

2 |----- MODULE *BPConProof* -----|

This module specifies a *Byzantine Paxos* algorithm—a version of *Paxos* in which failed acceptors and leaders can be malicious. It is an abstraction and generalization of the Castro-Liskov algorithm in

author = “Miguel *Castro* and *Barbara Liskov*”, title = “Practical byzantine fault tolerance and proactive recovery”,
journal = *ACM Transactions on Computer Systems*,
volume = 20,
number = 4, year = 2002, pages = “398–461”

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

19 |-----|

We need the following trivial axioms and theorem about finite sets.

23 AXIOM *EmptySetFinite* \triangleq *IsFiniteSet*($\{\}$)

25 AXIOM *SingletonSetFinite* \triangleq $\forall e : \text{IsFiniteSet}(\{e\})$

27 AXIOM *ImageOfFiniteSetFinite* \triangleq
28 $\forall S, f : \text{IsFiniteSet}(S) \Rightarrow \text{IsFiniteSet}(\{f[x] : x \in S\})$

30 AXIOM *SubsetOfFiniteSetFinite* \triangleq
31 $\forall S, T : \text{IsFiniteSet}(T) \wedge (S \subseteq T) \Rightarrow \text{IsFiniteSet}(S)$

33 AXIOM *UnionOfFiniteSetsFinite* \triangleq
34 $\forall S, T : \text{IsFiniteSet}(T) \wedge \text{IsFiniteSet}(S) \Rightarrow \text{IsFiniteSet}(S \cup T)$

36 THEOREM *OnePlusFinite* \triangleq $\forall S, e : \text{IsFiniteSet}(S) \Rightarrow \text{IsFiniteSet}(S \cup \{e\})$

37 BY *SingletonSetFinite*, *UnionOfFiniteSetsFinite*

Testing that the following formula is true provides a check for typos in the axioms above.

43 *TestAxioms* \triangleq
44 *SingletonSetFinite*
45 $\wedge \forall e \in 1 \dots 3 : \text{IsFiniteSet}(\{e\})$

47 *ImageOfFiniteSetFinite*
48 $\wedge \forall S, T \in \text{SUBSET } (1 \dots 4) : \forall f \in [S \rightarrow T] :$
49 $\text{IsFiniteSet}(S) \Rightarrow \text{IsFiniteSet}(\{f[x] : x \in S\})$

51 *SubsetOfFiniteSetFinite*
52 $\wedge \forall S, T \in \text{SUBSET } (1 \dots 4) :$
53 $\text{IsFiniteSet}(T) \wedge (S \subseteq T) \Rightarrow \text{IsFiniteSet}(S)$

55 *UnionOfFiniteSetsFinite*
56 $\wedge \forall S, T \in \text{SUBSET } (1 \dots 4) :$
57 $\text{IsFiniteSet}(T) \wedge \text{IsFiniteSet}(S) \Rightarrow \text{IsFiniteSet}(S \cup T)$

58 |-----|

The sets *Value* and *Ballot* are the same as in the *Voting* and *PaxosConsensus* specs.

63 CONSTANT *Value*

65 $Ballot \triangleq Nat$

As in module *PConProof*, we define *None* to be an unspecified value that is not an element of *Value*.

71 $None \triangleq \text{CHOOSE } v : v \notin Value$

72

We pretend that which acceptors are good and which are malicious is specified in advance. Of course, the algorithm executed by the good acceptors makes no use of which acceptors are which. Hence, we can think of the sets of good and malicious acceptors as “prophecy constants” that are used only for showing that the algorithm implements the *AbstratPaxosConsensus* spec.

We can assume that a maximal set of acceptors are bad, since a bad acceptor is allowed to do anything—including acting like a good one.

The basic idea is that the good acceptors try to execute the *Paxos* consensus algorithm, while the bad acceptors may try to prevent them.

We do not distinguish between faulty and non-faulty leaders. Safety must be preserved even if all leaders are malicious, so we allow any leader to send any syntactically correct message at any time. (In an implementation, syntactically incorrect messages are simply ignored by non-faulty acceptors and have no effect.) Assumptions about leader behavior are required only for liveness.

94 CONSTANTS *Acceptor*, The set of good (non-faulty) acceptors.

95 *FakeAcceptor*, The set of possibly malicious (faulty) acceptors.

