maxVVal} = \mathit{curState}.\mathit{maxVVal}$
$\land \lor \land \mathit{curState}.\mathit{maxVVal} \in \mathit{Value}$
$\land \mathit{curState}.\mathit{maxVBal} \in \mathit{Ballot}$
$\land \mathit{VotedForIn}(m.\mathit{from}, \mathit{curState}.\mathit{maxVBal}, \mathit{curState}.\mathit{maxVVal})$
$\lor \land \mathit{curState}.\mathit{maxVVal} = \mathit{None}$
$\land \mathit{curState}.\mathit{maxVBal} = -1$
$\land \mathit{curState}.\mathit{maxBal} \in \mathit{Ballot}$
$\land m.\mathit{from} \notin m.\mathit{to}$
$\land \forall q \in \mathit{Participant} : \land m.\mathit{state}[q].\mathit{maxVBal} \leq \mathit{state}[q][q].\mathit{maxVBal}$
$\land m.\mathit{state}[q].\mathit{maxBal} \leq \mathit{state}[q][q].\mathit{maxBal}$
$\mathit{AccInv} \triangleq$
$\forall a \in \mathit{Participant} :$
$\land (\mathit{state}[a][a].\mathit{maxVBal} = -1) \equiv (\mathit{state}[a][a].\mathit{maxVVal} = \mathit{None})$
$\land \forall q \in \mathit{Participant} : \mathit{state}[a][q].\mathit{maxVBal} \leq \mathit{state}[a][q].\mathit{maxBal}$
$\land (\mathit{state}[a][a].\mathit{maxVBal} \geq 0) \Rightarrow \mathit{VotedForIn}(a, \mathit{state}[a][a].\mathit{maxVBal}, \mathit{state}[a][a].\mathit{maxVVal})$
$\land \forall c \in \mathit{Ballot} : c > \mathit{state}[a][a].\mathit{maxVBal}$
$\Rightarrow \neg \exists v \in \mathit{Value} : \mathit{VotedForIn}(a, c, v)$
$\land \forall q \in \mathit{Participant} :$
$\land \mathit{state}[a][a].\mathit{maxBal} \geq \mathit{state}[q][a].\mathit{maxBal}$
$\land \mathit{state}[a][a].\mathit{maxVBal} \geq \mathit{state}[q][a].\mathit{maxVBal}$
```

$\land \forall q \in \mathit{Participant} :$
$\mathit{state}[a][q].\mathit{maxBal} \in \mathit{Ballot}$
$\Rightarrow \exists m \in \mathit{msgs} :$
$\land\ m.\mathit{from} = q$
$\land\ m.\mathit{state}[q].\mathit{maxBal} = \mathit{state}[a][q].\mathit{maxBal}$
$\land\ m.\mathit{state}[q].\mathit{maxVBal} = \mathit{state}[a][q].\mathit{maxVBal}$
$\land\ m.\mathit{state}[q].\mathit{maxVVal} = \mathit{state}[a][q].\mathit{maxVVal}$

$\mathit{Inv} \triangleq \mathit{MsgInv} \land \mathit{AccInv} \land \mathit{TypeOK}$

LEMMA $\mathit{VotedInv} \triangleq$
$\mathit{MsgInv} \land \mathit{TypeOK} \Rightarrow$
$\forall a \in \mathit{Participant},\ b \in \mathit{Ballot},\ v \in \mathit{Value} :$
$\mathit{VotedForIn}(a,\ b,\ v) \Rightarrow \mathit{SafeAt}(b,\ v)$
BY DEFS $\mathit{MsgInv},\ \mathit{VotedForIn},\ \mathit{Message},\ \mathit{TypeOK}$

LEMMA $\mathit{MaxBigger} \triangleq \forall a \in \mathit{Ballot} \cup \{-1\},\ b \in \mathit{Ballot} : \mathit{Max}(a,\ b) \geq a \land \mathit{Max}(a,\ b) \geq b$
BY DEFS $\mathit{Ballot},\ \mathit{Max}$

LEMMA $\mathit{MaxTypeOK} \triangleq \forall a \in \mathit{AllBallot},\ b \in \mathit{Ballot} : \mathit{Max}(a,\ b) \in \mathit{Ballot}$
BY DEFS $\mathit{AllBallot},\ \mathit{Ballot},\ \mathit{Max}$

LEMMA $\mathit{UpdateStateBiggerProperty} \triangleq$
ASSUME NEW $q \in \mathit{Participant}$, NEW $p \in \mathit{Participant}$, NEW $\mathit{pp} \in$
$[\mathit{maxBal} : \mathit{Ballot} \cup \{-1\},$
$\mathit{maxVBal} : \mathit{Ballot} \cup \{-1\},\ \mathit{maxVVal} : \mathit{Value} \cup \{\mathit{None}\}],$
$\mathit{UpdateState}(q,\ p,\ \mathit{pp}),\ \mathit{TypeOK}$
PROVE $\land\ \mathit{state}'[q][q].\mathit{maxBal} \in \mathit{AllBallot}$
$\land\ \mathit{state}'[q][q].\mathit{maxBal} \geq \mathit{state}[q][q].\mathit{maxBal}$
BY DEFS $\mathit{UpdateState},\ \mathit{Max},\ \mathit{TypeOK},\ \mathit{AllBallot},\ \mathit{Ballot},\ \mathit{State}$

LEMMA $\mathit{UpdateStateTypeOKProperty} \triangleq$
ASSUME NEW $q \in \mathit{Participant}$, NEW $p \in \mathit{Participant}$, NEW $\mathit{pp} \in \mathit{State}$,
$\mathit{UpdateState}(q,\ p,\ \mathit{pp}),\ \mathit{TypeOK}$
PROVE $\mathit{state}' \in [\mathit{Participant} \rightarrow [\mathit{Participant} \rightarrow \mathit{State}]]$
$\langle 1 \rangle$ USE DEFS $\mathit{AllBallot},\ \mathit{Ballot},\ \mathit{TypeOK},\ \mathit{State},\ \mathit{Message},\ \mathit{AllValue}$
$\langle 1 \rangle 1.\ \land\ \mathit{state}'[q][q].\mathit{maxBal} \in \mathit{AllBallot}$
$\land\ \mathit{state}'[q][q].\mathit{maxVBal} \in \mathit{AllBallot}$
$\land\ \mathit{state}'[q][q].\mathit{maxVVal} \in \mathit{AllValue}$
$\land\ \mathit{state}'[q][p].\mathit{maxBal} \in \mathit{AllBallot}$
$\land\ \mathit{state}'[q][p].\mathit{maxVBal} \in \mathit{AllBallot}$
$\land\ \mathit{state}'[q][p].\mathit{maxVVal} \in \mathit{AllValue}$
BY DEFS $\mathit{UpdateState},\ \mathit{Max}$
$\langle 1 \rangle 3.\ \mathit{state}'[q][q] \in \mathit{State} \land \mathit{state}'[q][p] \in \mathit{State}$
BY $\langle 1 \rangle 1$ DEFS $\mathit{UpdateState}$

$\langle 1 \rangle 4.\ state[q] \in [Participant \rightarrow State] \wedge state[q][q] \in State \wedge state[q][p] \in State$

OBVIOUS

$\langle 1 \rangle 5.\ state'[q] \in [Participant \rightarrow State]$

BY $\langle 1 \rangle 3$, $\langle 1 \rangle 4$ DEFS $UpdateState$

$\langle 1 \rangle$ QED

BY $\langle 1 \rangle 5$ DEFS $UpdateState$

LEMMA $OnMessageBiggerProperty\ \triangleq$

ASSUME NEW $q \in Participant$, $OnMessage(q)$, $TypeOK$

PROVE $state'[q][q].maxBal \geq state[q][q].maxBal$

$\langle 1 \rangle 1$ PICK $m \in msgs : OnMessage(q)!(m)$

BY DEFS $OnMessage$

$\langle 1 \rangle 2.\ UpdateState(q, m.from, m.state[m.from])$

BY $\langle 1 \rangle 1$ DEFS $OnMessage$

$\langle 1 \rangle$ QED

BY $\langle 1 \rangle 2$, $UpdateStateBiggerProperty$DEFS $OnMessage$, $TypeOK$, $Message$

LEMMA $MsgNotLost\ \triangleq\ Next \wedge TypeOK \Rightarrow$

$\forall m \in msgs, b1 \in Ballot, p1 \in Participant, v1 \in Value :$

$\wedge\ m.from = p1$

$\wedge\ m.state[p1].maxBal = b1$

$\wedge\ m.state[p1].maxVBal = b1$

$\wedge\ m.state[p1].maxVVal = v1$

$\Rightarrow m \in msgs'$

$\langle 1 \rangle$ USE DEFS $TypeOK$, $Ballot$, $State$, $Send$

$\langle 1 \rangle 1.$ ASSUME NEW $pp \in Participant$, NEW $bb \in Ballot$,

$Prepare(pp, bb)$, $TypeOK$

PROVE $\forall m \in msgs : m \in msgs'$

BY $\langle 1 \rangle 1$ DEFS $Prepare$

$\langle 1 \rangle 2.$ ASSUME NEW $pp \in Participant$, NEW $bb \in Ballot$, NEW $vv \in Value$,

$Accept(pp, bb, vv)$

PROVE $\forall m \in msgs : m \in msgs'$

BY $\langle 1 \rangle 2$ DEFS $Accept$

$\langle 1 \rangle 3.$ ASSUME NEW $pp \in Participant$, $OnMessage(pp)$, NEW $m \in msgs$,

NEW $b1 \in Ballot$, NEW $p1 \in Participant$, NEW $v1 \in Value$,

$m.from = p1$, $m.state[p1].maxBal = b1$, $m.state[p1].maxVBal = b1$,

$m.state[p1].maxVVal = v1$

PROVE $m \in msgs'$

$\langle 2 \rangle$ PICK $mm \in msgs : OnMessage(pp)!(mm)$

BY $\langle 1 \rangle 3$ DEFS $OnMessage$

$\langle 2 \rangle 1$CASE $\vee\ mm.state[pp].maxBal < state'[pp][pp].maxBal$

$\vee\ mm.state[pp].maxVBal < state'[pp][pp].maxVBal$

BY $\langle 2 \rangle 1$ DEFS $OnMessage$

$\langle 2 \rangle 2$CASE $\neg(\ \vee\ mm.state[pp].maxBal < state'[pp][pp].maxBal$

$\vee\ mm.state[pp].maxVBal < state'[pp][pp].maxVBal)$

```
BY ⟨2⟩2 DEFS OnMessage
⟨2⟩ QED
BY ⟨1⟩3, ⟨2⟩1, ⟨2⟩2
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3 DEFS Next

LEMMA VotedOnce ≜
MsgInv ⇒ ∀ a1, a2 ∈ Participant, b ∈ Ballot, v1, v2 ∈ Value :
VotedForIn(a1, b, v1) ∧ VotedForIn(a2, b, v2) ⇒ (v1 = v2)
BY DEFS MsgInv, VotedForIn

LEMMA SafeAtStable ≜ Inv ∧ Next ∧ TypeOK′ ⇒
∀ v ∈ Value, b ∈ Ballot :
SafeAt(b, v) ⇒ SafeAt(b, v)′
⟨1⟩ SUFFICES ASSUME Inv, Next, TypeOK′,
NEW b ∈ Ballot, NEW v ∈ Value,
SafeAt(b, v)
PROVE SafeAt(b, v)′
OBVIOUS
⟨1⟩ USE DEFS Send, Ballot, TypeOK, State, AllBallot, AllValue
⟨1⟩1. ASSUME NEW pp ∈ Participant, NEW bb ∈ Ballot, Prepare(pp, bb), TypeOK
PROVE SafeAt(b, v)′
⟨2⟩ DEFINE mm ≜ [from ↦ pp, to ↦ Participant \ {pp}, state ↦ state′[pp]]
⟨2⟩1. ∀ p1 ∈ Participant, b1 ∈ Ballot, v1 ∈ Value :
VotedForIn(p1, b1, v1) ⇒ VotedForIn(p1, b1, v1)′
BY ⟨1⟩1 DEFS VotedForIn, Prepare
⟨2⟩2. ∀ p1 ∈ Participant, b1 ∈ Ballot :
state[p1][p1].maxBal > b1 ⇒ state′[p1][p1].maxBal > b1
BY ⟨1⟩1 DEFS Prepare, Inv
⟨2⟩3. ∀ p1 ∈ Participant, b1 ∈ Ballot, v1 ∈ Value :
¬ VotedForIn(p1, b1, v1) ⇒ ¬ VotedForIn(p1, b1, v1)′
⟨3⟩a. ∧ state[pp][pp].maxVBal ∈ AllBallot
 ∧ state′[pp][pp].maxVBal ∈ AllBallot
 ∧ state[pp][pp].maxBal ∈ AllBallot
 ∧ state′[pp][pp].maxBal ∈ AllBallot
BY DEFS Prepare, Inv
⟨3⟩1. mm ∈ msgs′
BY ⟨1⟩1  DEF Prepare
⟨3⟩2. ∧ mm.state[pp].maxBal > state[pp][pp].maxBal
 ∧ mm.state[pp].maxVBal = state[pp][pp].maxVBal
BY ⟨1⟩1  DEF Prepare
⟨3⟩3. mm.state[pp].maxBal ≠ mm.state[pp].maxVBal
⟨4⟩1. state[pp][pp].maxBal ≥ state[pp][pp].maxVBal
BY DEFS Inv, AccInv
```

$\langle 4\rangle 2.$ $mm.state[pp].maxBal > mm.state[pp].maxVBal$

BY $\langle 3\rangle$a, $\langle 3\rangle 2$, $\langle 4\rangle 1$ DEFS Inv, $MsgInv$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 2$

$\langle 3\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 3\rangle 1$, $\langle 3\rangle 3$ DEFS $Prepare$, $VotedForIn$, Inv

$\langle 2\rangle 4.$ $\forall\, p1 \in Participant,\ b1 \in Ballot :$

$WontVoteIn(p1,\ b1) \Rightarrow WontVoteIn(p1,\ b1)'$

BY $\langle 2\rangle 2$, $\langle 2\rangle 3$ DEFS $Prepare$, $WontVoteIn$

$\langle 2\rangle 5.$ QED

BY $\langle 1\rangle 1$, $\langle 2\rangle 1$, $\langle 2\rangle 4$, $QuorumAssumption$DEFS $Prepare$, $SafeAt$

$\langle 1\rangle 2.$ ASSUME NEW $pp \in Participant$, NEW $bb \in Ballot$, NEW $vv \in Value$,

$Accept(pp,\ bb,\ vv)$

PROVE $SafeAt(b,\ v)'$

$\langle 2\rangle 1.$ $\forall\, p1 \in Participant,\ b1 \in Ballot,\ v1 \in Value :$

$VotedForIn(p1,\ b1,\ v1) \Rightarrow VotedForIn(p1,\ b1,\ v1)'$

BY $\langle 1\rangle 2$ DEFS $VotedForIn$, $Accept$

$\langle 2\rangle 2.$ $\forall\, p1 \in Participant,\ b1 \in Ballot :$

$state[p1][p1].maxBal > b1 \Rightarrow state'[p1][p1].maxBal > b1$

BY $\langle 1\rangle 2$ DEFS $Accept$

$\langle 2\rangle 3.$ ASSUME NEW $p1 \in Participant$, NEW $b1 \in Ballot$, NEW $v1 \in Value$,

$WontVoteIn(p1,\ b1),\ VotedForIn(p1,\ b1,\ v1)'$

PROVE FALSE

$\langle 3\rangle$ PICK $mm \in msgs' :\ \wedge\ mm.from = p1$

$\wedge\ mm.state[p1].maxBal = b1$

$\wedge\ mm.state[p1].maxVBal = b1$

$\wedge\ mm.state[p1].maxVVal = v1$

BY $\langle 2\rangle 3$ DEFS $VotedForIn$

$\langle 3\rangle 1.$ $mm \in msgs'$

BY $\langle 2\rangle 3$ DEFS $VotedForIn$

$\langle 3\rangle 2.$ $mm \notin msgs$

BY $\langle 2\rangle 3$ DEFS $WontVoteIn$, $VotedForIn$

$\langle 3\rangle 3.$ $p1 = pp$

BY $\langle 1\rangle 2$, $\langle 3\rangle 1$, $\langle 3\rangle 2$ DEFS $Accept$

$\langle 3\rangle 4.$ $mm = [from \mapsto pp,\ to \mapsto Participant \setminus \{pp\},$

$state \mapsto (state')[pp]]$

$\wedge\ state'[pp][pp].maxVBal = bb$

BY $\langle 1\rangle 2$, $\langle 3\rangle 1$, $\langle 3\rangle 2$ DEFS $Accept$

$\langle 3\rangle 5.$ $b1 = bb$

BY $\langle 1\rangle 2$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 4$ DEFS $Accept$, Inv

$\langle 3\rangle$ QED

BY $\langle 1\rangle 2$, $\langle 2\rangle 3$, $\langle 3\rangle 3$, $\langle 3\rangle 5$ DEFS $Accept$, $WontVoteIn$, $VotedForIn$, Inv

$\langle 2\rangle 4.$ $\forall\, p1 \in Participant,\ b1 \in Ballot :$

$WontVoteIn(p1,\ b1) \Rightarrow WontVoteIn(p1,\ b1)'$

BY $\langle 1\rangle 2$, $\langle 2\rangle 2$, $\langle 2\rangle 3$ DEFS $Accept$, $WontVoteIn$

```
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle 2$, $\langle 2 \rangle 1$, $\langle 2 \rangle 4$, $QuorumAssumption$ DEF $Accept$, $SafeAt$
$\langle 1 \rangle 3$. ASSUME NEW $pp \in Participant$, $OnMessage(pp)$, $TypeOK'$
PROVE $SafeAt(b, v)'$
$\langle 2 \rangle 1$. $\forall p1 \in Participant, b1 \in Ballot, v1 \in Value :$
$VotedForIn(p1, b1, v1) \Rightarrow VotedForIn(p1, b1, v1)'$

$\langle 3 \rangle 1$. SUFFICES ASSUME NEW $p1 \in Participant$, NEW $b1 \in Ballot$,
NEW $v1 \in Value$, $VotedForIn(p1, b1, v1)$
PROVE $VotedForIn(p1, b1, v1)'$
OBVIOUS
$\langle 3 \rangle 2$. PICK $m \in msgs :$
$\land m.from = p1$
$\land m.state[p1].maxBal = b1$
$\land m.state[p1].maxVBal = b1$
$\land m.state[p1].maxVVal = v1$
BY $\langle 3 \rangle 1$ DEFS $VotedForIn$
$\langle 3 \rangle 3$. $m \in msgs'$
BY $\langle 1 \rangle 3$, $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $MsgNotLost$DEFS $Inv$
$\langle 3 \rangle$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$ DEFS $VotedForIn$
$\langle 2 \rangle 2$. $\forall p1 \in Participant, b1 \in Ballot :$
$state[p1][p1].maxBal > b1 \Rightarrow state'[p1][p1].maxBal > b1$
$\langle 3 \rangle 1$. SUFFICES ASSUME NEW $p1 \in Participant$, NEW $b1 \in AllBallot$,
$state[p1][p1].maxBal > b1$
PROVE $state'[p1][p1].maxBal > b1$
OBVIOUS
$\langle 3 \rangle 2$. PICK $mm \in msgs : OnMessage(pp)!(mm)$
BY $\langle 1 \rangle 3$ DEFS $OnMessage$
$\langle 3 \rangle 3$.CASE $p1 = pp$
$\langle 4 \rangle 3$. $state[pp][pp].maxBal \in AllBallot$
BY DEFS $Inv$
$\langle 4 \rangle 1$. $state'[pp][pp].maxBal \in AllBallot$
BY $\langle 1 \rangle 3$
$\langle 4 \rangle 2$. $state'[pp][pp].maxBal \geq state[pp][pp].maxBal$
BY $\langle 1 \rangle 3$, $OnMessageBiggerProperty$DEFS $Inv$
$\langle 4 \rangle$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 3$, $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEFS $Inv$
$\langle 3 \rangle 4$.CASE $p1 \neq pp$
BY $\langle 1 \rangle 3$, $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 4$ DEFS $UpdateState$, $Max$, $OnMessage$
$\langle 3 \rangle$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$
$\langle 2 \rangle 3$. ASSUME NEW $p1 \in Participant$, NEW $b1 \in AllBallot$, NEW $v1 \in Value$,
$WontVoteIn(p1, b1)$, $VotedForIn(p1, b1, v1)'$
PROVE FALSE
```

$\langle 3\rangle 1.$ PICK $mm \in msgs' : \land mm.from = p1$

$\land mm.state[p1].maxBal = b1$

$\land mm.state[p1].maxVBal = b1$

$\land mm.state[p1].maxVVal = v1$

BY $\langle 2\rangle 3$ DEFS $VotedForIn$

$\langle 3\rangle 2.$ $mm \notin msgs$

BY $\langle 2\rangle 3$, $\langle 3\rangle 1$ DEFS $WontVoteIn$, $VotedForIn$, Inv

$\langle 3\rangle 3.$CASE $p1 = pp$

$\langle 4\rangle 1.$ $state'[pp][pp].maxBal = b1$

BY $\langle 1\rangle 3$, $\langle 2\rangle 3$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$ DEFS $OnMessage$

$\langle 4\rangle 2.$ $state[pp][pp].maxBal > b1$

BY $\langle 2\rangle 3$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$ DEFS $VotedForIn$, $WontVoteIn$

$\langle 4\rangle 3.$ $state'[pp][pp].maxBal \geq state[pp][pp].maxBal$

BY $\langle 1\rangle 3$, $OnMessageBiggerProperty$DEFS Inv

$\langle 4\rangle 5.$ $state[pp][pp].maxBal \in AllBallot$

BY DEFS Inv

$\langle 4\rangle 6.$ $state'[pp][pp].maxBal \in AllBallot$

BY $\langle 1\rangle 3$

$\langle 4\rangle 4.$ $state'[pp][pp].maxBal > b1$

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 5$, $\langle 4\rangle 6$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 4$

$\langle 3\rangle 4.$CASE $p1 \neq pp$

BY $\langle 1\rangle 3$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 4$ DEFS $OnMessage$

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$ DEFS $OnMessage$, $WontVoteIn$, $VotedForIn$, Inv

$\langle 2\rangle 4.$ $\forall\, p1 \in Participant,\ b1 \in Ballot :$

$WontVoteIn(p1,\ b1) \Rightarrow WontVoteIn(p1,\ b1)'$

BY $\langle 1\rangle 3$, $\langle 2\rangle 2$, $\langle 2\rangle 3$ DEFS $OnMessage$, $WontVoteIn$

$\langle 2\rangle$ QED

BY $\langle 1\rangle 3$, $\langle 2\rangle 1$, $\langle 2\rangle 4$, $QuorumAssumption$DEFS $OnMessage$, $SafeAt$

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 3$ DEF $Next$, Inv

LEMMA $PrepareMsgInv \triangleq$ ASSUME NEW $p \in Participant$, NEW $b \in Ballot$, $Prepare(p,\ b)$, Inv, $TypeOK'$

PROVE $MsgInv'$

$\langle 1\rangle$ USE DEF $TypeOK$, $Ballot$, $AllBallot$, Inv, $MsgInv$, $State$, $Send$, $Message$

$\langle 1\rangle$ SUFFICES ASSUME NEW $m \in msgs'$

PROVE $MsgInv!(m)'$

OBVIOUS

$\langle 1\rangle$ DEFINE $mm \triangleq [from \mapsto p,\ to \mapsto Participant \setminus \{p\},\ state \mapsto state'[p]]$

$\langle 1\rangle$a. $mm \in msgs' \land mm.from = p$

BY DEFS $Prepare$

$\langle 1\rangle$aa. $\land\, state'[p][p].maxBal \in AllBallot$

$\land\, state[p][p].maxBal \in AllBallot$

$\land\ state[p][p].maxVBal \in AllBallot$
OBVIOUS
$\langle 1\rangle$b. $\land\ mm.state[p].maxBal \neq mm.state[p].maxVBal$
$\land\ mm.state[p].maxBal \geq mm.state[p].maxVBal$
$\langle 2\rangle$1. $state'[p][p].maxBal > state[p][p].maxBal$
BY DEFS $Prepare$
$\langle 2\rangle$2. $state[p][p].maxBal \geq state[p][p].maxVBal$
BY DEFS $AccInv$
$\langle 2\rangle$3. $state'[p][p].maxVBal = state[p][p].maxVBal$
BY DEFS $Prepare$
$\langle 2\rangle$ QED
BY $\langle 1\rangle$aa, $\langle 2\rangle$1, $\langle 2\rangle$2, $\langle 2\rangle$3
$\langle 1\rangle$c. $m.from \notin m.to$
BY DEFS $Prepare$
$\langle 1\rangle$d. $mm.state[p].maxBal \geq mm.state[p].maxVBal$
BY $\langle 1\rangle$b
$\langle 1\rangle$1.CASE $m = mm$
$\langle 2\rangle$1. $m.state[m.from].maxBal \neq m.state[m.from].maxVBal$
BY $\langle 1\rangle$b, $\langle 1\rangle$1
$\langle 2\rangle$2. $m.state[m.from].maxBal \leq state'[m.from][m.from].maxBal$
BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 1\rangle$1 DEFS $Prepare$
$\langle 2\rangle$a. $m.state[m.from].maxBal \geq m.state[m.from].maxVBal$
BY $\langle 1\rangle$d, $\langle 1\rangle$1
$\langle 2\rangle$3. $\lor\ \land\ (m.state)[m.from].maxVVal \in Value$
$\land\ (m.state)[m.from].maxVBal \in Nat$
$\land\ VotedForIn(m.from,\ (m.state)[m.from].maxVBal,\ (m.state)[m.from].maxVVal)'$
$\lor\ \land\ (m.state)[m.from].maxVVal = None$
$\land\ (m.state)[m.from].maxVBal = \ -1$
BY $\langle 1\rangle$1 DEFS $Prepare$, $AccInv$, $VotedForIn$
$\langle 2\rangle$4. $\land\ \forall\, c \in (m.state)[m.from].maxVBal + 1\ ..\ (m.state)[m.from].maxBal - 1 :$
$\neg(\exists\, v \in Value : VotedForIn(m.from,\ c,\ v))'$
$\langle 3\rangle$1. $\forall\, c \in (m.state[m.from].maxVBal + 1)\ ..\ (m.state[m.from].maxBal - 1) :$
$\neg(\exists\, v \in Value : VotedForIn(m.from,\ c,\ v))$
$\langle 4\rangle$ SUFFICES ASSUME NEW $c \in (m.state[m.from].maxVBal + 1)\ ..\ (m.state[m.from].maxBal - 1)$
PROVE $\neg(\exists\, v \in Value : VotedForIn(m.from,\ c,\ v))$
OBVIOUS
$\langle 4\rangle$1a. $state[p][p].maxVBal = (m.state)[m.from].maxVBal$
BY $\langle 1\rangle$a, $\langle 1\rangle$1 DEFS $Prepare$
$\langle 4\rangle$1b. $b = m.state[m.from].maxBal$
BY $\langle 1\rangle$a, $\langle 1\rangle$1 DEFS $Prepare$
$\langle 4\rangle$1c. $m.from = p$
BY $\langle 1\rangle$a, $\langle 1\rangle$1 DEFS $Prepare$
$\langle 4\rangle$1d. $c \in Ballot \land c > state[p][p].maxVBal$
BY $\langle 4\rangle$1b, $\langle 4\rangle$1a, $\langle 4\rangle$1c
$\langle 4\rangle$1. $\neg(\exists\, v \in Value : VotedForIn(p,\ c,\ v))$

BY $\langle 4\rangle 1\text{d}$ DEFS $AccInv$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1\text{a}$, $\langle 4\rangle 1\text{b}$, $\langle 4\rangle 1\text{c}$, $\langle 4\rangle 1$ DEFS $AccInv$, $VotedForIn$

$\langle 3\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 3\rangle 1$ DEFS $Prepare$, $VotedForIn$

$\langle 2\rangle 5.$ $m.state[m.from].maxBal \in Ballot$

BY $\langle 1\rangle \text{a}$, $\langle 1\rangle \text{b}$ DEFS $Prepare$

$\langle 2\rangle 6.$ $\forall\, q \in Participant : \land\, m.state[q].maxVBal \leq state'[q][q].maxVBal$

$\land\, m.state[q].maxBal \leq state'[q][q].maxBal$

BY $\langle 1\rangle 1$, $\langle 2\rangle \text{a}$ DEFS $Prepare$, $AccInv$

$\langle 2\rangle$ QED

BY $\langle 1\rangle \text{c}$, $\langle 2\rangle 1$, $\langle 2\rangle \text{a}$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$ DEFS $VotedForIn$

$\langle 1\rangle 2.$CASE $m \neq mm$

$\langle 2\rangle \text{a}.$ $m \in msgs$

BY $\langle 1\rangle 2$ DEFS $Prepare$

$\langle 2\rangle \text{b}.$ $m.state[m.from].maxBal \in Ballot$

BY $\langle 2\rangle \text{a}$

$\langle 2\rangle \text{c}.$ $m.state[m.from].maxBal \geq m.state[m.from].maxVBal$

BY $\langle 2\rangle \text{a}$

$\langle 2\rangle \text{d}.$ $\forall\, q \in Participant : \land\, m.state[q].maxVBal \leq state'[q][q].maxVBal$

$\land\, m.state[q].maxBal \leq state'[q][q].maxBal$

$\langle 3\rangle$ SUFFICES ASSUME NEW $q \in Participant$

PROVE $\land\, m.state[q].maxVBal \leq state'[q][q].maxVBal$

$\land\, m.state[q].maxBal \leq state'[q][q].maxBal$

OBVIOUS

$\langle 3\rangle \text{a}.$ $\land\, m.state[q].maxBal \in AllBallot$

$\land\, state[q][q].maxBal \in AllBallot$

$\land\, state'[q][q].maxBal \in AllBallot$

BY DEFS $MsgInv$

$\langle 3\rangle 1.$ $state[q][q].maxBal \leq state'[q][q].maxBal$

BY $SMTT(100)$, $IsaT(100)$DEFS $Prepare$

$\langle 3\rangle 2.$ $m.state[q].maxBal \leq state'[q][q].maxBal$

BY $\langle 2\rangle \text{a}$, $\langle 3\rangle 1$, $\langle 3\rangle \text{a}$ DEFS $AccInv$

$\langle 3\rangle$ QED

BY $\langle 1\rangle 2$, $\langle 2\rangle \text{a}$, $\langle 3\rangle 1$, $\langle 3\rangle 2$ DEFS $Prepare$, $AccInv$

$\langle 2\rangle 1.$CASE $(m.state)[m.from].maxBal \neq (m.state)[m.from].maxVBal$

$\langle 3\rangle 1.$ $m.state[m.from].maxBal \leq state'[m.from][m.from].maxBal$

$\langle 4\rangle \text{a}.$ $m.state[m.from].maxBal \leq state[m.from][m.from].maxBal$

BY $\langle 2\rangle \text{a}$, $\langle 2\rangle 1$

$\langle 4\rangle 1.$CASE $m.from = p$

$\langle 5\rangle 1.$ $m.state[m.from].maxBal \in AllBallot \land state[m.from][m.from].maxBal \in AllBallot$

$\land\, state'[m.from][m.from].maxBal \in AllBallot$

BY $\langle 2\rangle 1$, $\langle 4\rangle 1$

$\langle 5\rangle$ QED

BY $\langle 4\rangle \text{a}$, $\langle 4\rangle 1$, $\langle 5\rangle 1$ DEFS $Prepare$

$\langle 4\rangle$2.CASE $m.from \neq p$

BY $\langle 4\rangle$a, $\langle 4\rangle$2 DEF $Prepare$

$\langle 4\rangle$ QED

BY $\langle 4\rangle$1, $\langle 4\rangle$2

$\langle 3\rangle$2. $\vee\ \wedge (m.state)[m.from].maxVVal \in Value$

$\wedge (m.state)[m.from].maxVBal \in Nat$

$\wedge\ VotedForIn(m.from, (m.state)[m.from].maxVBal, (m.state)[m.from].maxVVal)'$

$\vee\ \wedge (m.state)[m.from].maxVVal = None$

$\wedge (m.state)[m.from].maxVBal = -1$

BY $\langle 1\rangle$2, $\langle 2\rangle$1 DEFS $Prepare$, $AccInv$, $VotedForIn$

$\langle 3\rangle$3. $\wedge \forall c \in (m.state)[m.from].maxVBal + 1 \mathrel{..} (m.state)[m.from].maxBal - 1 :$

$\neg(\exists v \in Value : VotedForIn(m.from, c, v))'$

$\langle 4\rangle$1. $\wedge \forall c \in (m.state)[m.from].maxVBal + 1 \mathrel{..} (m.state)[m.from].maxBal - 1 :$

$\neg(\exists v \in Value : VotedForIn(m.from, c, v))$

BY $\langle 1\rangle$2, $\langle 2\rangle$1 DEFS $VotedForIn$, $Prepare$

$\langle 4\rangle$ QED

BY $\langle 1\rangle$b, $\langle 1\rangle$2, $\langle 2\rangle$1, $\langle 4\rangle$1, $AllProvers$ DEF $VotedForIn$, $Prepare$

$\langle 3\rangle$ QED

BY $\langle 1\rangle$c, $\langle 2\rangle$b, $\langle 2\rangle$c, $\langle 2\rangle$d, $\langle 2\rangle$1, $\langle 3\rangle$1, $\langle 3\rangle$2, $\langle 3\rangle$3

$\langle 2\rangle$2.CASE $(m.state)[m.from].maxBal = (m.state)[m.from].maxVBal$

$\langle 3\rangle$1. $\vee\ \wedge (m.state)[m.from].maxVVal \in Value$

$\wedge (m.state)[m.from].maxVBal \in Nat$

$\wedge\ VotedForIn(m.from, (m.state)[m.from].maxVBal, (m.state)[m.from].maxVVal)'$

$\vee\ \wedge (m.state)[m.from].maxVVal = None$

$\wedge (m.state)[m.from].maxVBal = -1$

BY $\langle 1\rangle$2, $\langle 2\rangle$2 DEFS $Prepare$, $AccInv$, $VotedForIn$

$\langle 3\rangle$2. $SafeAt(m.state[m.from].maxVBal, m.state[m.from].maxVVal)'$

$\langle 4\rangle$a. $m.state[m.from].maxVBal \in Ballot \wedge m.state[m.from].maxVVal \in Value$

BY $\langle 2\rangle$a, $\langle 2\rangle$b, $\langle 2\rangle$2, $\langle 3\rangle$1

$\langle 4\rangle$1. $SafeAt(m.state[m.from].maxVBal, m.state[m.from].maxVVal)$

BY $\langle 2\rangle$a, $\langle 2\rangle$2

$\langle 4\rangle$ QED

BY $\langle 4\rangle$a, $\langle 4\rangle$1, $SafeAtStable$DEFS $Next$

$\langle 3\rangle$3. $\forall ma \in msgs' : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$

$\wedge\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

$\langle 4\rangle$1. $\forall ma \in msgs : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$

$\wedge\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

BY $\langle 2\rangle$a, $\langle 2\rangle$2

$\langle 4\rangle$ QED

BY $\langle 4\rangle$1, $\langle 1\rangle$b DEFS $Prepare$

$\langle 3\rangle$ QED

BY $\langle 1\rangle$c, $\langle 2\rangle$b, $\langle 2\rangle$c, $\langle 2\rangle$d, $\langle 2\rangle$2, $\langle 3\rangle$1, $\langle 3\rangle$2, $\langle 3\rangle$3

$\langle 2\rangle$ QED

```
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

LEMMA $UpdateStateViewValue \triangleq$
ASSUME NEW $q \in Participant$, NEW $p \in Participant$, NEW $m \in msgs$, $p = m.from$, $q \in m.to$,
$UpdateState(q, p, m.state[m.from])$, $Inv$, $TypeOK'$
PROVE  $\land\ state'[q][p].maxBal \geq state'[q][p].maxVBal$
 $\land\ \lor\ \land\ state'[q][p].maxBal = state[q][p].maxBal$
 $\land\ state'[q][p].maxVBal = state[q][p].maxVBal$
 $\land\ state'[q][p].maxVVal = state[q][p].maxVVal$
 $\lor\ \land\ state'[q][p].maxBal = m.state[m.from].maxBal$
 $\land\ state'[q][p].maxVBal = m.state[m.from].maxVBal$
 $\land\ state'[q][p].maxVVal = m.state[m.from].maxVVal$
$\langle 1\rangle$ USE DEFS $AllBallot$, $Ballot$
$\langle 1\rangle$a. $\land\ state[q][p].maxBal \in AllBallot$
 $\land\ state[q][p].maxVBal \in AllBallot$
 $\land\ m.state[m.from].maxVBal \in AllBallot$
 $\land\ m.state[m.from].maxBal \in AllBallot$
BY DEFS $Inv$, $TypeOK$, $State$, $MsgInv$, $Message$
$\langle 1\rangle$b. $\land\ state'[q][p].maxBal = Max(state[q][p].maxBal, m.state[m.from].maxBal)$
 $\land\ state'[q][p].maxVBal = Max(state[q][p].maxVBal, m.state[m.from].maxVBal)$
 $\land\ state'[q][p].maxVVal =$ IF $(state[q][p].maxVBal \leq m.state[m.from].maxVBal)$
  THEN $m.state[m.from].maxVVal$
  ELSE  $state[q][p].maxVVal$
BY DEFS $UpdateState$, $State$, $Ballot$, $Inv$, $TypeOK$
$\langle 1\rangle$c. $\land\ state[q][p].maxVBal \leq state[q][p].maxBal$
 $\land\ m.state[m.from].maxBal \geq m.state[m.from].maxVBal$
BY DEFS $Inv$, $AccInv$, $MsgInv$
$\langle 1\rangle$d. $\land\ state[q][p].maxVBal \leq state'[q][p].maxBal$
 $\land\ m.state[m.from].maxVBal \leq state'[q][p].maxBal$
BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 1\rangle$c DEFS $Max$
$\langle 1\rangle$e. $p \neq q$
BY DEFS $Inv$, $MsgInv$
$\langle 1\rangle 1$. $state'[q][p].maxVBal \leq state'[q][p].maxBal$
BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 1\rangle$d DEFS $Max$
$\langle 1\rangle 2$.CASE $state[q][p].maxBal = -1$
$\langle 2\rangle 1$. $state[q][p].maxVBal = -1$
BY $\langle 1\rangle$a, $\langle 1\rangle 2$ DEFS $Inv$, $AccInv$
$\langle 2\rangle 2$. $\land\ state'[q][p].maxBal = m.state[m.from].maxBal$
 $\land\ state'[q][p].maxVBal = m.state[m.from].maxVBal$
 $\land\ state'[q][p].maxVVal = m.state[m.from].maxVVal$
BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 1\rangle 2$, $\langle 2\rangle 1$ DEFS $Max$
$\langle 2\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 2\rangle 2$
```

$\langle 1\rangle 3.$CASE $state[q][p].maxBal \in Ballot$

$\langle 2\rangle$a. PICK $mm \in msgs$:

$\land\ mm.from = p$

$\land\ mm.state[p].maxBal = state[q][p].maxBal$

$\land\ mm.state[p].maxVBal = state[q][p].maxVBal$

$\land\ mm.state[p].maxVVal = state[q][p].maxVVal$

BY $\langle 1\rangle$e, $\langle 1\rangle 3$ DEFS Inv, $AccInv$

$\langle 2\rangle 1.$CASE $state[q][p].maxBal < m.state[m.from].maxBal$

$\langle 3\rangle 1.$ $state[q][p].maxVBal \leq m.state[m.from].maxVBal$

$\langle 4\rangle$ SUFFICES ASSUME $state[q][p].maxVBal > m.state[m.from].maxVBal$

PROVE FALSE

BY $\langle 1\rangle$a, $\langle 2\rangle 1$

$\langle 4\rangle 1.$ $\land\ m.state[m.from].maxBal > m.state[m.from].maxVBal$

$\land\ state[q][p].maxVBal < m.state[m.from].maxBal$

BY $\langle 1\rangle$a, $\langle 2\rangle 1$ DEFS Inv, $AccInv$

$\langle 4\rangle 2.$ $\forall\, c \in (m.state[m.from].maxVBal + 1) \mathrel{..} (m.state[m.from].maxBal - 1)$:

$\neg\exists\, v \in Value : VotedForIn(m.from,\ c,\ v)$

BY $\langle 4\rangle 1$ DEFS Inv, $MsgInv$

$\langle 4\rangle 3.$ $state[q][p].maxVBal \in Ballot \land state[q][p].maxVVal \in Value$

BY $\langle 1\rangle$a, $\langle 2\rangle$a DEFS Inv, $MsgInv$

$\langle 4\rangle 4.$ $VotedForIn(p,\ state[q][p].maxVBal,\ state[q][p].maxVVal)$

BY $\langle 2\rangle$a, $\langle 4\rangle 3$ DEFS Inv, $MsgInv$

$\langle 4\rangle 5.$ $state[q][p].maxVBal \in (m.state[m.from].maxVBal + 1) \mathrel{..} (m.state[m.from].maxBal - 1)$

BY $\langle 1\rangle$a, $\langle 2\rangle 1$, $\langle 4\rangle 1$

$\langle 4\rangle$ QED

BY $\langle 1\rangle$a, $\langle 2\rangle$a, $\langle 2\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$ DEFS $VotedForIn$

$\langle 3\rangle 2.$ $\land\ state'[q][p].maxBal = m.state[m.from].maxBal$

$\land\ state'[q][p].maxVBal = m.state[m.from].maxVBal$

$\land\ state'[q][p].maxVVal = m.state[m.from].maxVVal$

BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 2\rangle 1$, $\langle 3\rangle 1$ DEFS Max

$\langle 3\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 3\rangle 2$

$\langle 2\rangle 2.$CASE $state[q][p].maxBal > m.state[m.from].maxBal$

$\langle 3\rangle 1.$ $state[q][p].maxVBal \geq m.state[m.from].maxVBal$

$\langle 4\rangle$ SUFFICES ASSUME $state[q][p].maxVBal < m.state[m.from].maxVBal$

PROVE FALSE

BY $\langle 1\rangle$a, $\langle 2\rangle 2$

$\langle 4\rangle 1.$ $\land\ state[q][p].maxBal > state[q][p].maxVBal$

$\land\ m.state[m.from].maxVBal < state[q][p].maxBal$

BY $\langle 1\rangle$a, $\langle 2\rangle 2$ DEFS Inv, $MsgInv$

$\langle 4\rangle 2.$ $\forall\, c \in (state[q][p].maxVBal + 1) \mathrel{..} (state[q][p].maxBal - 1)$:

$\neg\exists\, v \in Value : VotedForIn(p,\ c,\ v)$

BY $\langle 2\rangle$a, $\langle 4\rangle 1$ DEFS Inv, $MsgInv$

$\langle 4\rangle 3.$ $m.state[m.from].maxVBal \in Ballot \land m.state[m.from].maxVVal \in Value$

BY $\langle 1\rangle$a DEFS Inv, $MsgInv$

$\langle 4\rangle 4.\ \mathit{VotedForIn}(p,\ m.\mathit{state}[m.\mathit{from}].\mathit{maxVBal},\ m.\mathit{state}[m.\mathit{from}].\mathit{maxVVal})$

BY $\langle 4\rangle 3$ DEFS Inv, MsgInv

$\langle 4\rangle 5.\ m.\mathit{state}[m.\mathit{from}].\mathit{maxVBal} \in (\mathit{state}[q][p].\mathit{maxVBal} + 1) \mathrel{..} (\mathit{state}[q][p].\mathit{maxBal} - 1)$

BY $\langle 1\rangle$a, $\langle 2\rangle 2$, $\langle 4\rangle 1$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$

$\langle 3\rangle 2. \land \mathit{state}'[q][p].\mathit{maxBal} = \mathit{state}[q][p].\mathit{maxBal}$

$\land\ \mathit{state}'[q][p].\mathit{maxVBal} = \mathit{state}[q][p].\mathit{maxVBal}$

$\land\ \mathit{state}'[q][p].\mathit{maxVVal} = \mathit{state}[q][p].\mathit{maxVVal}$

$\langle 4\rangle 1.$CASE $\mathit{state}[q][p].\mathit{maxVBal} = m.\mathit{state}[m.\mathit{from}].\mathit{maxVBal}$

$\langle 5\rangle 1.$CASE $\mathit{state}[q][p].\mathit{maxVBal} = \ -1$

$\langle 6\rangle 1. \land \mathit{state}[q][p].\mathit{maxVVal} = \mathit{None}$

$\land\ m.\mathit{state}[m.\mathit{from}].\mathit{maxVVal} = \mathit{None}$

BY $\langle 2\rangle$a, $\langle 4\rangle 1$, $\langle 5\rangle 1$ DEFS Inv, MsgInv

$\langle 6\rangle$ QED

BY $\langle 1\rangle$b, $\langle 2\rangle 2$, $\langle 4\rangle 1$, $\langle 5\rangle 1$, $\langle 6\rangle 1$ DEFS Max

$\langle 5\rangle 2.$CASE $\mathit{state}[q][p].\mathit{maxVBal} \neq \ -1$

$\langle 6\rangle 1. \land \mathit{VotedForIn}(p,\ \mathit{state}[q][p].\mathit{maxVBal},\ \mathit{state}[q][p].\mathit{maxVVal})$

$\land\ \mathit{VotedForIn}(m.\mathit{from},\ m.\mathit{state}[m.\mathit{from}].\mathit{maxVBal},\ m.\mathit{state}[m.\mathit{from}].\mathit{maxVVal})$

BY $\langle 2\rangle$a, $\langle 4\rangle 1$, $\langle 5\rangle 2$ DEFS Inv, MsgInv

$\langle 6\rangle 2.\ \mathit{state}[q][p].\mathit{maxVVal} = m.\mathit{state}[m.\mathit{from}].\mathit{maxVVal}$

BY $\langle 4\rangle 1$, $\langle 6\rangle 1$ DEFS $\mathit{VotedForIn}$, MsgInv, Inv

$\langle 6\rangle$ QED

BY $\langle 1\rangle$b, $\langle 2\rangle 2$, $\langle 4\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle 2$ DEFS Max

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 2.$CASE $\mathit{state}[q][p].\mathit{maxVBal} > m.\mathit{state}[m.\mathit{from}].\mathit{maxVBal}$

BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 2\rangle$a, $\langle 2\rangle 2$, $\langle 4\rangle 2$ DEFS Max

$\langle 4\rangle$ QED

BY $\langle 1\rangle$a, $\langle 3\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 3\rangle 2$

$\langle 2\rangle 3.$CASE $\mathit{state}[q][p].\mathit{maxBal} = m.\mathit{state}[m.\mathit{from}].\mathit{maxBal}$

BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 1\rangle 1$, $\langle 2\rangle 3$ DEFS Max

$\langle 2\rangle$ QED

BY $\langle 1\rangle$a, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$

$\langle 1\rangle$ QED

BY $\langle 1\rangle$a, $\langle 1\rangle 2$, $\langle 1\rangle 3$

LEMMA $\mathit{UpdateStateValue} \ \triangleq$

ASSUME NEW $q \in \mathit{Participant}$, NEW $p \in \mathit{Participant}$, NEW $\mathit{pp} \in \mathit{State}$, $\mathit{pp}.\mathit{maxBal} \geq \mathit{pp}.\mathit{maxVBal}$, $\mathit{UpdateState}(q,\ p,\ \mathit{pp})$, Inv

PROVE $\ \lor \land \mathit{state}'[q][q].\mathit{maxVBal} = \mathit{state}[q][q].\mathit{maxVBal}$

$\land\ \mathit{state}'[q][q].\mathit{maxVVal} = \mathit{state}[q][q].\mathit{maxVVal}$

$\lor\ \land \mathit{state}'[q][q].\mathit{maxVBal} = \mathit{pp}.\mathit{maxVBal}$