96 *ByzQuorum*,

A *Byzantine* quorum is set of acceptors that includes a quorum of good ones. In the case that there are $2f + 1$ good acceptors and f bad ones, a *Byzantine* quorum is any set of $2f + 1$ acceptors.

103 *WeakQuorum*

A weak quorum is a set of acceptors that includes at least one good one. If there are f bad acceptors, then a weak quorum is any set of $f + 1$ acceptors.

We define *ByzAcceptor* to be the set of all real or fake acceptors.

113 $ByzAcceptor \triangleq Acceptor \cup FakeAcceptor$

As in the *Paxos* consensus algorithm, we assume that the set of ballot numbers and -1 is disjoint from the set of all (real and fake) acceptors.

120 ASSUME $BallotAssump \triangleq (Ballot \cup \{-1\}) \cap ByzAcceptor = \{\}$

The following are the assumptions about acceptors and quorums that are needed to ensure safety of our algorithm.

126 ASSUME $BQA \triangleq$

127 $\wedge Acceptor \cap FakeAcceptor = \{\}$

128 $\wedge \forall Q \in ByzQuorum : Q \subseteq ByzAcceptor$

129 $\wedge \forall Q1, Q2 \in ByzQuorum : Q1 \cap Q2 \cap Acceptor \neq \{\}$

130 $\wedge \forall Q \in WeakQuorum : \wedge Q \subseteq ByzAcceptor$

131 $\wedge Q \cap Acceptor \neq \{\}$

The following assumption is not needed for safety, but it will be needed to ensure liveness.

137 ASSUME $BQLA \triangleq$
138 $\wedge \exists Q \in ByzQuorum : Q \subseteq Acceptor$
139 $\wedge \exists Q \in WeakQuorum : Q \subseteq Acceptor$
140

We now define the set $BMessage$ of all possible messages.

144 $1aMessage \triangleq [type : \{“1a”\}, bal : Ballot]$
Type 1a messages are the same as in module $PConProof$.

149 $1bMessage \triangleq$
A 1b message serves the same function as a 1b message in ordinary Paxos, where the $mbal$ and $mval$ components correspond to the $mbal$ and $mval$ components in the 1b messages of $PConProof$. The $m2av$ component is set containing all records with val and bal components equal to the corresponding components of a 2av message that the acceptor has sent, except containing for each val only the record corresponding to the 2av message with the highest bal component.

159 $[type : \{“1b”\}, bal : Ballot,$
160 $mbal : Ballot \cup \{-1\}, mval : Value \cup \{None\},$
161 $m2av : SUBSET [val : Value, bal : Ballot],$
162 $acc : ByzAcceptor]$

164 $1cMessage \triangleq$
Type 1c messages are the same as in $PConProof$.

168 $[type : \{“1c”\}, bal : Ballot, val : Value]$

170 $2avMessage \triangleq$
When an acceptor receives a 1c message, it relays that message's contents to the other acceptors in a 2av message. It does this only for the first 1c message it receives for that ballot; it can receive a second 1c message only if the leader is malicious, in which case it ignores that second 1c message.

178 $[type : \{“2av”\}, bal : Ballot, val : Value, acc : ByzAcceptor]$

180 $2bMessage \triangleq [type : \{“2b”\}, acc : ByzAcceptor, bal : Ballot, val : Value]$
2b messages are the same as in ordinary Paxos.

185 $BMessage \triangleq$
186 $1aMessage \cup 1bMessage \cup 1cMessage \cup 2avMessage \cup 2bMessage$

We will need the following simple fact about these sets of messages.

191 LEMMA $BMessageLemma \triangleq$
192 $\forall m \in BMessage :$
193 $\wedge (m \in 1aMessage) \equiv (m.type = “1a”)$
194 $\wedge (m \in 1bMessage) \equiv (m.type = “1b”)$
195 $\wedge (m \in 1cMessage) \equiv (m.type = “1c”)$
196 $\wedge (m \in 2avMessage) \equiv (m.type = “2av”)$
197 $\wedge (m \in 2bMessage) \equiv (m.type = “2b”)$
198 $\langle 1 \rangle 1. \wedge \forall m \in 1aMessage : m.type = “1a”$
199 $\wedge \forall m \in 1bMessage : m.type = “1b”$

```

200       $\wedge \forall m \in 1cMessage : m.type = "1c"$ 
201       $\wedge \forall m \in 2avMessage : m.type = "2av"$ 
202       $\wedge \forall m \in 2bMessage : m.type = "2b"$ 
203  BY DEF 1aMessage, 1bMessage, 1cMessage, 2avMessage, 2bMessage
204   $\langle 1 \rangle 2$ . QED
205  BY  $\langle 1 \rangle 1$  DEF BMessage
206 |-----|

```

We now give the algorithm. The basic idea is that the set *Acceptor* of real acceptors emulate an execution of the *PaxosConsensus* algorithm with *Acceptor* as its set of acceptors. Of course, they must do that without knowing which of the other processes in *ByzAcceptor* are real acceptors and which are fake acceptors. In addition, they don't know whether a leader is behaving according to the *PaxosConsensus* algorithm or if it is malicious.

The main idea of the algorithm is that, before performing an action of the *PaxosConsensus* algorithm, a good acceptor determines that this action is actually enabled in that algorithm. Since an action is enabled by the receipt of one or more messages, the acceptor has to determine that the enabling messages are legal *PaxosConsensus* messages. Because *PaxosConsensus* allows a 1a message to be sent at any time, the only acceptor action whose enabling messages must be checked is the *Phase2b* action. It is enabled iff the appropriate 1c message and 2a message are legal. The 1c message is legal iff the leader has received the necessary 1b messages. The acceptor therefore maintains a set of 1b messages that it knows have been sent, and checks that those 1b messages enable the sending of the 1c message.

A 2a message is legal in the *PaxosConsensus* algorithm iff (i) the corresponding 1c message is legal and (ii) it is the only 2a message that the leader sends. In the *BPCon* algorithm, there are no explicit 2a messages. They are implicitly sent by the acceptors when they send enough 2av messages.

We leave unspecified how an acceptor discovers what 1b messages have been sent. In the Castro-Liskov algorithm, this is done by having acceptors relay messages sent by other acceptors. An acceptor knows that a 1b message has been sent if it receives it directly or else receives a copy from a weak *Byzantine* quorum of acceptors. A (non-malicious) leader must determine what 1b messages acceptors know about so it chooses a value so that a quorum of acceptors will act on its *Phase1c* message and cause that value to be chosen. However, this is necessary only for liveness, so we ignore this for now.

In other implementations of our algorithm, the leader sends along with the 1c message a proof that the necessary 1b messages have been sent. The easiest way to do this is to have acceptors digitally sign their 1b messages, so a copy of the message proves that it has been sent (by the acceptor indicated in the message's *acc* field). The necessary proofs can also be constructed using only message authenticators (like the ones used in the Castro-Liskov algorithm); how this is done is described elsewhere.

In the abstract algorithm presented here, which we call *BPCon*, we do not specify how acceptors learn what 1b messages have been sent. We simply introduce a variable *knowsSent* such that *knowsSent[a]* represents the set of 1b messages that (good) acceptor *a* knows have been sent, and have an action that nondeterministically adds sent 1b messages to this set.

263 --algorithm *BPCon*{

The variables:

maxBal[a] = Highest ballot in which acceptor *a* has participated.