```
$\land pp.maxVBal = pp.maxBal$
$\land state'[q][q].maxVVal = pp.maxVVal$
$\land state'[q][q].maxBal = pp.maxVBal$
$\land state'[q][q].maxBal \geq state'[q][q].maxVBal$
$\land state'[q][q].maxVBal \geq state[q][q].maxVBal$
$\langle 1 \rangle$ USE DEFS $TypeOK$, $State$, $AllBallot$, $Ballot$, $Message$, $Inv$
$\langle 1 \rangle$a. $state'[q][q].maxVBal =$ IF $(Max(state[q][q].maxBal, pp.maxBal) \leq pp.maxVBal)$
 THEN $pp.maxVBal$
 ELSE $state[q][q].maxVBal$
BY DEFS $UpdateState$
$\langle 1 \rangle$b. $state'[q][q].maxVVal =$ IF $(Max(state[q][q].maxBal, pp.maxBal) \leq pp.maxVBal)$
 THEN $pp.maxVVal$
 ELSE $state[q][q].maxVVal$
BY DEFS $UpdateState$
$\langle 1 \rangle$c. $state'[q][q].maxBal = Max(state[q][q].maxBal, pp.maxBal)$
BY DEFS $UpdateState$
$\langle 1 \rangle$d. $pp.maxVBal \leq Max(state[q][q].maxBal, pp.maxBal)$
BY DEFS $Max$
$\langle 1 \rangle$f. $state[q][q].maxBal \geq state[q][q].maxVBal$
BY DEFS $AccInv$
$\langle 1 \rangle$e. $state[q][q].maxVBal \leq Max(state[q][q].maxBal, pp.maxBal)$
$\langle 2 \rangle$1. $state[q][q].maxBal \leq Max(state[q][q].maxBal, pp.maxBal)$
BY DEFS $Max$
$\langle 2 \rangle$2. $state[q][q].maxBal \in AllBallot \land Max(state[q][q].maxBal, pp.maxBal) \in AllBallot$
BY DEFS $Max$
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$f, $\langle 2 \rangle$1, $\langle 2 \rangle$2
$\langle 1 \rangle$1.CASE $(Max(state[q][q].maxBal, pp.maxBal) \leq pp.maxVBal)$
$\langle 2 \rangle$1. $state'[q][q].maxVBal = pp.maxVBal$
BY $\langle 1 \rangle$1 DEFS $UpdateState$
$\langle 2 \rangle$2. $state'[q][q].maxVVal = pp.maxVVal$
BY $\langle 1 \rangle$1 DEFS $UpdateState$
$\langle 2 \rangle$3. $state'[q][q].maxVBal \geq state[q][q].maxVBal$
$\langle 3 \rangle$1. $pp.maxVBal \geq state[q][q].maxBal$
BY $\langle 1 \rangle$1 DEFS $Max$
$\langle 3 \rangle$2. $pp.maxVBal \geq state[q][q].maxVBal$
BY $\langle 3 \rangle$1, $\langle 1 \rangle$f DEFS $MsgInv$
$\langle 3 \rangle$ QED
BY $\langle 2 \rangle$1, $\langle 3 \rangle$2
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$1, $\langle 2 \rangle$1, $\langle 2 \rangle$2, $\langle 2 \rangle$3, $\langle 1 \rangle$c, $\langle 1 \rangle$d, $\langle 1 \rangle$e DEFS $Max$
$\langle 1 \rangle$2.CASE $\neg(Max(state[q][q].maxBal, pp.maxBal) \leq pp.maxVBal)$
$\langle 2 \rangle$1. $state'[q][q].maxVBal = state[q][q].maxVBal$
BY $\langle 1 \rangle$2 DEFS $UpdateState$
$\langle 2 \rangle$2. $state'[q][q].maxVVal = state[q][q].maxVVal$
```

BY $\langle 1\rangle 2$ DEFS $UpdateState$

$\langle 2\rangle 3.$ $state'[q][q].maxVBal \geq state[q][q].maxVBal$

BY $\langle 2\rangle 1$ DEFS $AccInv$

$\langle 2\rangle$ QED

BY $\langle 1\rangle 2$, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 1\rangle$c, $\langle 1\rangle$e DEFS Max

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

LEMMA $AcceptMsgInv \triangleq$ ASSUME NEW $p \in Participant$, NEW $b \in Ballot$, NEW $v \in Value$, $Accept(p,\ b,\ v)$, I

PROVE $MsgInv'$

$\langle 1\rangle$ USE DEF $TypeOK$, $Ballot$, $AllBallot$, Inv, $MsgInv$, $State$, $Send$, $Message$

$\langle 1\rangle$ SUFFICES ASSUME NEW $m \in msgs'$

PROVE $MsgInv!(m)'$

OBVIOUS

$\langle 1\rangle$ DEFINE $mm \triangleq [from \mapsto p,\ to \mapsto Participant \setminus \{p\},\ state \mapsto state'[p]]$

$\langle 1\rangle$a. $mm \in msgs' \land mm.state[p].maxVBal \in Ballot \land mm.state[p].maxVVal \in Value$

BY DEFS $Accept$

$\langle 1\rangle$b. $mm.state[p].maxBal = mm.state[p].maxVBal \land mm.state[p].maxBal = b$

BY $\langle 1\rangle$a DEFS $Accept$

$\langle 1\rangle$c. $m.from \notin m.to$

BY DEFS $Accept$

$\langle 1\rangle$d. $mm.state[p].maxBal \geq mm.state[p].maxVBal$

BY SMTDEFS $AccInv$, $Accept$

$\langle 1\rangle$e. $\land\ state[p][p].maxVBal \leq state'[p][p].maxVBal$

$\land\ state[p][p].maxBal \leq state'[p][p].maxBal$

BY $\langle 1\rangle$a DEFS $Accept$, $AccInv$

$\langle 1\rangle$1.CASE $mm = m$

$\langle 2\rangle 2.$ $\land\ m.state[m.from].maxBal = m.state[m.from].maxVBal$

$\land\ m.from = p$

$\land\ m.state[p].maxBal = b$

BY $\langle 1\rangle 1$, $\langle 1\rangle$b DEFS $Accept$

$\langle 2\rangle 1.$ $\lor\ \land\ (m.state)[m.from].maxVVal \in Value$

$\land\ (m.state)[m.from].maxVBal \in Nat$

$\land\ VotedForIn(m.from,\ (m.state)[m.from].maxVBal,\ (m.state)[m.from].maxVVal)'$

$\lor\ \land\ (m.state)[m.from].maxVVal = None$

$\land\ (m.state)[m.from].maxVBal = -1$

BY $\langle 1\rangle 1$, $\langle 2\rangle 2$ DEFS $Accept$, $VotedForIn$

$\langle 2\rangle$a. $m.state[m.from].maxBal \geq m.state[m.from].maxVBal$

BY $\langle 1\rangle$d, $\langle 1\rangle 1$

$\langle 2\rangle$b. $\forall\, q \in Participant :\ \land\ m.state[q].maxVBal \leq state'[q][q].maxVBal$

$\land\ m.state[q].maxBal \leq state'[q][q].maxBal$

BY $\langle 1\rangle 1$, $\langle 2\rangle 2$ DEFS $AccInv$, $Accept$

$\langle 2\rangle 3.$ $SafeAt(m.state[m.from].maxVBal,\ m.state[m.from].maxVVal)'$

$\langle 3\rangle$a. $m.state[m.from].maxVBal \in Ballot \land m.state[m.from].maxVVal \in Value$

BY $\langle 1\rangle$a, $\langle 1\rangle 1$ DEFS $Accept$

$\langle 3\rangle 1.$ $SafeAt(m.state[m.from].maxVBal,\ m.state[m.from].maxVVal)$

$\langle 4\rangle 1.$ PICK $Q \in Quorum :$

$\land \forall\, q \in Q : state[p][q].maxBal = b$

$\land\ \lor \forall\, q \in Q : state[p][q].maxVBal = \ -1$

$\lor \exists\, c \in 0 \,..\, (b-1) :$

$\land \forall\, r \in Q : state[p][r].maxVBal \leq c$

$\land \exists\, r \in Q :\ \land\, state[p][r].maxVBal = c$

$\land\, state[p][r].maxVVal = v$

BY DEFS $Accept$

$\langle 4\rangle 2.$CASE $\forall\, q \in Q : state[p][q].maxVBal = \ -1$

$\langle 5\rangle 1.$ $\forall\, qq \in Q :$

$\exists\, qm \in msgs :$

$\land\, qm.from = qq$

$\land\, qm.state[qq].maxBal = state[p][qq].maxBal$

$\land\, qm.state[qq].maxVBal = state[p][qq].maxVBal$

$\land\, qm.state[qq].maxVVal = state[p][qq].maxVVal$

$\langle 6\rangle 1.$ $\forall\, qq \in Q : state[p][qq].maxBal \in Ballot$

BY $\langle 4\rangle 1$

$\langle 6\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 6\rangle 1$, $QuorumAssumption$DEFS $AccInv$

$\langle 5\rangle 2.$ $\forall\, c \in 0 \,..\, (b-1) : \forall\, qq \in Q : WontVoteIn(qq,\ c)$

$\langle 6\rangle 1.$ $\forall\, qq \in Q : \forall\, cc \in 0 \,..\, (b-1) : \forall\, vv \in Value : \neg VotedForIn(qq,\ cc,\ vv)$

$\langle 7\rangle$ SUFFICES ASSUME NEW $qq \in Q$

PROVE $\forall\, cc \in 0 \,..\, (b-1) :$

$\neg\exists\, vv \in Value : VotedForIn(qq,\ cc,\ vv)$

OBVIOUS

$\langle 7\rangle 1$a. PICK $qm \in msgs :$

$\land\, qm.from = qq$

$\land\, qm.state[qq].maxBal = state[p][qq].maxBal$

$\land\, qm.state[qq].maxVBal = state[p][qq].maxVBal$

$\land\, qm.state[qq].maxVVal = state[p][qq].maxVVal$

BY $\langle 5\rangle 1$

$\langle 7\rangle 2.$ $\forall\, cc \in (qm.state[qq].maxVBal + 1) \,..\, (qm.state[qq].maxBal - 1) :$

$\neg\exists\, vv \in Value : VotedForIn(qq,\ cc,\ vv)$

$\langle 8\rangle 1.$ $qm.state[qq].maxBal \neq qm.state[qq].maxVBal$

BY $\langle 4\rangle 2$, $\langle 4\rangle 1$, $\langle 7\rangle 1$a

$\langle 8\rangle$ QED

BY $\langle 7\rangle 1$a, $\langle 8\rangle 1$ DEFS $MsgInv$

$\langle 7\rangle 3.$ $state[p][qq].maxBal = b \land state[p][qq].maxVBal = \ -1$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 7\rangle$ QED

BY $\langle 7\rangle 1$a, $\langle 7\rangle 2$, $\langle 7\rangle 3$

$\langle 6\rangle 2.$ $\forall\, qq \in Q : \forall\, cc \in 0 \,..\, (b-1) : state[qq][qq].maxBal > cc$

$\langle 7\rangle$ SUFFICES ASSUME NEW $qq \in Q$, NEW $cc \in 0 \,..\, (b-1)$

PROVE $state[qq][qq].maxBal > cc$