$maxVVal[a]$ = Highest ballot in which acceptor a has cast a vote (sent a $2b$ message); or -1 if it hasn't cast a vote.
 $maxVVal[a]$ = *Value* acceptor a has voted for in ballot $maxVVal[a]$, or *None* if $maxVVal[a] = -1$.
 $2avSent[a]$ = A set of records in $[val : Value, bal : Ballot]$ describing the $2av$ messages that a has sent. A record is added to this set, and any element with a the same val field (and lower bal field) removed when a sends a $2av$ message.
 $knownSent[a]$ = The set of $1b$ messages that acceptor a knows have been sent.
 $bmsgs$ = The set of all messages that have been sent. See the discussion of the $msgs$ variable in module *PConProof* to understand our modeling of message passing.

```

288 variables  $maxBal$    =  $[a \in \text{Acceptor} \mapsto -1]$ ,
289            $maxVVal$  =  $[a \in \text{Acceptor} \mapsto -1]$ ,
290            $maxVVal$  =  $[a \in \text{Acceptor} \mapsto \text{None}]$ ,
291            $2avSent$   =  $[a \in \text{Acceptor} \mapsto \{\}]$ ,
292            $knownSent$  =  $[a \in \text{Acceptor} \mapsto \{\}]$ ,
293            $bmsgs$  =  $\{\}$ 
294 define {
295    $sentMsgs(type, bal) \triangleq \{m \in bmsgs : m.type = type \wedge m.bal = bal\}$ 
296
297    $KnowsSafeAt(ac, b, v) \triangleq$ 
    True for an acceptor  $ac$ , ballot  $b$ , and value  $v$  iff the set of  $1b$  messages in  $knownSent[ac]$ 
    implies that value  $v$  is safe at ballot  $b$  in the PaxosConsensus algorithm being emulated
    by the good acceptors. To understand the definition, see the definition of ShowsSafeAt in
    module PConProof and recall (a) the meaning of the  $mCBal$  and  $mCVal$  fields of a  $1b$ 
    message and (b) that the set of real acceptors in a ByzQuorum forms a quorum of the
    PaxosConsensus algorithm.
    LET  $S \triangleq \{m \in knownSent[ac] : m.bal = b\}$ 
    IN    $\forall \exists BQ \in ByzQuorum :$ 
         $\forall a \in BQ : \exists m \in S : \wedge m.acc = a$ 
         $\wedge m.mbal = -1$ 
         $\vee \exists c \in 0 .. (b-1) :$ 
         $\wedge \exists BQ \in ByzQuorum :$ 
         $\forall a \in BQ : \exists m \in S : \wedge m.acc = a$ 
         $\wedge m.mbal \leq c$ 
         $\wedge (m.mbal = c) \Rightarrow (m.mval = v)$ 
         $\wedge \exists WQ \in WeakQuorum :$ 
         $\forall a \in WQ :$ 
         $\exists m \in S : \wedge m.acc = a$ 
         $\wedge \exists r \in m.m2av : \wedge r.bal \geq c$ 
         $\wedge r.val = v$ 
    }
  
```

We now describe the processes' actions as macros.

389

}

Acceptor *self* can send a phase 2*b* message with value *v* if it has received phase 2*av* messages from a *Byzantine* quorum, which implies that a quorum of good acceptors assert that this is the first 1*c* message sent by the leader and that the leader was allowed to send that message. It sets *maxBal*[*self*], *maxVBal*[*self*], and *maxVVal*[*self*] as in the non-Byzantine algorithm.

399

macro *Phase2b*(*b*){

400

when *maxBal*[*self*] ≤ *b* ;

401

with (*v* ∈ {*vv* ∈ *Value* :

402

 ∃ *Q* ∈ *ByzQuorum* :

403

 ∀ *aa* ∈ *Q* :

404

 ∃ *m* ∈ *sentMsgs*("2*av*", *b*) : ∧ *m.val* = *vv*

405

 ∧ *m.acc* = *aa*)}{

406

bmsgs := *bmsgs* ∪

407

 {[*type* ↦ "2*b*", *acc* ↦ *self*, *bal* ↦ *b*, *val* ↦ *v*]} ;

408

maxVVal[*self*] := *v* ;

409

};

410

maxBal[*self*] := *b* ;

411

maxVBal[*self*] := *b*

412

}

At any time, an acceptor can learn that some set of 1*b* messages were sent (but only if they actually were sent).

418

macro *LearnsSent*(*b*){

419

with (*S* ∈ SUBSET *sentMsgs*("1*b*", *b*)){

420

knowsSent[*self*] := *knowsSent*[*self*] ∪ *S*

421

}

422

}

A malicious acceptor *self* can send any acceptor message indicating that it is from itself. Since a malicious acceptor could allow other malicious processes to forge its messages, this action could represent the sending of the message by any malicious process.

429

macro *FakingAcceptor*() {

430

with (*m* ∈ {*mm* ∈ 1*bMessage* ∪ 2*avMessage* ∪ 2*bMessage* :

431

mm.acc = *self*}){

432

bmsgs := *bmsgs* ∪ {*m*}

433

}

434

}

We combine these individual actions into a complete algorithm in the usual way, with separate process declarations for the acceptor, leader, and fake acceptor processes.