```
OBVIOUS
$\langle 7\rangle 1.\ state[qq][qq].maxBal \geq b$
BY $QuorumAssumption$, $\langle 4\rangle 1$ DEFS $AccInv$
$\langle 7\rangle 2.\ cc \in AllBallot \land cc < b \land b \in AllBallot \land state[qq][qq].maxBal \in AllBallot$
BY $QuorumAssumption$DEFS $AllBallot$
$\langle 7\rangle$ QED
BY $\langle 7\rangle 1$, $QuorumAssumption$, $\langle 7\rangle 2$
$\langle 6\rangle$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$ DEFS $WontVoteIn$
$\langle 5\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 2\rangle 2$, $\langle 4\rangle 1$, $\langle 5\rangle 2$, $QuorumAssumption$DEFS $SafeAt$, $Accept$
$\langle 4\rangle 3.$CASE $\exists\, c \in 0 \,..\, (b-1) :$
$\land\ \forall\, r \in Q : state[p][r].maxVBal \leq c$
$\land\ \exists\, r \in Q :\ \land\ state[p][r].maxVBal = c$
$\land\ state[p][r].maxVVal = v$
$\langle 5\rangle 1a.\ m.state[m.from].maxVBal = b$
BY $\langle 2\rangle 2$
$\langle 5\rangle 1b.\ state'[p][p].maxVVal = v$
BY DEFS $Accept$
$\langle 5\rangle 1c.\ m.state[m.from].maxVVal = v$
BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 1\rangle 1$, $\langle 5\rangle 1b$ DEFS $Accept$
$\langle 5\rangle 0.$ SUFFICES ASSUME NEW $cc \in 0 \,..\, (b-1)$, $\forall\, qq \in Q : state[p][qq].maxVBal \leq cc$,
NEW $qq \in Q$, $state[p][qq].maxVBal = cc$, $state[p][qq].maxVVal = v$,
NEW $d \in 0 \,..\, (b-1)$
PROVE $\exists\, QQ \in Quorum : \forall\, a \in QQ : VotedForIn(a, d, v) \lor WontVoteIn(a, d)$
BY $\langle 5\rangle 1a$, $\langle 5\rangle 1c$, $\langle 4\rangle 1$, $\langle 4\rangle 3$ DEFS $SafeAt$
$\langle 5\rangle 1d.\ state[p][qq].maxBal = b$
BY $\langle 4\rangle 1$
$\langle 5\rangle 1e.\ VotedForIn(qq, cc, v)$
$\langle 6\rangle 1.$ PICK $qqm \in msgs :$
$\land\ qqm.from = qq$
$\land\ qqm.state[qq].maxVBal = cc$
$\land\ qqm.state[qq].maxVVal = v$
$\langle 7\rangle 1.\ state[p][qq].maxBal \in Ballot$
BY $\langle 4\rangle 1$
$\langle 7\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 7\rangle 1$, $\langle 5\rangle 0$, $QuorumAssumption$DEFS $AccInv$
$\langle 6\rangle 2.\ \land\ v \in Value$
$\land\ cc \in Ballot$
BY $\langle 6\rangle 1$, $QuorumAssumption$
$\langle 6\rangle$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $QuorumAssumption$, $IsaT(200)$
$\langle 5\rangle 1.$CASE $d \in 0 \,..\, (cc-1)$
BY $\langle 5\rangle 1e$, $\langle 5\rangle 1$, $VotedInv$, $QuorumAssumption$DEFS $SafeAt$
$\langle 5\rangle 2.$CASE $d = cc$
```

$\langle 6\rangle 1.\ \forall\, qq1 \in Q,\ v1 \in \mathit{Value} : \mathit{VotedForIn}(qq1,\ cc,\ v1) \Rightarrow v1 = v$

BY $\langle 5\rangle$1e, $\mathit{VotedOnce}$, $\mathit{QuorumAssumption}$

$\langle 6\rangle 2.\ \forall\, qq1 \in Q : \mathit{state}[qq1][qq1].\mathit{maxBal} > cc$

$\langle 7\rangle$ SUFFICES ASSUME NEW $qq1 \in Q$

PROVE $\mathit{state}[qq1][qq1].\mathit{maxBal} > cc$

OBVIOUS

$\langle 7\rangle 1.\ \mathit{state}[qq1][qq1].\mathit{maxBal} \geq b$

BY $\mathit{QuorumAssumption}$, $\langle 4\rangle 1$ DEFS AccInv

$\langle 7\rangle 2.\ cc \in \mathit{AllBallot} \land cc < b \land b \in \mathit{AllBallot} \land \mathit{state}[qq1][qq1].\mathit{maxBal} \in \mathit{AllBallot}$

BY $\mathit{QuorumAssumption}$DEFS $\mathit{AllBallot}$

$\langle 7\rangle$ QED

BY $\langle 7\rangle 1$, $\mathit{QuorumAssumption}$, $\langle 7\rangle 2$

$\langle 6\rangle$ QED

BY $\langle 5\rangle 2$, $\langle 6\rangle 1$, $\langle 6\rangle 2$ DEFS $\mathit{WontVoteIn}$

$\langle 5\rangle 3.$CASE $d \in (cc + 1) \mathrel{..} (b - 1)$

$\langle 6\rangle 1.\ \forall\, qq1 \in Q : \forall\, v1 \in \mathit{Value} : \neg\, \mathit{VotedForIn}(qq1,\ d,\ v1)$

$\langle 7\rangle$ SUFFICES ASSUME NEW $qq1 \in Q$, NEW $v1 \in \mathit{Value}$

PROVE $\neg\, \mathit{VotedForIn}(qq1,\ d,\ v1)$

OBVIOUS

$\langle 7\rangle 1.$ PICK $qqm \in \mathit{msgs}$:

$\land\ qqm.\mathit{from} = qq1$

$\land\ qqm.\mathit{state}[qq1].\mathit{maxBal} = \mathit{state}[p][qq1].\mathit{maxBal}$

$\land\ qqm.\mathit{state}[qq1].\mathit{maxVBal} = \mathit{state}[p][qq1].\mathit{maxVBal}$

$\land\ qqm.\mathit{state}[qq1].\mathit{maxVVal} = \mathit{state}[p][qq1].\mathit{maxVVal}$

$\langle 8\rangle 1.\ \mathit{state}[p][qq1].\mathit{maxBal} \in \mathit{Ballot}$

BY $\langle 4\rangle 1$

$\langle 8\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 8\rangle 1$, $\mathit{QuorumAssumption}$DEFS AccInv

$\langle 7\rangle 2.\ \mathit{state}[p][qq1].\mathit{maxBal} = b \land \mathit{state}[p][qq1].\mathit{maxVBal} \leq cc$

BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 5\rangle 0$

$\langle 7\rangle 4.\ qqm.\mathit{state}[qq1].\mathit{maxBal} \neq qqm.\mathit{state}[qq1].\mathit{maxVBal}$

BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 5\rangle 0$, $\langle 7\rangle 1$, $\langle 7\rangle 2$

$\langle 7\rangle 3.\ \forall\, cc1 \in (qqm.\mathit{state}[qq1].\mathit{maxVBal} + 1) \mathrel{..} (qqm.\mathit{state}[qq1].\mathit{maxBal} - 1) : \neg \exists\, v2 \in \mathit{Value} : \mathit{VotedForIn}(qq1,$

BY $\langle 7\rangle 1$, $\langle 7\rangle 4$, $\mathit{QuorumAssumption}$

$\langle 7\rangle 5.\ d \in (qqm.\mathit{state}[qq1].\mathit{maxVBal} + 1) \mathrel{..} (qqm.\mathit{state}[qq1].\mathit{maxBal} - 1)$

$\langle 8\rangle 1.\ cc \in \mathit{AllBallot} \land \mathit{state}[p][qq1].\mathit{maxVBal} \in \mathit{AllBallot}$

BY $\mathit{QuorumAssumption}$

$\langle 8\rangle$ QED

BY $\langle 5\rangle 3$, $\langle 7\rangle 1$, $\langle 7\rangle 2$, $\langle 8\rangle 1$

$\langle 7\rangle$ QED

BY $\langle 5\rangle 3$, $\langle 7\rangle 5$, $\langle 7\rangle 3$

$\langle 6\rangle 2.\ \forall\, qq1 \in Q : \mathit{state}[qq1][qq1].\mathit{maxBal} > d$

$\langle 7\rangle$ SUFFICES ASSUME NEW $qq1 \in Q$

PROVE $\mathit{state}[qq1][qq1].\mathit{maxBal} > d$

OBVIOUS

$\langle 7\rangle 1.$ $state[qq1][qq1].maxBal \geq b$

BY $QuorumAssumption$, $\langle 4\rangle 1$ DEFS $AccInv$

$\langle 7\rangle 2.$ $d \in AllBallot \land d < b \land b \in AllBallot \land state[qq1][qq1].maxBal \in AllBallot$

BY $QuorumAssumption$DEFS $AllBallot$

$\langle 7\rangle$ QED

BY $\langle 7\rangle 1$, $QuorumAssumption$, $\langle 7\rangle 2$

$\langle 6\rangle$ QED

BY $\langle 5\rangle 3$, $\langle 6\rangle 1$, $\langle 6\rangle 2$ DEFS $WontVoteIn$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1a$, $\langle 5\rangle 1c$, $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEFS $Accept$

$\langle 3\rangle$ QED

BY $\langle 3\rangle a$, $\langle 3\rangle 1$, $SafeAtStable$DEFS $Next$

$\langle 2\rangle 4.$ $\forall\, ma \in msgs' : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$
$\land\, ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$
$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

BY $\langle 1\rangle 1$, $\langle 1\rangle a$, $\langle 1\rangle b$, $\langle 2\rangle 2$ DEFS $Accept$

$\langle 2\rangle 5.$ $m.state[m.from].maxBal \in Ballot$

BY $\langle 1\rangle 1$, $\langle 1\rangle a$, $\langle 1\rangle b$ DEF $Accept$

$\langle 2\rangle$ QED

BY $\langle 1\rangle d$, $\langle 1\rangle 1$, $\langle 2\rangle 1$, $\langle 2\rangle a$, $\langle 2\rangle b$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$

$\langle 1\rangle 2.$CASE $mm \neq m$

$\langle 2\rangle a.$ $m \in msgs$

BY $\langle 1\rangle 2$ DEFS $Accept$

$\langle 2\rangle b.$ $\forall\, q \in Participant : \land\, m.state[q].maxVBal \leq state'[q][q].maxVBal$
$\land\, m.state[q].maxBal \leq state'[q][q].maxBal$

$\langle 3\rangle$ SUFFICES ASSUME NEW $q \in Participant$
PROVE $\land\, m.state[q].maxVBal \leq state'[q][q].maxVBal$
$\land\, m.state[q].maxBal \leq state'[q][q].maxBal$

OBVIOUS

$\langle 3\rangle 1.$ $\land\, m.state[q].maxVBal \leq state[q][q].maxVBal$
$\land\, m.state[q].maxBal \leq state[q][q].maxBal$

BY $\langle 2\rangle a$

$\langle 3\rangle 2.$ $\land\, state[q][q].maxVBal \leq state'[q][q].maxVBal$
$\land\, state[q][q].maxBal \leq state'[q][q].maxBal$

BY $\langle 1\rangle e$ DEFS $Accept$, $AccInv$

$\langle 3\rangle 3.$ $\land\, state[q][q].maxVBal \in AllBallot \land m.state[q].maxVBal \in AllBallot$
$\land\, state[q][q]'.maxVBal \in AllBallot$
$\land\, state[q][q].maxBal \in AllBallot \land m.state[q].maxBal \in AllBallot$
$\land\, state[q][q]'.maxBal \in AllBallot$

OBVIOUS

$\langle 3\rangle$ QED

BY $\langle 2\rangle a$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle c.$ $m.state[m.from].maxBal \geq m.state[m.from].maxVBal$

BY $\langle 2\rangle$a

$\langle 2\rangle 1.$ $m.state[m.from].maxBal \in Ballot$

BY $\langle 2\rangle$a

$\langle 2\rangle 2.$ $\lor\ \land (m.state)[m.from].maxVVal \in Value$

$\land (m.state)[m.from].maxVBal \in Nat$

$\land\ VotedForIn(m.from,\ (m.state)[m.from].maxVBal,\ (m.state)[m.from].maxVVal)'$

$\lor\ \land (m.state)[m.from].maxVVal = None$

$\land (m.state)[m.from].maxVBal = -1$

BY $\langle 1\rangle 2$, $\langle 2\rangle 1$ DEFS $Accept$, $VotedForIn$

$\langle 2\rangle 3.$CASE $(m.state)[m.from].maxBal \neq (m.state)[m.from].maxVBal$

$\langle 3\rangle 1.$ $(m.state)[m.from].maxBal \leq state'[m.from][m.from].maxBal$

$\langle 4\rangle 1$ $(m.state)[m.from].maxBal \leq state[m.from][m.from].maxBal$

BY $\langle 1\rangle 2$, $\langle 2\rangle$a, $\langle 2\rangle 3$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$ DEFS $Accept$

$\langle 3\rangle 2.$ $\forall\, cc \in (m.state)[m.from].maxVBal + 1 \,..\, (m.state)[m.from].maxBal - 1 :$

$\neg(\exists\, vv \in Value : VotedForIn(m.from,\ cc,\ vv))'$

$\langle 4\rangle 1.$ $\forall\, cc \in (m.state)[m.from].maxVBal + 1 \,..\, (m.state)[m.from].maxBal - 1 :$

$\neg(\exists\, vv \in Value : VotedForIn(m.from,\ cc,\ vv))$

BY $\langle 1\rangle 2$, $\langle 2\rangle$a, $\langle 2\rangle 3$ DEFS $VotedForIn$, $Accept$

$\langle 4\rangle 2.$CASE $m.from = p$

$\langle 5\rangle$.SUFFICES ASSUME NEW $cc \in (m.state[m.from].maxVBal) + 1 \,..\, (m.state[m.from].maxBal - 1)$,

NEW $vv \in Value$, $VotedForIn(p,\ cc,\ vv)'$

PROVE FALSE

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 5\rangle$a. PICK $pm \in msgs'$:

$\land\ pm.from = p$

$\land\ pm.state[p].maxBal = cc$

$\land\ pm.state[p].maxVBal = cc$

$\land\ pm.state[p].maxVVal = vv$

BY DEFS $VotedForIn$

$\langle 5\rangle$b. $pm \notin msgs$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 5\rangle$a DEFS $VotedForIn$

$\langle 5\rangle 1.$ $b = cc$

$\langle 6\rangle 1.$ $pm = mm$

BY $\langle 1\rangle$a, $\langle 1\rangle$b, $\langle 5\rangle$a, $\langle 5\rangle$b DEFS $Accept$, $VotedForIn$

$\langle 6\rangle$ QED

BY $\langle 5\rangle$a, $\langle 6\rangle 1$ DEFS $Accept$

$\langle 5\rangle 2.$ $m.state[m.from].maxBal > b$

$\langle 6\rangle 1.$ $m.state[m.from].maxBal - 1 \geq cc \land (m.state)[m.from].maxVBal \in AllBallot$

OBVIOUS

$\langle 6\rangle 2.$ $cc \in AllBallot \land m.state[m.from].maxBal \in AllBallot$

BY $\langle 2\rangle 1$, $\langle 6\rangle 1$

$\langle 6\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle 3.\ m.state[m.from].maxBal \leq b$

BY $\langle 3\rangle 1$, $\langle 4\rangle 2$ DEFS $Accept$

$\langle 5\rangle$ QED

BY $\langle 1\rangle 2$, $\langle 2\rangle 3$, $\langle 4\rangle 2$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ DEFS $VotedForIn$, $Accept$

$\langle 4\rangle 3.$CASE $m.from \neq p$

BY $\langle 4\rangle 1$, $\langle 4\rangle 3$ DEFS $Accept$, $VotedForIn$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle$ QED

BY $\langle 1\rangle c$, $\langle 2\rangle 1$, $\langle 2\rangle b$, $\langle 2\rangle c$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 3\rangle 1$, $\langle 3\rangle 2$

$\langle 2\rangle 4.$CASE $(m.state)[m.from].maxBal = (m.state)[m.from].maxVBal$

$\langle 3\rangle 1.\ SafeAt(m.state[m.from].maxVBal,\ m.state[m.from].maxVVal)'$

$\langle 4\rangle a.\ m.state[m.from].maxVBal \in Ballot \land m.state[m.from].maxVVal \in Value$

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 4$

$\langle 4\rangle 1.\ SafeAt(m.state[m.from].maxVBal,\ m.state[m.from].maxVVal)$

BY $\langle 2\rangle a$, $\langle 2\rangle 4$

$\langle 4\rangle 2.$ QED

BY $\langle 4\rangle a$, $\langle 4\rangle 1$, $SafeAtStable$DEFS $Next$

$\langle 3\rangle 2.\ \forall\, ma \in msgs' : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$

$\land\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

$\langle 4\rangle 1.\ \forall\, ma \in msgs : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$

$\land\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

BY $\langle 2\rangle a$, $\langle 2\rangle 4$

$\langle 4\rangle 2.\ m.state[m.from].maxBal \neq mm.state[mm.from].maxBal$

BY $\langle 1\rangle a$, $\langle 1\rangle b$, $\langle 2\rangle a$, $\langle 2\rangle 4$ DEFS $Accept$

$\langle 4\rangle$ QED

BY $\langle 1\rangle a$, $\langle 1\rangle b$, $\langle 1\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEFS $Accept$

$\langle 3\rangle$ QED

BY $\langle 1\rangle c$, $\langle 2\rangle 1$, $\langle 2\rangle b$, $\langle 2\rangle c$, $\langle 2\rangle 2$, $\langle 2\rangle 4$, $\langle 3\rangle 1$, $\langle 3\rangle 2$

$\langle 2\rangle$ QED

BY $\langle 1\rangle c$, $\langle 2\rangle 1$, $\langle 2\rangle c$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

LEMMA $UpdateStateMsgInv \triangleq$

ASSUME NEW $q \in Participant$, NEW $p \in Participant$, NEW $mm \in msgs$, $mm.from = p$, Inv, $q \in mm.to$, $Next$

$UpdateState(q,\ p,\ mm.state[p])$, $TypeOK'$, $Send([from \mapsto q,\ to \mapsto \{mm.from\},\ state \mapsto state'[q]])$

PROVE $MsgInv'$

$\langle 1\rangle$ USE DEFS $TypeOK$, $Ballot$, $AllBallot$, $MsgInv$, $State$, $Send$, $Message$

$\langle 1\rangle$ DEFINE $nm \triangleq [from \mapsto q,\ to \mapsto \{mm.from\},\ state \mapsto state'[q]]$

$\langle 1\rangle a.\ nm \in msgs'$

OBVIOUS

$\langle 1\rangle aa.\ state'[q][q].maxBal = Max(state[q][q].maxBal,\ mm.state[p].maxBal)$

BY DEFS $UpdateState$

$\langle 1\rangle$aaa. $state'[q][q].maxBal \geq state[q][q].maxBal$

$\langle 2\rangle$1. $mm.state[p].maxBal \in Ballot \land state[q][q].maxBal \in AllBallot$

BY DEFS Inv

$\langle 2\rangle$ QED

BY $\langle 1\rangle$aa, $\langle 2\rangle$1 DEFS Max

$\langle 1\rangle$.SUFFICES ASSUME NEW $m \in msgs'$

PROVE $MsgInv!(m)'$

OBVIOUS

$\langle 1\rangle$bb. $\land \lor \land state'[q][q].maxVBal = state[q][q].maxVBal$

$\land state'[q][q].maxVVal = state[q][q].maxVVal$

$\lor \land state'[q][q].maxVBal = mm.state[p].maxVBal$

$\land mm.state[p].maxVBal = mm.state[p].maxBal$

$\land state'[q][q].maxVVal = mm.state[p].maxVVal$

$\land state'[q][q].maxBal = mm.state[p].maxVBal$

$\land state'[q][q].maxBal \geq state'[q][q].maxVBal$

$\land state'[q][q].maxVBal \geq state[q][q].maxVBal$

$\langle 2\rangle$1. $mm.state[p] \in State$

OBVIOUS

$\langle 2\rangle$2. $mm.state[p].maxBal \geq mm.state[p].maxVBal$

BY DEFS Inv

$\langle 2\rangle$ QED

BY $\langle 2\rangle$1, $\langle 2\rangle$2, $UpdateStateValue$DEFS $Next$

$\langle 1\rangle$b. $\land \lor \land nm.state[q].maxVBal = state[q][q].maxVBal$

$\land nm.state[q].maxVVal = state[q][q].maxVVal$

$\land nm.state[q].maxBal = Max(state[q][q].maxBal, mm.state[p].maxBal)$

$\lor \land nm.state[q].maxBal = mm.state[p].maxVBal$

$\land mm.state[p].maxVBal = mm.state[p].maxBal$

$\land nm.state[q].maxVBal = mm.state[p].maxVBal$

$\land nm.state[q].maxVVal = mm.state[p].maxVVal$

$\land nm.state[q].maxBal = Max(state[q][q].maxBal, mm.state[p].maxBal)$

$\land nm.state[q].maxVBal \geq state[q][q].maxVBal$

$\langle 2\rangle$3. $nm.state[q].maxVBal \geq state[q][q].maxVBal$

BY $\langle 1\rangle$bb

$\langle 2\rangle$ QED

BY $\langle 1\rangle$bb, $\langle 1\rangle$aa, $\langle 2\rangle$3, $\langle 1\rangle$a

$\langle 1\rangle$c. $nm.state[q].maxBal \geq nm.state[q].maxVBal$

BY $\langle 1\rangle$bb

$\langle 1\rangle$d. $m.from \notin m.to$

BY DEFS Inv

$\langle 1\rangle$e. $nm.state[nm.from].maxBal = state'[q][q].maxBal$

BY DEFS Inv

$\langle 1\rangle$1.CASE $nm = m$

$\langle 2\rangle$a. $m.state[m.from].maxBal \in Ballot$

$\langle 3\rangle$1. $mm.state[p].maxBal \in Ballot \land state[q][q].maxBal \in AllBallot$

```
BY DEFS $Inv$
$\langle 3 \rangle$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle$b, $\langle 3 \rangle 1$ DEFS $Max$
$\langle 2 \rangle$b. $m.state[m.from].maxBal \geq m.state[m.from].maxVBal$
BY $\langle 1 \rangle$c, $\langle 1 \rangle 1$
$\langle 2 \rangle$c. $\lor \land (m.state)[m.from].maxVVal \in Value$
$\land (m.state)[m.from].maxVBal \in Ballot$
$\lor \land (m.state)[m.from].maxVVal = None$
$\land (m.state)[m.from].maxVBal = -1$
BY $\langle 1 \rangle$b, $\langle 1 \rangle 1$, $\langle 2 \rangle$a DEFS $Inv$, $AccInv$
$\langle 2 \rangle$d. $m.state[m.from].maxBal = state'[m.from][m.from].maxBal$
BY $\langle 1 \rangle 1$
$\langle 2 \rangle$e. $\forall a \in Participant : \land m.state[a].maxVBal \leq state'[a][a].maxVBal$
$\land m.state[a].maxBal \leq state'[a][a].maxBal$
$\langle 3 \rangle$ SUFFICES ASSUME NEW $a \in Participant$
PROVE $\land m.state[a].maxVBal \leq state'[a][a].maxVBal$
$\land m.state[a].maxBal \leq state'[a][a].maxBal$
OBVIOUS
$\langle 3 \rangle 1$. $\land state'[q][p].maxVBal = Max(state[q][p].maxVBal, mm.state[mm.from].maxVBal)$
$\land state'[q][p].maxBal = Max(state[q][p].maxBal, mm.state[mm.from].maxBal)$
BY DEFS $UpdateState$
$\langle 3 \rangle 2$. $\land state[q][p].maxVBal \leq state[p][p].maxVBal \land mm.state[mm.from].maxVBal \leq state[p][p].maxVBal$
$\land state[q][p].maxBal \leq state[p][p].maxBal \land mm.state[mm.from].maxBal \leq state[p][p].maxBal$
BY DEFS $MsgInv$, $AccInv$, $Inv$
$\langle 3 \rangle 3$. $\land state'[q][p].maxVBal \leq state[p][p].maxVBal$
$\land state'[q][p].maxBal \leq state[p][p].maxBal$
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$ DEFS $Max$
$\langle 3 \rangle 4$. $\land state'[p][p].maxVBal = state[p][p].maxVBal$
$\land state'[p][p].maxBal = state[p][p].maxBal$
$\langle 4 \rangle 1$. $p \neq q$
BY DEFS $Inv$
$\langle 4 \rangle$ QED
BY $\langle 4 \rangle 1$ DEFS $UpdateState$
$\langle 3 \rangle 5$.CASE $a = p$
BY $\langle 1 \rangle 1$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$
$\langle 3 \rangle 6$.CASE $a = q$
$\langle 4 \rangle 1$. $\land m.state[a].maxVBal = state'[q][q].maxVBal$
$\land m.state[a].maxBal = state'[q][q].maxBal$
BY $\langle 1 \rangle 1$, $\langle 3 \rangle 6$
$\langle 4 \rangle 2$. $\land m.state[a].maxVBal \in AllBallot \land state'[q][q].maxVBal \in AllBallot$
$\land m.state[a].maxBal \in AllBallot \land state'[q][q].maxBal \in AllBallot$
BY DEFS $Inv$
$\langle 4 \rangle$ QED
BY $\langle 3 \rangle 6$, $\langle 4 \rangle 1$, $\langle 4 \rangle 2$
$\langle 3 \rangle 7$.CASE $a \neq p \land a \neq q$
```

```
$\langle 4\rangle 1.\ \land\ state'[a][a].maxVBal = state[a][a].maxVBal$
$\land\ state'[a][a].maxBal = state[a][a].maxBal$
BY $\langle 3\rangle 7$ DEFS $UpdateState$
$\langle 4\rangle 2.\ \land\ state[q][a].maxVBal \leq state[a][a].maxVBal$
$\land\ state[q][a].maxBal \leq state[a][a].maxBal$
BY DEFS $Inv$, $AccInv$
$\langle 4\rangle 3.\ \land\ state'[q][a].maxVBal \leq state[a][a].maxVBal$
$\land\ state'[q][a].maxBal \leq state[a][a].maxBal$
BY $\langle 3\rangle 7$, $\langle 4\rangle 2$ DEFS $UpdateState$
$\langle 4\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 3\rangle 7$, $\langle 4\rangle 1$, $\langle 4\rangle 3$
$\langle 3\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $\langle 3\rangle 7$
$\langle 2\rangle 1.$CASE $m.state[q].maxBal = m.state[q].maxVBal$
$\langle 3\rangle a.\ \land\ (m.state)[m.from].maxVVal \in Value$
$\land\ (m.state)[m.from].maxVBal \in Ballot$
BY $\langle 1\rangle 1$, $\langle 2\rangle c$, $\langle 2\rangle 1$, $\langle 2\rangle a$
$\langle 3\rangle 1.\ SafeAt(m.state[m.from].maxVBal,\ m.state[m.from].maxVVal)'$
$\langle 4\rangle 1.$CASE $(\ \land\ m.state[m.from].maxVBal = state[q][q].maxVBal$
$\land\ m.state[m.from].maxVVal = state[q][q].maxVVal)$
$\langle 5\rangle a.\ state[q][q].maxVBal \in Ballot \land state[q][q].maxVVal \in Value$
BY $\langle 3\rangle a$, $\langle 4\rangle 1$
$\langle 5\rangle b.\ VotedForIn(q,\ state[q][q].maxVBal,\ state[q][q].maxVVal)$
BY $\langle 5\rangle a$ DEFS $Inv$, $AccInv$
$\langle 5\rangle 1.\ SafeAt(state[q][q].maxVBal,\ state[q][q].maxVVal)$
BY $\langle 5\rangle a$, $\langle 5\rangle b$, $VotedInv$DEFS $Inv$
$\langle 5\rangle 2.\ SafeAt(m.state[m.from].maxVBal,\ m.state[m.from].maxVVal)$
BY $\langle 5\rangle 1$, $\langle 4\rangle 1$
$\langle 5\rangle$ QED
BY $\langle 3\rangle a$, $\langle 5\rangle 2$, $SafeAtStable$
$\langle 4\rangle 2.$CASE $(\ \land\ m.state[m.from].maxBal = mm.state[p].maxVBal$
$\land\ m.state[m.from].maxVBal = mm.state[p].maxVBal$
$\land\ m.state[m.from].maxVVal = mm.state[p].maxVVal)$
$\langle 5\rangle a.\ mm.state[p].maxBal = mm.state[p].maxVBal$
BY $\langle 1\rangle 1$, $\langle 1\rangle b$, $\langle 2\rangle 1$, $\langle 4\rangle 2$ DEFS $Max$, $Inv$
$\langle 5\rangle 1.\ SafeAt(mm.state[p].maxVBal,\ mm.state[p].maxVVal)$
BY $\langle 5\rangle a$ DEFS $Inv$
$\langle 5\rangle 2.\ SafeAt(m.state[m.from].maxVBal,\ m.state[m.from].maxVVal)$
BY $\langle 5\rangle 1$, $\langle 4\rangle 2$
$\langle 5\rangle$ QED
BY $\langle 3\rangle a$, $\langle 5\rangle 2$, $SafeAtStable$
$\langle 4\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 1\rangle b$, $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 2.\ \forall\, ma \in msgs' : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$
$\land\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$
```

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

$\langle 4\rangle 1.\ \forall\, ma \in msgs : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$

$\land\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

$\langle 5\rangle 1.$CASE $(\ \land\ m.state[m.from].maxBal = mm.state[p].maxVBal$

$\land\ m.state[m.from].maxVBal = mm.state[p].maxVBal$

$\land\ m.state[m.from].maxVVal = mm.state[p].maxVVal)$

$\langle 6\rangle$a. $mm.state[p].maxBal = mm.state[p].maxVBal$

BY $\langle 1\rangle 1$, $\langle 1\rangle$b, $\langle 2\rangle 1$, $\langle 5\rangle 1$ DEFS Max, Inv

$\langle 6\rangle 1.\ \forall\, ma \in msgs : (ma.state[ma.from].maxBal = mm.state[p].maxBal$

$\land\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = mm.state[p].maxVVal$

BY $\langle 6\rangle$a DEFS Inv

$\langle 6\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 2\rangle 1$, $\langle 5\rangle 1$, $\langle 6\rangle 1$, $\langle 6\rangle$a

$\langle 5\rangle 2.$CASE $(\ \land\ m.state[m.from].maxVBal = state[q][q].maxVBal$

$\land\ m.state[m.from].maxVVal = state[q][q].maxVVal)$

$\langle 6\rangle$a. $VotedForIn(q,\ state[q][q].maxVBal,\ state[q][q].maxVVal)$

BY $\langle 3\rangle$a, $\langle 5\rangle 2$ DEFS $AccInv$, Inv

$\langle 6\rangle$b. PICK $qqm \in msgs$:

$\land\ qqm.from = q$

$\land\ qqm.state[q].maxBal = state[q][q].maxVBal$

$\land\ qqm.state[q].maxVBal = state[q][q].maxVBal$

$\land\ qqm.state[q].maxVVal = state[q][q].maxVVal$

BY $\langle 6\rangle$a DEFS $VotedForIn$

$\langle 6\rangle$c. $qqm.state[q].maxBal = m.state[m.from].maxBal \land qqm.state[q].maxBal = m.state[m.from].maxVBal$

BY $\langle 1\rangle 1$, $\langle 2\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle$b

$\langle 6\rangle 1.\ \forall\, ma \in msgs : (ma.state[ma.from].maxBal = qqm.state[q].maxBal$

$\land\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = qqm.state[q].maxVVal$

BY $\langle 6\rangle$b DEFS Inv

$\langle 6\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 2\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle$b, $\langle 6\rangle$c, $\langle 6\rangle 1$

$\langle 5\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle$b, $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 1\rangle 1$

$\langle 3\rangle 3.\ VotedForIn(m.from,\ (m.state)[m.from].maxVBal,\ (m.state)[m.from].maxVVal)'$

$\langle 4\rangle$a. $\land\ (m.state)[m.from].maxVVal \in Value$

$\land\ (m.state)[m.from].maxVBal \in Ballot$

BY $\langle 1\rangle 1$, $\langle 2\rangle$c, $\langle 2\rangle 1$, $\langle 2\rangle$a

$\langle 4\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 2\rangle 1$, $\langle 4\rangle$a DEFS $VotedForIn$

$\langle 3\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle$d, $\langle 2\rangle$a, $\langle 2\rangle$b, $\langle 2\rangle$c, $\langle 2\rangle$e, $\langle 2\rangle 1$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle$2.CASE $m.state[q].maxBal \neq m.state[q].maxVBal$

$\langle 3\rangle$2. $\forall\, cc \in (m.state)[m.from].maxVBal + 1 \,..\, (m.state)[m.from].maxBal - 1 :$

$\neg(\exists\, vv \in Value : VotedForIn(m.from,\ cc,\ vv))'$

$\langle 4\rangle$1. $\forall\, cc \in (m.state)[m.from].maxVBal + 1 \,..\, (m.state)[m.from].maxBal - 1 :$

$\neg(\exists\, vv \in Value : VotedForIn(m.from,\ cc,\ vv))$

$\langle 5\rangle$ SUFFICES ASSUME NEW $cc \in (m.state)[m.from].maxVBal + 1 \,..\, (m.state)[m.from].maxBal - 1$

PROVE $\neg(\exists\, vv \in Value : VotedForIn(m.from,\ cc,\ vv))$

OBVIOUS

$\langle 5\rangle$a. $cc > (m.state)[q].maxVBal$

$\langle 6\rangle$1. $cc \geq (m.state)[m.from].maxVBal + 1$

OBVIOUS

$\langle 6\rangle$2. $(m.state)[m.from].maxVBal \in AllBallot$

BY $\langle 1\rangle$1, $\langle 1\rangle$b

$\langle 6\rangle$ QED

BY $\langle 1\rangle$1, $\langle 6\rangle$1, $\langle 6\rangle$2

$\langle 5\rangle$b. $cc \in Ballot$

$\langle 6\rangle$1. $(m.state)[m.from].maxVBal \in AllBallot$

BY $\langle 1\rangle$1, $\langle 1\rangle$b

$\langle 6\rangle$2. $(m.state)[m.from].maxVBal + 1 \in Ballot$

BY $\langle 6\rangle$1

$\langle 6\rangle$ QED

BY $\langle 6\rangle$2

$\langle 5\rangle$1. $\forall\, c \in Ballot : c > state[q][q].maxVBal \Rightarrow$

$\neg\exists\, v \in Value : VotedForIn(q,\ c,\ v)$

BY DEFS $AccInv$, Inv

$\langle 5\rangle$2. $(m.state)[m.from].maxVBal \geq state[q][q].maxVBal$

BY $\langle 1\rangle$1, $\langle 1\rangle$b

$\langle 5\rangle$3. $cc > state[q][q].maxVBal$

BY $\langle 1\rangle$1, $\langle 1\rangle$b, $\langle 5\rangle$2, $\langle 5\rangle$a DEFS Inv

$\langle 5\rangle$4. $\neg\exists\, vv \in Value : VotedForIn(q,\ cc,\ vv)$

BY $\langle 5\rangle$1, $\langle 5\rangle$3, $\langle 5\rangle$b

$\langle 5\rangle$ QED

BY $\langle 1\rangle$1, $\langle 5\rangle$4 DEF Inv

$\langle 4\rangle$ QED

BY $\langle 1\rangle$1, $\langle 2\rangle$2, $\langle 4\rangle$1 DEFS $VotedForIn$

$\langle 3\rangle$3. $\vee\ \wedge (m.state)[m.from].maxVVal \in Value$

$\wedge (m.state)[m.from].maxVBal \in Nat$

$\wedge\ VotedForIn(m.from,\ (m.state)[m.from].maxVBal,\ (m.state)[m.from].maxVVal)'$

$\vee\ \wedge (m.state)[m.from].maxVVal = None$

$\wedge (m.state)[m.from].maxVBal = -1$

$\langle 4\rangle$1. $\wedge\ m.state[m.from].maxVBal = state[q][q].maxVBal$

$\wedge\ m.state[m.from].maxVVal = state[q][q].maxVVal$

BY $\langle 1\rangle$b, $\langle 1\rangle$1, $\langle 2\rangle$2

$\langle 4\rangle$ QED

BY $\langle 1\rangle$b, $\langle 1\rangle$1, $\langle 2\rangle$a, $\langle 4\rangle$1 DEFS $AccInv$, $VotedForIn$, Inv

$\langle 3\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle$d, $\langle 2\rangle$a, $\langle 2\rangle$b, $\langle 2\rangle$c, $\langle 2\rangle$e, $\langle 2\rangle 2$, $\langle 2\rangle$d, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$

$\langle 1\rangle$2.CASE $nm \neq m$

$\langle 2\rangle$a. $m \in msgs$

BY $\langle 1\rangle 2$

$\langle 2\rangle$b. $m.from \notin m.to$

BY $\langle 2\rangle$a DEFS Inv

$\langle 2\rangle$c. $m.state[m.from].maxBal \geq m.state[m.from].maxVBal$

BY $\langle 2\rangle$a DEFS Inv

$\langle 2\rangle$d. $\forall\, a \in Participant : \wedge\, m.state[a].maxVBal \leq state'[a][a].maxVBal$

$\wedge\, m.state[a].maxBal \leq state'[a][a].maxBal$

$\langle 3\rangle$ SUFFICES ASSUME NEW $a \in Participant$

PROVE $\wedge\, m.state[a].maxVBal \leq state'[a][a].maxVBal$

$\wedge\, m.state[a].maxBal \leq state'[a][a].maxBal$

OBVIOUS

$\langle 3\rangle$1. $\wedge\, m.state[a].maxVBal \leq state[a][a].maxVBal$

$\wedge\, m.state[a].maxBal \leq state[a][a].maxBal$

BY $\langle 2\rangle$a DEFS Inv, $AccInv$

$\langle 3\rangle$2. $\wedge\, state[a][a].maxVBal \leq state'[a][a].maxVBal$

$\wedge\, state[a][a].maxBal \leq state'[a][a].maxBal$

$\langle 4\rangle$1.CASE $a = q$

BY $\langle 1\rangle$bb, $\langle 1\rangle$aaa, $\langle 4\rangle 1$

$\langle 4\rangle$2.CASE $a \neq q$

$\langle 5\rangle$1. $\wedge\, state[a][a].maxVBal = state'[a][a].maxVBal$

$\wedge\, state[a][a].maxBal = state'[a][a].maxBal$

BY $\langle 4\rangle 2$ DEFS $UpdateState$

$\langle 5\rangle$2. $\wedge\, state[a][a].maxVBal \in AllBallot \wedge state'[a][a].maxVBal \in AllBallot$

$\wedge\, state[a][a].maxBal \in AllBallot \wedge state'[a][a].maxBal \in AllBallot$

BY DEFS Inv

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle$3. $\wedge\, state[a][a].maxVBal \in AllBallot$

$\wedge\, m.state[a].maxVBal \in AllBallot$

$\wedge\, state'[a][a].maxVBal \in AllBallot$

$\wedge\, state[a][a].maxBal \in AllBallot$

$\wedge\, m.state[a].maxBal \in AllBallot$

$\wedge\, state'[a][a].maxBal \in AllBallot$

BY DEFS Inv

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle$1. $m.state[m.from].maxBal \in Ballot$

BY $\langle 1\rangle 2$, $\langle 2\rangle a$ DEFS Inv

$\langle 2\rangle 2.\ \lor \land (m.state)[m.from].maxVVal \in Value$

$\land (m.state)[m.from].maxVBal \in Nat$

$\land VotedForIn(m.from, (m.state)[m.from].maxVBal, (m.state)[m.from].maxVVal)'$

$\lor \land (m.state)[m.from].maxVVal = None$

$\land (m.state)[m.from].maxVBal = -1$

BY $\langle 1\rangle 2$, $\langle 2\rangle a$ DEFS $VotedForIn$, Inv

$\langle 2\rangle 3.$CASE $(m.state)[m.from].maxBal \neq (m.state)[m.from].maxVBal$

$\langle 3\rangle 1.\ (m.state)[m.from].maxBal \leq state'[m.from][m.from].maxBal$

$\langle 4\rangle a.\ (m.state)[m.from].maxBal \leq state[m.from][m.from].maxBal$

BY $\langle 1\rangle 2$, $\langle 2\rangle a$, $\langle 2\rangle 3$ DEFS Inv

$\langle 4\rangle 1.$CASE $m.from = q$

$\langle 5\rangle 1.\ state'[m.from][m.from].maxBal \geq state[m.from][m.from].maxBal$

BY $\langle 1\rangle aaa$, $\langle 4\rangle 1$

$\langle 5\rangle 2.\ state[m.from][m.from].maxBal \in AllBallot \land state'[m.from][m.from].maxBal \in AllBallot$

BY DEFS Inv

$\langle 5\rangle$ QED

BY $\langle 4\rangle a$, $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEFS Inv

$\langle 4\rangle 2.$CASE $m.from \neq q$

$\langle 5\rangle 1.$ UNCHANGED $state[m.from][m.from]$

BY $\langle 4\rangle 2$ DEFS $UpdateState$

$\langle 5\rangle$ QED

BY $\langle 4\rangle a$, $\langle 5\rangle 1$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle 2.\ \forall cc \in (m.state)[m.from].maxVBal + 1 \mathrel{..} (m.state)[m.from].maxBal - 1 :$

$\neg(\exists vv \in Value : VotedForIn(m.from, cc, vv))'$

$\langle 4\rangle 1.\ \forall cc \in (m.state)[m.from].maxVBal + 1 \mathrel{..} (m.state)[m.from].maxBal - 1 :$

$\neg(\exists vv \in Value : VotedForIn(m.from, cc, vv))$

BY $\langle 2\rangle a$, $\langle 2\rangle 3$ DEFS Inv

$\langle 4\rangle 2.$CASE $m.from = q$

BY $\langle 3\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEFS $VotedForIn$, Inv

$\langle 4\rangle 3.$CASE $m.from \neq q$

BY $\langle 4\rangle 1$, $\langle 4\rangle 3$ DEFS $VotedForIn$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle$ QED

BY $\langle 2\rangle b$, $\langle 2\rangle c$, $\langle 2\rangle d$, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 3\rangle 1$, $\langle 3\rangle 2$

$\langle 2\rangle 4.$CASE $(m.state)[m.from].maxBal = (m.state)[m.from].maxVBal$

$\langle 3\rangle a.\ m.state[m.from].maxVBal \in Ballot \land m.state[m.from].maxVVal \in Value$

BY $\langle 2\rangle a$, $\langle 2\rangle 4$ DEFS Inv

$\langle 3\rangle 1.\ SafeAt(m.state[m.from].maxVBal, m.state[m.from].maxVVal)'$

$\langle 4\rangle 1.\ SafeAt(m.state[m.from].maxVBal, m.state[m.from].maxVVal)$

BY $\langle 2\rangle a$, $\langle 2\rangle 4$ DEFS Inv

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 3\rangle$a, $\mathit{SafeAtStable}$

$\langle 3\rangle 2.\ \forall\, ma \in msgs' : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$

$\wedge\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

$\langle 4\rangle 1.\ \forall\, ma \in msgs : (ma.state[ma.from].maxBal = m.state[m.from].maxBal$

$\wedge\ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)$

$\Rightarrow ma.state[ma.from].maxVVal = m.state[m.from].maxVVal$

BY $\langle 2\rangle$a, $\langle 2\rangle 4$ DEFS Inv

$\langle 4\rangle 2.$CASE $\wedge\ nm.state[q].maxVBal = state[q][q].maxVBal$

$\wedge\ nm.state[q].maxVVal = state[q][q].maxVVal$

$\wedge\ nm.state[q].maxBal = Max(state[q][q].maxBal,\ mm.state[p].maxBal)$

$\langle 5\rangle 1.$CASE $nm.state[q].maxBal \neq nm.state[q].maxVBal$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 5\rangle 1$

$\langle 5\rangle 2.$CASE $nm.state[q].maxBal = nm.state[q].maxVBal$

$\langle 6\rangle$a. $nm.state[q].maxBal \in Ballot$

$\langle 7\rangle$a. $state[q][q].maxBal \in AllBallot \wedge mm.state[p].maxBal \in Ballot$

BY DEFS Inv

$\langle 7\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 5\rangle 2$, $\langle 7\rangle$a DEFS Max

$\langle 6\rangle 1.\ VotedForIn(q,\ state[q][q].maxVBal,\ state[q][q].maxVVal)$

BY $\langle 4\rangle 2$, $\langle 5\rangle 2$, $\langle 6\rangle$a DEFS AccInv, Inv

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEFS $\mathit{VotedForIn}$, Inv

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 3.$CASE $\wedge\ nm.state[q].maxBal = mm.state[p].maxVBal$

$\wedge\ mm.state[p].maxVBal = mm.state[p].maxBal$

$\wedge\ nm.state[q].maxVBal = mm.state[p].maxVBal$

$\wedge\ nm.state[q].maxVVal = mm.state[p].maxVVal$

BY $\langle 4\rangle 1$, $\langle 4\rangle 3$ DEFS Inv

$\langle 4\rangle$ QED

BY $\langle 1\rangle$b, $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle$ QED

BY $\langle 2\rangle$b, $\langle 2\rangle$c, $\langle 2\rangle$d, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 4$, $\langle 3\rangle 1$, $\langle 3\rangle 2$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

LEMMA $\mathit{OnMessageMsgInv} \triangleq$ ASSUME NEW $q \in Participant$, $OnMessage(q)$, Inv, TypeOK'

PROVE MsgInv'

$\langle 1\rangle$ USE DEF TypeOK, Ballot, $\mathit{AllBallot}$, Inv, MsgInv, State, Send, $\mathit{Message}$

$\langle 1\rangle$ SUFFICES ASSUME NEW $m \in msgs'$, NEW $mm \in msgs$, $OnMessage(q)!(mm)$

PROVE $MsgInv!(m)'$

BY DEFS $\mathit{OnMessage}$

$\langle 1 \rangle$a. $state'[q][q].maxBal \geq state[q][q].maxBal$

$\langle 2 \rangle$1. $state[q][q].maxBal \in AllBallot$

OBVIOUS

$\langle 2 \rangle$2. $mm.state[mm.from].maxBal \in AllBallot$

OBVIOUS

$\langle 2 \rangle$3. $state'[q][q].maxBal = Max(state[q][q].maxBal, mm.state[mm.from].maxBal)$

BY $ZenonT(100)$, $IsaT(100)$, $Z3T(100)$DEFS $OnMessage$, $UpdateState$

$\langle 2 \rangle$4. $Max(state[q][q].maxBal, mm.state[mm.from].maxBal) \geq state[q][q].maxBal$

BY $\langle 2 \rangle$1, $\langle 2 \rangle$2 DEFS Max

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle$1, $\langle 2 \rangle$2, $\langle 2 \rangle$3, $\langle 2 \rangle$4, $ZenonT(100)$, $IsaT(100)$, $Z3T(100)$

$\langle 1 \rangle$b. $\lor \ \land state'[q][q].maxVBal = state[q][q].maxVBal$

$\land state'[q][q].maxVVal = state[q][q].maxVVal$

$\lor \ \land state'[q][q].maxVBal = mm.state[mm.from].maxVBal$

$\land state'[q][q].maxVVal = mm.state[mm.from].maxVVal$

$\langle 2 \rangle$1. $mm.state[mm.from] \in State$

OBVIOUS

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle$1, $UpdateStateValue$ DEF $OnMessage$

$\langle 1 \rangle$c. $m.from \notin m.to$

BY DEFS $OnMessage$

$\langle 1 \rangle$d. $state'[q][q].maxVBal \geq state[q][q].maxVBal$

BY $UpdateStateValue$DEFS $OnMessage$

$\langle 1 \rangle$1.CASE $\lor (mm.state)[q].maxBal < (state')[q][q].maxBal$

$\lor (mm.state)[q].maxVBal < (state')[q][q].maxVBal$

$\langle 2 \rangle$1a. DEFINE $nm \triangleq [from \mapsto q, to \mapsto \{mm.from\}, state \mapsto state'[q]]$

$\langle 2 \rangle$1b. $nm \in msgs'$

BY $\langle 1 \rangle$1, $\langle 1 \rangle$a DEFS $OnMessage$

$\langle 2 \rangle$ QED

BY $UpdateStateMsgInv$, $\langle 1 \rangle$1 DEFS $Next$

$\langle 1 \rangle$2.CASE $\neg(\lor (mm.state)[q].maxBal < (state')[q][q].maxBal$

$\lor (mm.state)[q].maxVBal < (state')[q][q].maxVBal)$

$\langle 2 \rangle$1a. $m \in msgs$

BY $\langle 1 \rangle$2 DEFS $OnMessage$

$\langle 2 \rangle$b. $\forall a \in Participant : \ \land m.state[a].maxVBal \leq state'[a][a].maxVBal$

$\land m.state[a].maxBal \leq state'[a][a].maxBal$

$\langle 3 \rangle$ SUFFICES ASSUME NEW $a \in Participant$

PROVE $\ \land m.state[a].maxVBal \leq state'[a][a].maxVBal$

$\land m.state[a].maxBal \leq state'[a][a].maxBal$

OBVIOUS

$\langle 3 \rangle$1. $\land m.state[a].maxVBal \leq state[a][a].maxVBal$

$\land m.state[a].maxBal \leq state[a][a].maxBal$

BY $\langle 2 \rangle$1a

$\langle 3 \rangle$2. $\land state[a][a].maxVBal \leq state'[a][a].maxVBal$

$\land state[a][a].maxBal \leq state'[a][a].maxBal$

BY $\langle 1\rangle$a, $\langle 1\rangle$d DEFS $AccInv$, $UpdateState$

$\langle 3\rangle 3.$ $state[a][a].maxVBal \in AllBallot \land m.state[a].maxVBal \in AllBallot$

$\land\ state[a][a]'.maxVBal \in AllBallot \land state[a][a].maxBal \in AllBallot$

$\land\ state'[a][a].maxBal \in AllBallot \land m.state[a].maxBal \in AllBallot$

OBVIOUS

$\langle 3\rangle$ QED

BY $\langle 2\rangle$1a, $\langle 3\rangle$1, $\langle 3\rangle$2, $\langle 3\rangle$3

$\langle 2\rangle 1.$ $m.state[m.from].maxBal \in Ballot$

BY $\langle 2\rangle$1a

$\langle 2\rangle 2.$ $\lor\ \land (m.state)[m.from].maxVVal \in Value$

$\land (m.state)[m.from].maxVBal \in Nat$

$\land\ VotedForIn(m.from, (m.state)[m.from].maxVBal, (m.state)[m.from].maxVVal)'$

$\lor\ \land (m.state)[m.from].maxVVal = None$

$\land (m.state)[m.from].maxVBal = -1$

BY $\langle 1\rangle$2, $\langle 2\rangle$1 DEFS $OnMessage$, $VotedForIn$

$\langle 2\rangle$3.CASE $(m.state)[m.from].maxBal \neq (m.state)[m.from].maxVBal$

$\langle 3\rangle 1.$ $(m.state)[m.from].maxBal \leq state'[m.from][m.from].maxBal$

$\langle 4\rangle 1$ $(m.state)[m.from].maxBal \leq state[m.from][m.from].maxBal$

BY $\langle 1\rangle$2, $\langle 2\rangle$1a, $\langle 2\rangle$3

$\langle 4\rangle$2.CASE $m.from = q$

$\langle 5\rangle 1.$ $state'[m.from][m.from].maxBal \geq state[m.from][m.from].maxBal$

BY $\langle 1\rangle$a, $\langle 4\rangle$2

$\langle 5\rangle 2.$ $\land\ state'[m.from][m.from].maxBal \in AllBallot$

$\land\ state[m.from][m.from].maxBal \in AllBallot$

$\land (m.state)[m.from].maxBal \in AllBallot$

OBVIOUS

$\langle 5\rangle$ QED

BY $\langle 5\rangle$1, $\langle 4\rangle$1, $\langle 5\rangle$2

$\langle 4\rangle$3.CASE $m.from \neq q$

$\langle 5\rangle 1.$ $state'[m.from][m.from].maxBal = state[m.from][m.from].maxBal$

BY $\langle 2\rangle$1a, $\langle 4\rangle$3 DEFS $UpdateState$, Max, $OnMessage$

$\langle 5\rangle$ QED

BY $\langle 4\rangle$1, $\langle 4\rangle$3 DEFS $UpdateState$, $OnMessage$, Max

$\langle 4\rangle$ QED

BY $\langle 4\rangle$2, $\langle 4\rangle$3

$\langle 3\rangle 2.$ $\forall\, cc \in (m.state)[m.from].maxVBal + 1 \,..\, (m.state)[m.from].maxBal - 1 :$

$\neg(\exists\, vv \in Value : VotedForIn(m.from, cc, vv))'$

$\langle 4\rangle 1.$ $\forall\, cc \in (m.state)[m.from].maxVBal + 1 \,..\, (m.state)[m.from].maxBal - 1 :$

$\neg(\exists\, vv \in Value : VotedForIn(m.from, cc, vv))$

BY $\langle 1\rangle$2, $\langle 2\rangle$1a, $\langle 2\rangle$3 DEFS $VotedForIn$, $OnMessage$

$\langle 4\rangle$ QED

BY $\langle 4\rangle$1, $\langle 1\rangle$2 DEFS $OnMessage$, $VotedForIn$

$\langle 3\rangle$ QED

BY $\langle 1\rangle$2, $\langle 2\rangle$b, $\langle 2\rangle$1, $\langle 2\rangle$2, $\langle 2\rangle$3, $\langle 3\rangle$1, $\langle 3\rangle$2

$\langle 2\rangle$4.CASE $(m.state)[m.from].maxBal = (m.state)[m.from].maxVBal$

```
⟨3⟩1. SafeAt(m.state[m.from].maxVBal, m.state[m.from].maxVVal)′
⟨4⟩a. m.state[m.from].maxVBal ∈ Ballot ∧ m.state[m.from].maxVVal ∈ Value
BY ⟨2⟩1a, ⟨2⟩2, ⟨2⟩4
⟨4⟩1. SafeAt(m.state[m.from].maxVBal, m.state[m.from].maxVVal)
BY ⟨2⟩1a, ⟨2⟩4
⟨4⟩2. QED
BY ⟨4⟩a, ⟨4⟩1, SafeAtStableDEFS Next
⟨3⟩2. ∀ ma ∈ msgs′ : (ma.state[ma.from].maxBal = m.state[m.from].maxBal
 ∧ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)
 ⇒ ma.state[ma.from].maxVVal = m.state[m.from].maxVVal
⟨4⟩1. ∀ ma ∈ msgs : (ma.state[ma.from].maxBal = m.state[m.from].maxBal
 ∧ ma.state[ma.from].maxBal = ma.state[ma.from].maxVBal)
 ⇒ ma.state[ma.from].maxVVal = m.state[m.from].maxVVal
BY ⟨2⟩1a, ⟨2⟩4
⟨4⟩ QED
BY ⟨1⟩a, ⟨1⟩2, ⟨4⟩1 DEFS OnMessage
⟨3⟩ QED
BY ⟨1⟩c, ⟨2⟩b, ⟨2⟩1, ⟨2⟩2, ⟨2⟩4, ⟨3⟩1, ⟨3⟩2
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2


LEMMA OnMessageAccInv ≜
ASSUME NEW qq ∈ Participant, OnMessage(qq), Inv, TypeOK′
PROVE AccInv′
⟨1⟩ USE DEFS Ballot, AllBallot, Send, Message, State, TypeOK
⟨1⟩.PICK mm ∈ msgs : OnMessage(qq)!(mm)
BY DEFS OnMessage
⟨1⟩a. ∧ state′[qq][qq].maxBal ≥ state′[qq][qq].maxVBal
 ∧ state′[qq][qq].maxVBal ≥ state[qq][qq].maxVBal
BY UpdateStateValueDEFS OnMessage, Inv, MsgInv
⟨1⟩b. ∨ ∧ state′[qq][qq].maxVBal = state[qq][qq].maxVBal
 ∧ state′[qq][qq].maxVVal = state[qq][qq].maxVVal
 ∨ ∧ state′[qq][qq].maxVBal = mm.state[mm.from].maxVBal
 ∧ mm.state[mm.from].maxVBal = mm.state[mm.from].maxBal
 ∧ state′[qq][qq].maxVVal = mm.state[mm.from].maxVVal
 ∧ state′[qq][qq].maxBal = mm.state[mm.from].maxVBal
BY UpdateStateValue, ZenonT(100), SMTT(100), IsaT(100)DEFS OnMessage, Inv, MsgInv
⟨1⟩c. ∀ a ∈ Participant : a ≠ qq ⇒ state′[a] = state[a]
BY ZenonT(100), SMTT(100), IsaT(100)DEFS UpdateState
⟨1⟩d. DEFINE nm ≜ [from ↦ qq, to ↦ {mm.from}, state ↦ state′[qq]]
⟨1⟩e. ∧ state′[qq][qq].maxVBal ∈ AllBallot
 ∧ state[qq][qq].maxVBal ∈ AllBallot
```

$\land\ state[qq][qq].maxBal \in AllBallot$

$\land\ mm.state[mm.from].maxBal \in AllBallot$

$\land\ mm.state[mm.from].maxVBal \in AllBallot$

BY DEFS Inv

$\langle 1\rangle$f. $state'[qq][qq].maxBal \geq state[qq][qq].maxBal$

$\langle 2\rangle$1. $state'[qq][qq].maxBal = Max(state[qq][qq].maxBal,\ mm.state[mm.from].maxBal)$

BY DEFS $UpdateState$

$\langle 2\rangle$ QED

BY $\langle 1\rangle$e, $\langle 2\rangle$1 DEFS Max

$\langle 1\rangle$g. $\land\ state'[qq][mm.from].maxBal \geq state'[qq][mm.from].maxVBal$

$\land\ \lor\ \land\ state'[qq][mm.from].maxBal = state[qq][mm.from].maxBal$

$\land\ state'[qq][mm.from].maxVBal = state[qq][mm.from].maxVBal$

$\land\ state'[qq][mm.from].maxVVal = state[qq][mm.from].maxVVal$

$\lor\ \land\ state'[qq][mm.from].maxBal = mm.state[mm.from].maxBal$

$\land\ state'[qq][mm.from].maxVBal = mm.state[mm.from].maxVBal$

$\land\ state'[qq][mm.from].maxVVal = mm.state[mm.from].maxVVal$

BY $UpdateStateViewValue$, $ZenonT(100)$DEFS $OnMessage$, Inv, $MsgInv$

$\langle 1\rangle$1. $\forall\, a \in Participant :$

$\land\ (state'[a][a].maxVBal = -1) \equiv (state'[a][a].maxVVal = None)$

$\langle 2\rangle$ SUFFICES ASSUME NEW $a \in Participant$

PROVE $(state'[a][a].maxVBal = -1) \equiv (state'[a][a].maxVVal = None)$

OBVIOUS

$\langle 2\rangle$1. $(state[a][a].maxVBal = -1) \equiv (state[a][a].maxVVal = None)$

BY DEFS Inv, $AccInv$

$\langle 2\rangle$2.CASE $a \neq qq$

BY $\langle 2\rangle$1, $\langle 2\rangle$2 DEFS $UpdateState$

$\langle 2\rangle$3.CASE $a = qq$

$\langle 3\rangle$1. $((mm.state)[mm.from].maxVBal = -1) \equiv ((mm.state)[mm.from].maxVVal = None)$

BY $NoneNotAValue$, $ZenonT(100)$, $SMTT(100)$, $IsaT(100)$DEFS Inv, $MsgInv$

$\langle 3\rangle$ QED

BY $\langle 1\rangle$b, $\langle 2\rangle$3, $\langle 3\rangle$1 DEFS Inv, $MsgInv$, $AccInv$

$\langle 2\rangle$ QED

BY $\langle 2\rangle$2, $\langle 2\rangle$3

$\langle 1\rangle$2. $\forall\, a \in Participant :$

$\forall\, q \in Participant : state'[a][q].maxVBal \leq state'[a][q].maxBal$

$\langle 2\rangle$ SUFFICES ASSUME NEW $a \in Participant$, NEW $q \in Participant$

PROVE $state'[a][q].maxVBal \leq state'[a][q].maxBal$

OBVIOUS

$\langle 2\rangle$1.CASE $a \neq qq$

BY $\langle 2\rangle$1 DEFS $UpdateState$, Inv, $AccInv$

$\langle 2\rangle$2.CASE $a = qq$

$\langle 3\rangle$1.CASE $q = mm.from$

BY $\langle 1\rangle$g, $\langle 2\rangle$2, $\langle 3\rangle$1

$\langle 3\rangle$2.CASE $q = qq$

BY $\langle 1\rangle$a, $\langle 2\rangle$2, $\langle 3\rangle$2

$\langle 3\rangle 3.$CASE $q \neq mm.\mathit{from} \land q \neq qq$

$\langle 4\rangle 1. \land \mathit{state}'[a][q].\mathit{maxVBal} = \mathit{state}[a][q].\mathit{maxVBal}$

$\land \mathit{state}'[a][q].\mathit{maxBal} = \mathit{state}[a][q].\mathit{maxBal}$

BY $\langle 2\rangle 2$, $\langle 3\rangle 3$ DEFS $\mathit{UpdateState}$

$\langle 4\rangle$ QED

BY $\langle 2\rangle 2$, $\langle 3\rangle 3$, $\langle 4\rangle 1$ DEFS AccInv, Inv

$\langle 3\rangle$ QED

BY $\langle 2\rangle 2$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$

$\langle 1\rangle 3.\ \forall\, a \in \mathit{Participant} :$

$\mathit{state}'[a][a].\mathit{maxVBal} \geq 0$

$\Rightarrow \mathit{VotedForIn}(a,\ \mathit{state}[a][a].\mathit{maxVBal},\ \mathit{state}[a][a].\mathit{maxVVal})'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, $\mathit{state}'[a][a].\mathit{maxVBal} \geq 0$

PROVE $\mathit{VotedForIn}(a,\ \mathit{state}[a][a].\mathit{maxVBal},\ \mathit{state}[a][a].\mathit{maxVVal})'$

OBVIOUS

$\langle 4\rangle 1.$CASE $a = qq$

$\langle 5\rangle 1.$CASE $\land \mathit{state}'[qq][qq].\mathit{maxVBal} = \mathit{state}[qq][qq].\mathit{maxVBal}$

$\land \mathit{state}'[qq][qq].\mathit{maxVVal} = \mathit{state}[qq][qq].\mathit{maxVVal}$

$\langle 6\rangle 1.\ \mathit{VotedForIn}(a,\ \mathit{state}[a][a].\mathit{maxVBal},\ \mathit{state}[a][a].\mathit{maxVVal})$

BY $\langle 4\rangle 1$, $\langle 5\rangle 1$ DEFS AccInv, Inv

$\langle 6\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 5\rangle 1$, $\langle 6\rangle 1$ DEFS $\mathit{VotedForIn}$, $\mathit{UpdateState}$

$\langle 5\rangle 2.$CASE $\land \mathit{state}'[qq][qq].\mathit{maxVBal} = mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVBal}$

$\land mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVBal} = mm.\mathit{state}[mm.\mathit{from}].\mathit{maxBal}$

$\land \mathit{state}'[qq][qq].\mathit{maxVVal} = mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVVal}$

$\land \mathit{state}'[qq][qq].\mathit{maxBal} = mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVBal}$

$\langle 6\rangle 1.$CASE $\mathit{state}[qq][qq].\mathit{maxVBal} = mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVBal}$

$\langle 7\rangle$a. $\mathit{state}[qq][qq].\mathit{maxVBal} \geq 0 \land \mathit{state}[qq][qq].\mathit{maxVBal} \in \mathit{Ballot}$

BY $\langle 4\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle 1$

$\langle 7\rangle$b. $\mathit{VotedForIn}(mm.\mathit{from},\ mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVBal},\ mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVVal})$

BY $\langle 6\rangle 1$, $\langle 7\rangle$a DEFS MsgInv, Inv

$\langle 7\rangle$c. $\mathit{VotedForIn}(qq,\ \mathit{state}[qq][qq].\mathit{maxVBal},\ \mathit{state}[qq][qq].\mathit{maxVVal})$

BY $\langle 7\rangle$a DEFS Inv, AccInv

$\langle 7\rangle$d. $\mathit{state}[qq][qq].\mathit{maxVVal} \in \mathit{Value} \land mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVVal} \in \mathit{Value}$

BY $\langle 6\rangle 1$, $\langle 7\rangle$a DEFS Inv, AccInv, MsgInv

$\langle 7\rangle 1.\ \mathit{state}[qq][qq].\mathit{maxVVal} = mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVVal}$

BY $\langle 4\rangle 1$, $\langle 6\rangle 1$, $\langle 7\rangle$a, $\langle 7\rangle$b, $\langle 7\rangle$c, $\langle 7\rangle$d, $\mathit{VotedOnce}$DEFS Inv

$\langle 7\rangle 2.\ \mathit{VotedForIn}(qq,\ \mathit{state}'[qq][qq].\mathit{maxVBal},\ \mathit{state}'[qq][qq].\mathit{maxVVal})$

BY $\langle 5\rangle 2$, $\langle 6\rangle 1$, $\langle 7\rangle$c, $\langle 7\rangle 1$

$\langle 7\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 7\rangle 2$ DEFS $\mathit{VotedForIn}$, $\mathit{OnMessage}$

$\langle 6\rangle 2.$CASE $mm.\mathit{state}[mm.\mathit{from}].\mathit{maxVBal} \neq \mathit{state}[qq][qq].\mathit{maxVBal}$

$\langle 7\rangle$a. $\land\ mm.\mathit{state}[qq].\mathit{maxVBal} \in \mathit{AllBallot}$

$\land \mathit{state}[qq][qq].\mathit{maxVBal} \in \mathit{AllBallot}$

$\land\ mm.state[mm.from].maxVBal \in AllBallot$

$\land\ state'[qq][qq].maxVBal \in AllBallot$

BY DEFS Inv

$\langle 7\rangle$b. $mm.state[mm.from].maxVBal \geq state[qq][qq].maxVBal$

BY $\langle 1\rangle$a, $\langle 5\rangle 2$

$\langle 7\rangle$c. $mm.state[mm.from].maxVBal > state[qq][qq].maxVBal$

BY $\langle 6\rangle 2$, $\langle 7\rangle$a, $\langle 7\rangle$b

$\langle 7\rangle$d. $mm.state[qq].maxVBal \leq state[qq][qq].maxVBal$

BY DEFS Inv, $MsgInv$

$\langle 7\rangle$e. $mm.state[qq].maxVBal < state'[qq][qq].maxVBal$

BY $\langle 5\rangle 2$, $\langle 7\rangle$a, $\langle 7\rangle$c, $\langle 7\rangle$d

$\langle 7\rangle 1$. $nm \in msgs'$

BY $\langle 7\rangle$e DEFS $OnMessage$

$\langle 7\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle 2$, $\langle 7\rangle 1$ DEFS $VotedForIn$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle$ QED

BY $\langle 1\rangle$b, $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 2$.CASE $a \neq qq$

$\langle 5\rangle 2$. $VotedForIn(a,\ state[a][a].maxVBal,\ state[a][a].maxVVal)$

BY $\langle 4\rangle 2$ DEFS $UpdateState$, Inv, $AccInv$

$\langle 5\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 5\rangle 2$ DEFS $VotedForIn$, $UpdateState$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 1\rangle 4$. $\forall\, a \in Participant :$

$\land\ \forall\, c \in Ballot : c > state'[a][a].maxVBal$

$\Rightarrow \neg\exists\, v \in Value : VotedForIn(a,\ c,\ v)'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $a \in Participant$, NEW $c \in Ballot$, $c > state'[a][a].maxVBal$

PROVE $\neg\exists\, v \in Value : VotedForIn(a,\ c,\ v)'$

OBVIOUS

$\langle 2\rangle 1$. $c > state[a][a].maxVBal$

$\langle 3\rangle 1$.CASE $a = qq$

BY $\langle 1\rangle$a, $\langle 1\rangle$e, $\langle 3\rangle 1$

$\langle 3\rangle 2$.CASE $a \neq qq$

BY $\langle 3\rangle 2$ DEFS $UpdateState$

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$

$\langle 2\rangle 2$. $\neg\exists\, v \in Value : VotedForIn(a,\ c,\ v)$

BY $\langle 2\rangle 1$ DEFS $AccInv$, Inv

$\langle 2\rangle 3$.CASE $a = qq$

BY $\langle 1\rangle$b, $\langle 2\rangle 2$ DEFS $OnMessage$, $VotedForIn$

$\langle 2\rangle 4$.CASE $a \neq qq$

BY $\langle 2\rangle 2$ DEFS $OnMessage$, $VotedForIn$

```
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 3$, $\langle 2 \rangle 4$
$\langle 1 \rangle 5.\ \forall\, a \in \mathit{Participant} :$
$\forall\, q \in \mathit{Participant} :$
$\wedge\ \mathit{state}'[a][a].\mathit{maxBal} \geq \mathit{state}'[q][a].\mathit{maxBal}$
$\wedge\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}'[q][a].\mathit{maxVBal}$
$\langle 2 \rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, NEW $q \in \mathit{Participant}$
PROVE $\wedge\ \mathit{state}'[a][a].\mathit{maxBal} \geq \mathit{state}'[q][a].\mathit{maxBal}$
$\wedge\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}'[q][a].\mathit{maxVBal}$
OBVIOUS
$\langle 2 \rangle$a. $\wedge\ \mathit{state}'[a][a].\mathit{maxBal} \in \mathit{AllBallot}$
$\wedge\ \mathit{state}'[q][a].\mathit{maxBal} \in \mathit{AllBallot}$
$\wedge\ \mathit{state}'[a][a].\mathit{maxVBal} \in \mathit{AllBallot}$
$\wedge\ \mathit{state}'[q][a].\mathit{maxBal} \in \mathit{AllBallot}$
$\wedge\ \mathit{state}[a][a].\mathit{maxBal} \in \mathit{AllBallot}$
$\wedge\ \mathit{state}[a][a].\mathit{maxVBal} \in \mathit{AllBallot}$
$\wedge\ \mathit{state}[q][a].\mathit{maxBal} \in \mathit{AllBallot}$
$\wedge\ \mathit{state}[q][a].\mathit{maxVBal} \in \mathit{AllBallot}$
BY DEFS $\mathit{Inv}$
$\langle 2 \rangle$b. $\wedge\ \mathit{state}[a][a].\mathit{maxBal} \geq \mathit{state}[q][a].\mathit{maxBal}$
$\wedge\ \mathit{state}[a][a].\mathit{maxVBal} \geq \mathit{state}[q][a].\mathit{maxVBal}$
BY DEFS $\mathit{Inv}$, $\mathit{AccInv}$
$\langle 2 \rangle 1.$CASE $q = a \wedge a = qq$
BY $\langle 2 \rangle 1$, $\langle 2 \rangle$a
$\langle 2 \rangle 2.$CASE $q \neq a \wedge a = qq$
$\langle 3 \rangle 1.\ \wedge\ \mathit{state}'[q][a].\mathit{maxBal} = \mathit{state}[q][a].\mathit{maxBal}$
$\wedge\ \mathit{state}'[q][a].\mathit{maxVBal} = \mathit{state}[q][a].\mathit{maxVBal}$
BY $\langle 2 \rangle 2$ DEFS $\mathit{UpdateState}$
$\langle 3 \rangle 2.\ \wedge\ \mathit{state}'[a][a].\mathit{maxBal} \geq \mathit{state}[a][a].\mathit{maxBal}$
$\wedge\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}[a][a].\mathit{maxVBal}$
BY $\langle 2 \rangle 2$, $\langle 1 \rangle$a, $\langle 1 \rangle$f
$\langle 3 \rangle$ QED
BY $\langle 2 \rangle$a, $\langle 2 \rangle$b, $\langle 2 \rangle 2$, $\langle 3 \rangle 1$, $\langle 3 \rangle 2$
$\langle 2 \rangle 3.$CASE $q = a \wedge a \neq qq$
BY $\langle 2 \rangle 3$ DEFS $\mathit{UpdateState}$, $\mathit{Inv}$, $\mathit{AccInv}$
$\langle 2 \rangle 4.$CASE $q \neq a \wedge a \neq qq$
$\langle 3 \rangle 1.\ \wedge\ \mathit{state}'[a][a].\mathit{maxBal} = \mathit{state}[a][a].\mathit{maxBal}$
$\wedge\ \mathit{state}'[a][a].\mathit{maxVBal} = \mathit{state}[a][a].\mathit{maxVBal}$
BY $\langle 2 \rangle 4$ DEFS $\mathit{UpdateState}$
$\langle 3 \rangle 2.$CASE $q = qq \wedge a = \mathit{mm.from}$
$\langle 4 \rangle 1.\ \wedge\ \mathit{mm.state}[\mathit{mm.from}].\mathit{maxVBal} \leq \mathit{state}[a][a].\mathit{maxVBal}$
BY $\langle 3 \rangle 2$ DEFS $\mathit{Inv}$, $\mathit{MsgInv}$
$\langle 4 \rangle 2.\ \wedge\ \mathit{mm.state}[\mathit{mm.from}].\mathit{maxBal} \leq \mathit{state}[a][a].\mathit{maxBal}$
$\langle 5 \rangle 1.$CASE $\mathit{mm.state}[\mathit{mm.from}].\mathit{maxBal} \neq \mathit{mm.state}[\mathit{mm.from}].\mathit{maxVBal}$
BY $\langle 3 \rangle 2$, $\langle 5 \rangle 1$ DEFS $\mathit{Inv}$, $\mathit{MsgInv}$
```

$\langle 5\rangle 2.$CASE $mm.state[mm.from].maxBal = mm.state[mm.from].maxVBal$

$\langle 6\rangle 1.$ $mm.state[mm.from].maxBal \leq state[a][a].maxVBal$

BY $\langle 3\rangle 2$, $\langle 5\rangle 2$ DEFS Inv, $MsgInv$

$\langle 6\rangle$ QED

BY $\langle 1\rangle$e, $\langle 2\rangle$a, $\langle 6\rangle 1$ DEFS Inv, $AccInv$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 3.$ $\land\ state'[q][a].maxVBal = Max(state[qq][a].maxVBal,\ mm.state[mm.from].maxVBal)$

$\land\ state'[q][a].maxBal = Max(state[qq][a].maxBal,\ mm.state[mm.from].maxBal)$

BY $\langle 3\rangle 2$ DEFS $UpdateState$

$\langle 4\rangle 4.$ $Max(state[qq][a].maxBal,\ mm.state[mm.from].maxBal) \leq state[a][a].maxBal$

BY $\langle 1\rangle$e, $\langle 2\rangle$a, $\langle 2\rangle$b, $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEFS Max

$\langle 4\rangle 5.$ $Max(state[qq][a].maxVBal,\ mm.state[mm.from].maxVBal) \leq state[a][a].maxVBal$

BY $\langle 1\rangle$e, $\langle 2\rangle$a, $\langle 2\rangle$b, $\langle 4\rangle 1$, $\langle 3\rangle 2$ DEFS Max

$\langle 4\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$

$\langle 3\rangle 3.$CASE $\neg(q = qq \land a = mm.from)$

$\langle 4\rangle 1.$ $\land\ state'[q][a].maxBal = state[q][a].maxBal$

$\land\ state'[q][a].maxVBal = state[q][a].maxVBal$

BY $\langle 2\rangle 4$, $\langle 3\rangle 3$ DEFS $UpdateState$

$\langle 4\rangle$ QED

BY $\langle 2\rangle$a, $\langle 2\rangle$b, $\langle 3\rangle 1$, $\langle 4\rangle 1$

$\langle 3\rangle$ QED

BY $\langle 2\rangle 4$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 1\rangle 6.$ $\forall\, a \in Participant :$

$\forall\, q \in Participant :$

$state'[a][q].maxBal \in Ballot$

$\Rightarrow \exists\, m \in msgs' :$

$\land\ m.from = q$

$\land\ m.state[q].maxBal = state'[a][q].maxBal$

$\land\ m.state[q].maxVBal = state'[a][q].maxVBal$

$\land\ m.state[q].maxVVal = state'[a][q].maxVVal$

$\langle 2\rangle$ SUFFICES ASSUME NEW $a \in Participant$, NEW $q \in Participant$, $state'[a][q].maxBal \in Ballot$

PROVE $\exists\, m \in msgs' :$

$\land\ m.from = q$

$\land\ m.state[q].maxBal = state'[a][q].maxBal$

$\land\ m.state[q].maxVBal = state'[a][q].maxVBal$

$\land\ m.state[q].maxVVal = state'[a][q].maxVVal$

OBVIOUS

$\langle 2\rangle$a. $\land\ state'[a][q].maxBal \in AllBallot$

$\land\ state[a][q].maxBal \in AllBallot$

$\land\ state'[a][q].maxVBal \in AllBallot$

$\land\ state[a][q].maxVBal \in AllBallot$

BY DEFS Inv, $MsgInv$

$\langle 2\rangle 2.$CASE $a = qq$

$\langle 3\rangle 1.$CASE $mm.from = q$

BY $\langle 1\rangle$g, $\langle 2\rangle 2$, $\langle 3\rangle 1$, $SMTT(100)$DEFS $AccInv$, Inv, $OnMessage$

$\langle 3\rangle 2.$CASE $a = q$

$\langle 4\rangle$a. $state'[qq][qq].maxBal = Max(state[qq][qq].maxBal, mm.state[mm.from].maxBal)$

BY DEFS $UpdateState$

$\langle 4\rangle 1.$CASE

$\wedge\ state'[qq][qq].maxVBal = mm.state[mm.from].maxVBal$

$\wedge\ mm.state[mm.from].maxVBal = mm.state[mm.from].maxBal$

$\wedge\ state'[qq][qq].maxVVal = mm.state[mm.from].maxVVal$

$\wedge\ state'[qq][qq].maxBal = mm.state[mm.from].maxVBal$

$\langle 5\rangle 1.$ $VotedForIn(qq, mm.state[mm.from].maxVBal, mm.state[mm.from].maxVVal)'$

BY $\langle 1\rangle 3$, $\langle 4\rangle 1$ DEFS Inv, $MsgInv$

$\langle 5\rangle$ QED

BY $\langle 2\rangle 2$, $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 5\rangle 1$ DEFS $VotedForIn$

$\langle 4\rangle 2.$CASE

$\wedge\ state'[qq][qq].maxVBal = state[qq][qq].maxVBal$

$\wedge\ state'[qq][qq].maxVVal = state[qq][qq].maxVVal$

$\langle 5\rangle 1.$CASE $state'[qq][qq].maxBal = state[qq][qq].maxBal$

$\langle 6\rangle 1.$ $state[a][q].maxBal \in Ballot$

BY $\langle 2\rangle 2$, $\langle 3\rangle 2$, $\langle 4\rangle 2$, $\langle 5\rangle 1$

$\langle 6\rangle 2.$ $\exists\, m \in msgs :$

$\wedge\ m.from = q$

$\wedge\ m.state[q].maxBal = state[a][q].maxBal$

$\wedge\ m.state[q].maxVBal = state[a][q].maxVBal$

$\wedge\ m.state[q].maxVVal = state[a][q].maxVVal$

BY $\langle 6\rangle 1$ DEFS Inv, $AccInv$

$\langle 6\rangle$ QED

BY $\langle 2\rangle 2$, $\langle 3\rangle 2$, $\langle 4\rangle 2$, $\langle 5\rangle 1$, $\langle 6\rangle 2$ DEFS Inv, $AccInv$, $OnMessage$

$\langle 5\rangle 2.$CASE $state'[qq][qq].maxBal > state[qq][qq].maxBal$

$\langle 6\rangle$a. $\wedge\ state'[qq][qq].maxBal \in AllBallot$

$\wedge\ state[qq][qq].maxBal \in AllBallot$

$\wedge\ mm.state[qq].maxBal \in AllBallot$

BY DEFS Inv

$\langle 6\rangle 1.$ $mm.state[qq].maxBal \leq state[qq][qq].maxBal$

BY $\langle 2\rangle 2$, $\langle 3\rangle 2$, $\langle 4\rangle 2$, $\langle 5\rangle 2$ DEFS Inv, $MsgInv$

$\langle 6\rangle 2.$ $mm.state[qq].maxBal < state'[qq][qq].maxBal$

BY $\langle 5\rangle 2$, $\langle 6\rangle 1$, $\langle 6\rangle$a

$\langle 6\rangle 3.$ $nm \in msgs'$

BY $\langle 6\rangle 2$

$\langle 6\rangle$ QED

BY $\langle 2\rangle 2$, $\langle 3\rangle 2$, $\langle 5\rangle 2$, $\langle 6\rangle 3$

$\langle 5\rangle$ QED

BY $\langle 1\rangle$e, $\langle 1\rangle$f, $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle$ QED
BY $\langle 1\rangle$b, $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 3$.CASE $a \neq q \wedge q \neq mm.from$
$\langle 4\rangle 1$. $\wedge\ state'[a][q].maxBal = state[a][q].maxBal$
$\wedge\ state'[a][q].maxVBal = state[a][q].maxVBal$
$\wedge\ state'[a][q].maxVVal = state[a][q].maxVVal$
BY $\langle 2\rangle 2$, $\langle 3\rangle 3$, $ZenonT(100)$, $IsaT(100)$, $SMTT(100)$DEFS $UpdateState$
$\langle 4\rangle 2$. $\exists\, m \in msgs :$
$\wedge\ m.from = q$
$\wedge\ m.state[q].maxBal = state[a][q].maxBal$
$\wedge\ m.state[q].maxVBal = state[a][q].maxVBal$
$\wedge\ m.state[q].maxVVal = state[a][q].maxVVal$
BY $\langle 4\rangle 1$ DEFS Inv, $AccInv$
$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEFS $OnMessage$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$
$\langle 2\rangle 3$.CASE $a \neq qq$
$\langle 3\rangle 1$. $\wedge\ state'[a][q].maxBal = state[a][q].maxBal$
$\wedge\ state'[a][q].maxVBal = state[a][q].maxVBal$
$\wedge\ state'[a][q].maxVVal = state[a][q].maxVVal$
BY $\langle 2\rangle 3$ DEFS $UpdateState$
$\langle 3\rangle 2$. $\exists\, m \in msgs :$
$\wedge\ m.from = q$
$\wedge\ m.state[q].maxBal = state[a][q].maxBal$
$\wedge\ m.state[q].maxVBal = state[a][q].maxVBal$
$\wedge\ m.state[q].maxVVal = state[a][q].maxVVal$
BY $\langle 3\rangle 1$ DEFS Inv, $AccInv$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$ DEFS $OnMessage$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$
$\langle 1\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\langle 1\rangle 5$, $\langle 1\rangle 6$ DEFS $AccInv$

THEOREM $Invariant \triangleq Spec \Rightarrow \Box Inv$
$\langle 1\rangle$ USE DEFS $Send$, $Ballot$, $TypeOK$, $State$, $AllBallot$, $InitState$, $AllValue$, $Message$, $vars$
$\langle 1\rangle 1$. $Init \Rightarrow Inv$
BY DEFS $Init$, $AccInv$, $InitState$, $VotedForIn$, $MsgInv$, $TypeOK$, Inv
$\langle 1\rangle 2$. $Inv \wedge [Next]_{vars} \Rightarrow Inv'$
$\langle 2\rangle$ SUFFICES ASSUME Inv, $[Next]_{vars}$
PROVE Inv'
OBVIOUS
$\langle 2\rangle$ USE DEF Inv

$\langle 2 \rangle 1.$CASE $Next$

$\langle 3 \rangle 1.$ $TypeOK'$

$\langle 4 \rangle 1.$ ASSUME NEW $p \in Participant$, NEW $b \in Ballot$, $Prepare(p, b)$, Inv

PROVE $TypeOK'$

$\langle 5 \rangle 1.$ $state'[p][p].maxBal \in AllBallot$

BY $\langle 4 \rangle 1$ DEFS $Prepare$

$\langle 5 \rangle 2.$ $state'[p][p].maxVBal \in AllBallot$

BY $\langle 4 \rangle 1$ DEFS $Prepare$

$\langle 5 \rangle 3.$ $state'[p][p].maxVVal \in AllValue$

BY $\langle 4 \rangle 1$ DEFS $Prepare$

$\langle 5 \rangle 4.$ $state'[p][p] \in [maxBal : AllBallot, maxVBal : Ballot \cup \{-1\}, maxVVal : Value \cup \{None\}]$

BY $\langle 4 \rangle 1$, $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$ DEFS $Prepare$

$\langle 5 \rangle 5.$ $state' \in [Participant \rightarrow [Participant \rightarrow State]]$

BY $\langle 4 \rangle 1$, $\langle 5 \rangle 4$ DEFS $Prepare$

$\langle 5 \rangle 6.$ $[from \mapsto p, to \mapsto Participant \setminus \{p\},$
$state \mapsto (state')[p]] \in Message$

BY $\langle 5 \rangle 5$

$\langle 5 \rangle 7.$ $msgs' \subseteq Message$

BY $\langle 4 \rangle 1$, $\langle 5 \rangle 6$ DEFS $Prepare$

$\langle 5 \rangle$ QED

BY $\langle 5 \rangle 5$, $\langle 5 \rangle 7$ DEFS $Prepare$

$\langle 4 \rangle 2.$ ASSUME NEW $p \in Participant$, NEW $b \in Ballot$, NEW $v \in Value$, $Accept(p, b, v)$, Inv

PROVE $TypeOK'$

$\langle 5 \rangle 1.$ $state[p][p].maxBal \geq b$

BY $\langle 4 \rangle 2$, $QuorumAssumption$DEFS $AccInv$, $Accept$

$\langle 5 \rangle 2.$ $state[p][p].maxBal \leq b$

BY $\langle 4 \rangle 2$, $\langle 5 \rangle 1$ DEFS $Accept$

$\langle 5 \rangle 3.$ $state'[p][p].maxBal = b \land state'[p][p].maxVBal = b \land state'[p][p].maxVVal = v$

BY $\langle 4 \rangle 2$, $\langle 5 \rangle 1$, $\langle 5 \rangle 2$ DEFS $Accept$

$\langle 5 \rangle 5.$ $state' \in [Participant \rightarrow [Participant \rightarrow State]]$

BY $\langle 4 \rangle 2$, $\langle 5 \rangle 3$, $ZenonT(100)$DEFS $Accept$

$\langle 5 \rangle 6.$ $[from \mapsto p, to \mapsto Participant \setminus \{p\},$
$state \mapsto (state')[p]] \in Message$

BY $\langle 5 \rangle 5$

$\langle 5 \rangle 7.$ $msgs' \subseteq Message$

BY $\langle 4 \rangle 2$, $\langle 5 \rangle 6$ DEFS $Accept$

$\langle 5 \rangle$ QED

BY $\langle 4 \rangle 2$, $\langle 5 \rangle 6$, $\langle 5 \rangle 7$ DEFS $Accept$

$\langle 4 \rangle 3.$ ASSUME NEW $p \in Participant$, $OnMessage(p)$, Inv

PROVE $TypeOK'$

$\langle 5 \rangle 1.$ PICK $mm \in msgs : OnMessage(p)!(mm)$

BY $\langle 4 \rangle 3$ DEFS $OnMessage$

$\langle 5 \rangle 2.$ $state' \in [Participant \rightarrow [Participant \rightarrow State]]$

BY $\langle 4 \rangle 3$, $UpdateStateTypeOKProperty$DEFS $OnMessage$

$\langle 5 \rangle 3.$ $[from \mapsto p, to \mapsto \{mm.from\}, state \mapsto (state')[p]] \in Message$

```
BY $\langle 4\rangle 3$, $\langle 5\rangle 2$ DEFS $OnMessage$, $UpdateState$
$\langle 5\rangle 5.$ $msgs' \subseteq Message$
$\langle 6\rangle 1.$CASE $\lor (mm.state)[p].maxBal < (state')[p][p].maxBal$
$\lor (mm.state)[p].maxVBal < (state')[p][p].maxVBal$
BY $\langle 4\rangle 3$, $\langle 5\rangle 3$ DEFS $OnMessage$
$\langle 6\rangle 2.$CASE $\neg( \lor (mm.state)[p].maxBal < (state')[p][p].maxBal$
$\lor (mm.state)[p].maxVBal < (state')[p][p].maxVBal)$
BY $\langle 4\rangle 3$, $\langle 5\rangle 3$ DEFS $OnMessage$
$\langle 6\rangle$ QED
BY $\langle 4\rangle 3$, $\langle 6\rangle 1$, $\langle 6\rangle 2$ DEF $OnMessage$
$\langle 5\rangle$ QED
BY $\langle 4\rangle 3$, $\langle 5\rangle 2$, $\langle 5\rangle 5$ DEFS $OnMessage$
$\langle 4\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEFS $Next$
$\langle 3\rangle 2.$ $MsgInv'$
$\langle 4\rangle$ USE DEF $MsgInv$
$\langle 4\rangle 1.$ ASSUME NEW $p \in Participant$, NEW $b \in Ballot$, $Prepare(p, b)$, $Inv$
PROVE $MsgInv'$
BY $\langle 3\rangle 1$, $\langle 4\rangle 1$, $PrepareMsgInv$
$\langle 4\rangle 2.$ ASSUME NEW $p \in Participant$, NEW $b \in Ballot$, NEW $v \in Value$, $Accept(p, b, v)$, $Inv$
PROVE $MsgInv'$
BY $\langle 3\rangle 1$, $\langle 4\rangle 2$, $AcceptMsgInv$
$\langle 4\rangle 3.$ ASSUME NEW $p \in Participant$, $OnMessage(p)$, $Inv$
PROVE $MsgInv'$
BY $\langle 3\rangle 1$, $\langle 4\rangle 3$, $OnMessageMsgInv$
$\langle 4\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEFS $Next$
$\langle 3\rangle 3.$ $AccInv'$
$\langle 4\rangle 1.$ ASSUME NEW $p \in Participant$, NEW $b \in Ballot$, $Prepare(p, b)$, $Inv$
PROVE $AccInv'$
$\langle 5\rangle$ DEFINE $nm \triangleq [from \mapsto p, to \mapsto Participant \setminus \{p\},$
$state \mapsto (state')[p]]$
$\langle 5\rangle a.$ $\forall a \in Participant :$
$state[a][a].maxVBal = state'[a][a].maxVBal$
BY $\langle 4\rangle 1$ DEFS $Prepare$
$\langle 5\rangle b.$ $nm.state[p].maxBal \neq nm.state[p].maxVBal$
BY $\langle 4\rangle 1$ DEFS $Prepare$, $AccInv$
$\langle 5\rangle 1.$ $\forall a \in Participant :$
$\land state'[a][a].maxVBal = -1 \equiv state'[a][a].maxVVal = None$
$\land \forall q \in Participant : state'[a][q].maxVBal \leq state'[a][q].maxBal$
BY $\langle 4\rangle 1$ DEFS $Prepare$, $AccInv$
$\langle 5\rangle 3.$ $\forall a \in Participant :$
$state'[a][a].maxVBal \geq 0$
$\Rightarrow VotedForIn(a, state[a][a].maxVBal, state[a][a].maxVVal)'$
BY $\langle 5\rangle a$, $\langle 4\rangle 1$ DEFS $VotedForIn$, $Prepare$, $AccInv$
```

$\langle 5\rangle 4.\ \forall\, a \in \mathit{Participant} :$

$\land\ \forall\, c \in \mathit{Ballot} : c > \mathit{state}'[a][a].\mathit{maxVBal}$

$\Rightarrow \neg\exists\, v \in \mathit{Value} : \mathit{VotedForIn}(a,\, c,\, v)'$

$\langle 6\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, NEW $c \in \mathit{Ballot},\ c > \mathit{state}'[a][a].\mathit{maxVBal}$

PROVE $\neg\exists\, v \in \mathit{Value} : \mathit{VotedForIn}(a,\, c,\, v)'$

OBVIOUS

$\langle 6\rangle 1.\ \neg\exists\, v \in \mathit{Value} : \mathit{VotedForIn}(a,\, c,\, v)$

BY $\langle 5\rangle$a DEFS AccInv

$\langle 6\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 5\rangle$a, $\langle 5\rangle$b, $\langle 6\rangle 1$ DEFS $\mathit{VotedForIn}$, $\mathit{Prepare}$

$\langle 5\rangle 5.\ \forall\, a \in \mathit{Participant} :$

$\forall\, q \in \mathit{Participant} :$

$\land\ \mathit{state}'[a][a].\mathit{maxBal} \geq \mathit{state}'[q][a].\mathit{maxBal}$

$\land\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}'[q][a].\mathit{maxVBal}$

$\langle 6\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, NEW $q \in \mathit{Participant}$

PROVE $\land\ \mathit{state}'[a][a].\mathit{maxBal} \geq \mathit{state}'[q][a].\mathit{maxBal}$

$\land\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}'[q][a].\mathit{maxVBal}$

OBVIOUS

$\langle 6\rangle 1.$CASE $a \neq p$

BY $\langle 4\rangle 1$, $\langle 6\rangle 1$ DEFS $\mathit{Prepare}$, AccInv, $\mathit{VotedForIn}$

$\langle 6\rangle 2.$CASE $a = p$

BY $\langle 4\rangle 1$, $\langle 5\rangle$a, $\langle 6\rangle 2$ DEFS $\mathit{Prepare}$, AccInv, $\mathit{VotedForIn}$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle 6.\ \forall\, a \in \mathit{Participant} :$

$\forall\, q \in \mathit{Participant} :$

$\mathit{state}'[a][q].\mathit{maxBal} \in \mathit{Ballot}$

$\Rightarrow \exists\, m \in \mathit{msgs}' :$

$\land\ m.\mathit{from} = q$

$\land\ m.\mathit{state}[q].\mathit{maxBal} = \mathit{state}'[a][q].\mathit{maxBal}$

$\land\ m.\mathit{state}[q].\mathit{maxVBal} = \mathit{state}'[a][q].\mathit{maxVBal}$

$\land\ m.\mathit{state}[q].\mathit{maxVVal} = \mathit{state}'[a][q].\mathit{maxVVal}$

$\langle 6\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, NEW $q \in \mathit{Participant}$, $\mathit{state}'[a][q].\mathit{maxBal} \in \mathit{Ballot}$

PROVE $\exists\, m \in \mathit{msgs}' :$

$\land\ m.\mathit{from} = q$

$\land\ m.\mathit{state}[q].\mathit{maxBal} = \mathit{state}'[a][q].\mathit{maxBal}$

$\land\ m.\mathit{state}[q].\mathit{maxVBal} = \mathit{state}'[a][q].\mathit{maxVBal}$

$\land\ m.\mathit{state}[q].\mathit{maxVVal} = \mathit{state}'[a][q].\mathit{maxVVal}$

OBVIOUS

$\langle 6\rangle 1.$CASE $(a = q \land a = p)$

BY $\langle 4\rangle 1$, $\langle 6\rangle 1$, $\mathit{IsaT}(100)$DEFS $\mathit{Prepare}$

$\langle 6\rangle 2.$CASE $\neg(a = q \land a = p)$

$\langle 7\rangle 1.\ \land\ \mathit{state}'[a][q].\mathit{maxBal} = \mathit{state}[a][q].\mathit{maxBal}$

$\land\ \mathit{state}'[a][q].\mathit{maxVBal} = \mathit{state}[a][q].\mathit{maxVBal}$

$\land\ \mathit{state}'[a][q].\mathit{maxVVal} = \mathit{state}[a][q].\mathit{maxVVal}$

BY $\langle 4\rangle 1$, $\langle 6\rangle 2$ DEFS $\mathit{Prepare}$

$\langle 7\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 6\rangle 2$, $\langle 7\rangle 1$ DEFS AccInv, $\mathit{Prepare}$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 3$, $\langle 5\rangle 4$, $\langle 5\rangle 5$, $\langle 5\rangle 6$ DEFS AccInv

$\langle 4\rangle 2$. ASSUME NEW $p \in \mathit{Participant}$, NEW $b \in \mathit{Ballot}$, NEW $v \in \mathit{Value}$, $\mathit{Accept}(p, b, v)$, Inv

PROVE AccInv'

$\langle 5\rangle$ DEFINE $\mathit{nm} \triangleq [\mathit{from} \mapsto p, \mathit{to} \mapsto \mathit{Participant} \setminus \{p\}, \mathit{state} \mapsto \mathit{state}'[p]]$

$\langle 5\rangle$a. $\mathit{nm}.\mathit{state}[p].\mathit{maxBal} = \mathit{nm}.\mathit{state}[p].\mathit{maxVBal}$

BY $\langle 4\rangle 2$ DEFS Accept

$\langle 5\rangle$b. $\mathit{state}'[p][p].\mathit{maxVBal} \geq \mathit{state}[p][p].\mathit{maxVBal}$

BY $\langle 4\rangle 2$ DEFS Accept, AccInv

$\langle 5\rangle 1$. $\mathit{state}'[p][p].\mathit{maxBal} = \mathit{state}'[p][p].\mathit{maxVBal} \land \mathit{state}'[p][p].\mathit{maxBal} = \mathit{state}[p][p].\mathit{maxBal}$

BY $\langle 4\rangle 2$ DEFS Accept

$\langle 5\rangle 2$. $\mathit{state}'[p][p].\mathit{maxVBal} \in \mathit{Ballot} \land \mathit{state}'[p][p].\mathit{maxVVal} \in \mathit{Value}$

BY $\langle 4\rangle 2$ DEFS Accept

$\langle 5\rangle 3$. $\mathit{VotedForIn}(p, \mathit{state}[p][p].\mathit{maxVBal}, \mathit{state}[p][p].\mathit{maxVVal})'$

BY $\langle 4\rangle 2$, $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\mathit{IsaT}(100)$DEFS Accept, $\mathit{VotedForIn}$

$\langle 5\rangle 4$. $\forall a \in \mathit{Participant}$:

$\land\, \mathit{state}'[a][a].\mathit{maxVBal} = -1 \equiv \mathit{state}'[a][a].\mathit{maxVVal} = \mathit{None}$

$\land\, \forall q \in \mathit{Participant} : \mathit{state}'[a][q].\mathit{maxVBal} \leq \mathit{state}'[a][q].\mathit{maxBal}$

BY $\langle 4\rangle 2$, $\langle 5\rangle 2$, $\mathit{NoneNotAValue}$DEFS AccInv, Accept

$\langle 5\rangle 5$. $\forall a \in \mathit{Participant}$:

$\mathit{state}'[a][a].\mathit{maxVBal} \geq 0$

$\Rightarrow \mathit{VotedForIn}(a, \mathit{state}[a][a].\mathit{maxVBal}, \mathit{state}[a][a].\mathit{maxVVal})'$

$\langle 6\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, $\mathit{state}'[a][a].\mathit{maxVBal} \geq 0$

PROVE $\mathit{VotedForIn}(a, \mathit{state}[a][a].\mathit{maxVBal}, \mathit{state}[a][a].\mathit{maxVVal})'$

OBVIOUS

$\langle 6\rangle 1$.CASE $a \neq p$

BY $\langle 4\rangle 2$, $\langle 6\rangle 1$ DEFS Accept, AccInv, $\mathit{VotedForIn}$

$\langle 6\rangle 2$.CASE $a = p$

BY $\langle 4\rangle 2$, $\langle 5\rangle 3$, $\langle 6\rangle 2$, $\mathit{IsaT}(100)$DEFS Accept, AccInv, $\mathit{VotedForIn}$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle 6$. $\forall a \in \mathit{Participant}$:

$\land\, \forall c \in \mathit{Ballot} : c > \mathit{state}'[a][a].\mathit{maxVBal}$

$\Rightarrow \neg\exists \mathit{vv} \in \mathit{Value} : \mathit{VotedForIn}(a, c, \mathit{vv})'$

$\langle 6\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, NEW $c \in \mathit{Ballot}$, $c > \mathit{state}'[a][a].\mathit{maxVBal}$

PROVE $\neg\exists \mathit{vv} \in \mathit{Value} : \mathit{VotedForIn}(a, c, \mathit{vv})'$

OBVIOUS

$\langle 6\rangle 1$. $c > \mathit{state}[a][a].\mathit{maxVBal}$

$\langle 7\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 5\rangle$b DEFS Accept

$\langle 6\rangle 2.\ \neg\exists\, vv \in \mathit{Value} : \mathit{VotedForIn}(a,\ c,\ vv)$
BY $\langle 6\rangle 1$ DEFS AccInv
$\langle 6\rangle$ QED
BY $\langle 4\rangle 2$, $\langle 5\rangle 3$, $\langle 6\rangle 2$ DEFS Accept, $\mathit{VotedForIn}$
$\langle 5\rangle 7.\ \forall\, a \in \mathit{Participant} :$
$\forall\, q \in \mathit{Participant} :$
$\land\ \mathit{state}'[a][a].\mathit{maxBal} \geq \mathit{state}'[q][a].\mathit{maxBal}$
$\land\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}'[q][a].\mathit{maxVBal}$
$\langle 6\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, NEW $q \in \mathit{Participant}$
PROVE $\land\ \mathit{state}'[a][a].\mathit{maxBal} \geq \mathit{state}'[q][a].\mathit{maxBal}$
$\land\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}'[q][a].\mathit{maxVBal}$
OBVIOUS
$\langle 6\rangle 1.$CASE $\neg(q \neq a \land a = p)$
BY $\langle 4\rangle 2$, $\langle 6\rangle 1$ DEFS Accept, AccInv
$\langle 6\rangle 2.$CASE $q \neq a \land a = p$
$\langle 7\rangle 1.\ \land\ \mathit{state}'[q][a].\mathit{maxBal} = \mathit{state}[q][a].\mathit{maxBal}$
$\land\ \mathit{state}'[q][a].\mathit{maxVBal} = \mathit{state}[q][a].\mathit{maxVBal}$
$\land\ \mathit{state}'[a][a].\mathit{maxBal} = \mathit{state}[a][a].\mathit{maxBal}$
$\land\ \mathit{state}'[a][a].\mathit{maxVBal} \geq \mathit{state}[a][a].\mathit{maxVBal}$
BY $\langle 4\rangle 2$, $\langle 5\rangle$b, $\langle 6\rangle 2$ DEFS Accept
$\langle 7\rangle 2.\ \land\ \mathit{state}'[a][a].\mathit{maxVBal} \in \mathit{AllBallot} \land \mathit{state}[q][a].\mathit{maxVBal} \in \mathit{AllBallot}$
$\land\ \mathit{state}'[a][a].\mathit{maxBal} \in \mathit{AllBallot} \land \mathit{state}[q][a].\mathit{maxBal} \in \mathit{AllBallot}$
BY $\langle 3\rangle 1$
$\langle 7\rangle$ QED
BY $\langle 4\rangle 2$, $\langle 6\rangle 2$, $\langle 7\rangle 1$, $\langle 7\rangle 2$ DEFS Accept, AccInv
$\langle 6\rangle$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$
$\langle 5\rangle 8.\ \forall\, a \in \mathit{Participant} :$
$\forall\, q \in \mathit{Participant} :$
$\mathit{state}'[a][q].\mathit{maxBal} \in \mathit{Ballot}$
$\Rightarrow \exists\, m \in \mathit{msgs}' :$
$\land\ m.\mathit{from} = q$
$\land\ m.\mathit{state}[q].\mathit{maxBal} = \mathit{state}'[a][q].\mathit{maxBal}$
$\land\ m.\mathit{state}[q].\mathit{maxVBal} = \mathit{state}'[a][q].\mathit{maxVBal}$
$\land\ m.\mathit{state}[q].\mathit{maxVVal} = \mathit{state}'[a][q].\mathit{maxVVal}$
$\langle 6\rangle$ SUFFICES ASSUME NEW $a \in \mathit{Participant}$, NEW $q \in \mathit{Participant}$, $\mathit{state}'[a][q].\mathit{maxBal} \in \mathit{Ballot}$
PROVE $\exists\, m \in \mathit{msgs}' :$
$\land\ m.\mathit{from} = q$
$\land\ m.\mathit{state}[q].\mathit{maxBal} = \mathit{state}'[a][q].\mathit{maxBal}$
$\land\ m.\mathit{state}[q].\mathit{maxVBal} = \mathit{state}'[a][q].\mathit{maxVBal}$
$\land\ m.\mathit{state}[q].\mathit{maxVVal} = \mathit{state}'[a][q].\mathit{maxVVal}$
OBVIOUS
$\langle 6\rangle 1.$CASE $(a = q \land a = p)$
BY $\langle 4\rangle 2$, $\langle 6\rangle 1$, $\mathit{IsaT}(100)$DEFS Accept
$\langle 6\rangle 2.$CASE $\neg(a = q \land a = p)$

```
$\langle 7 \rangle 1.\ \land\ state'[a][q].maxBal = state[a][q].maxBal$
$\land\ state'[a][q].maxVBal = state[a][q].maxVBal$
$\land\ state'[a][q].maxVVal = state[a][q].maxVVal$
BY $\langle 4 \rangle 2$, $\langle 6 \rangle 2$ DEFS $Accept$
$\langle 7 \rangle$ QED
BY $\langle 4 \rangle 2$, $\langle 6 \rangle 2$, $\langle 7 \rangle 1$ DEFS $AccInv$, $Accept$
$\langle 6 \rangle$ QED
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$
$\langle 5 \rangle$ QED
BY $\langle 5 \rangle 4$, $\langle 5 \rangle 5$, $\langle 5 \rangle 6$, $\langle 5 \rangle 7$, $\langle 5 \rangle 8$ DEFS $AccInv$
$\langle 4 \rangle 3.$ ASSUME NEW $p \in Participant$, $OnMessage(p)$, $Inv$
PROVE $AccInv'$
BY $\langle 4 \rangle 3$, $\langle 3 \rangle 1$, $OnMessageAccInv$
$\langle 4 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEFS $Next$
$\langle 3 \rangle$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$ DEFS $Inv$
$\langle 2 \rangle 2.$CASE UNCHANGED $vars$
BY $\langle 2 \rangle 2$ DEFS $AccInv$, $MsgInv$, $TypeOK$, $VotedForIn$, $Next$,
$SafeAt$, $WontVoteIn$, $VotedForIn$
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $PTL$DEFS $Spec$
```

```
THEOREM $Consistent \triangleq Spec \Rightarrow \Box Consistency$
$\langle 1 \rangle$ USE DEF $Ballot$
$\langle 1 \rangle 1.\ Inv \Rightarrow Consistency$
$\langle 2 \rangle$ SUFFICES ASSUME $Inv$,
NEW $b1 \in Ballot$, NEW $b2 \in Ballot$,
NEW $v1 \in Value$, NEW $v2 \in Value$,
$ChosenIn(b1, v1)$, $ChosenIn(b2, v2)$,
$b1 \leq b2$
PROVE $v1 = v2$
BY DEFS $Chosen$, $Consistency$
$\langle 2 \rangle 1.$CASE $b1 = b2$
BY $\langle 2 \rangle 1$, $VotedOnce$, $QuorumAssumption$DEFS $Inv$, $ChosenIn$
$\langle 2 \rangle 2.$CASE $b1 < b2$
$\langle 3 \rangle 1.\ SafeAt(b2, v2)$
BY $VotedInv$, $QuorumAssumption$DEFS $ChosenIn$, $Inv$
$\langle 3 \rangle 2.$ PICK $Q2 \in Quorum :$
$\forall a \in Q2 : VotedForIn(a, b1, v2) \lor WontVoteIn(a, b1)$
BY $\langle 2 \rangle 2$, $\langle 3 \rangle 1$ DEFS $SafeAt$
$\langle 3 \rangle 3.$ PICK $Q1 \in Quorum :$
```

$\forall\, a \in Q1 : \mathit{VotedForIn}(a,\ b1,\ v1)$
BY DEF $\mathit{ChosenIn}$
$\langle 3\rangle 4.$ QED
BY $\langle 3\rangle 3,\ \langle 3\rangle 2,\ \mathit{QuorumAssumption},\ \mathit{VotedOnce}$DEFS $\mathit{WontVoteIn},\ \mathit{Inv}$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1,\ \langle 2\rangle 2$
$\langle 1\rangle 2.$ QED
BY $\mathit{Invariant},\ \mathit{PTL},\ \langle 1\rangle 1$

$\mathit{LConstrain} \ \triangleq\ \land\, \exists\, p \in \mathit{Participant} :$
$\land\, \mathit{MaxBallot} \in \mathit{Bals}(p)$
$\land\, \mathrm{WF}_{\mathit{vars}}(\mathit{Prepare}(p,\ \mathit{MaxBallot}))$
$\land\, \forall\, v \in \mathit{Value} : \mathrm{WF}_{\mathit{vars}}(\mathit{Accept}(p,\ \mathit{MaxBallot},\ v))$
$\land\, \exists\, Q \in \mathit{Quorum} :$
$\land\, p \in Q$
$\land\, \forall\, q \in Q : \mathrm{WF}_{\mathit{vars}}(\mathit{OnMessage}(q))$

$\mathit{LSpec} \ \triangleq\ \mathit{Spec} \land \mathit{LConstrain}$

$\mathit{Liveness} \ \triangleq\ \Diamond(\mathit{chosen} \neq \{\})$