441

process (*acceptor* ∈ *Acceptor*){

442

acc: **while** (TRUE){

443

with (*b* ∈ *Ballot*){**either** *Phase1b*(*b*)**or** *Phase2av*(*b*)

444

or *Phase2b*(*b*)**or** *LearnsSent*(*b*)}

445

}

446

}

```

448 process (leader ∈ Ballot){
449   ldr: while (TRUE){
450     either Phase1a()or Phase1c()
451   }
452 }

454 process (facceptor ∈ FakeAcceptor){
455   facc: while (TRUE){FakingAcceptor()}
456 }
457 }

```

Below is the TLA+ translation, as produced by the translator. (Some blank lines have been removed.)

```

462 BEGIN TRANSLATION
463 VARIABLES maxBal, maxVVal, maxVVal, 2avSent, knowsSent, bmsgs

465 define statement
466 sentMsgs(type, bal)  $\triangleq$  {m ∈ bmsgs : m.type = type ∧ m.bal = bal}

468 KnowsSafeAt(ac, b, v)  $\triangleq$ 
469   LET S  $\triangleq$  {m ∈ knowsSent[ac] : m.bal = b}
470   IN   ∨ ∃ BQ ∈ ByzQuorum :
471         ∨ a ∈ BQ : ∃ m ∈ S : ∧ m.acc = a
472           ∧ m.mbal = - 1
473       ∨ ∃ c ∈ 0 .. (b - 1) :
474         ∧ ∃ BQ ∈ ByzQuorum :
475           ∨ a ∈ BQ : ∃ m ∈ S : ∧ m.acc = a
476             ∧ m.mbal ≤ c
477             ∧ (m.mbal = c) ⇒ (m.mval = v)
478         ∧ ∃ WQ ∈ WeakQuorum :
479           ∨ a ∈ WQ :
480             ∃ m ∈ S : ∧ m.acc = a
481             ∧ ∃ r ∈ m.m2av : ∧ r.bal ≥ c
482               ∧ r.val = v

484 vars  $\triangleq$  ⟨maxBal, maxVVal, maxVVal, 2avSent, knowsSent, bmsgs⟩

486 ProcSet  $\triangleq$  (Acceptor) ∪ (Ballot) ∪ (FakeAcceptor)

488 Init  $\triangleq$  Global variables
489   ∧ maxBal = [a ∈ Acceptor ↦ - 1]
490   ∧ maxVVal = [a ∈ Acceptor ↦ - 1]
491   ∧ maxVVal = [a ∈ Acceptor ↦ None]
492   ∧ 2avSent = [a ∈ Acceptor ↦ {}]
493   ∧ knowsSent = [a ∈ Acceptor ↦ {}]
494   ∧ bmsgs = {}

```



```

496  $acceptor(self) \triangleq \exists b \in Ballot :$ 
497  $\vee \wedge (b > maxBal[self]) \wedge (sentMsgs("1a", b) \neq \{\})$ 
498  $\wedge maxBal' = [maxBal \text{ EXCEPT } ![self] = b]$ 
499  $\wedge bmsgs' = (bmsgs \cup \{[type \mapsto "1b", bal \mapsto b, acc \mapsto self,$ 
500  $m2av \mapsto 2avSent[self],$ 
501  $mbal \mapsto maxVBal[self], mval \mapsto maxVVal[self]]\})$ 
502  $\wedge \text{UNCHANGED } \langle maxVBal, maxVVal, 2avSent, knowsSent \rangle$ 
503  $\vee \wedge \wedge maxBal[self] \leq b$ 
504  $\wedge \forall r \in 2avSent[self] : r.bal < b$ 
505  $\wedge \exists m \in \{ms \in sentMsgs("1c", b) : KnowsSafeAt(self, b, ms.val)\} :$ 
506  $\wedge bmsgs' = (bmsgs \cup$ 
507  $\{[type \mapsto "2av", bal \mapsto b, val \mapsto m.val, acc \mapsto self]\})$ 
508  $\wedge 2avSent' = [2avSent \text{ EXCEPT } ![self] = \{r \in 2avSent[self] : r.val \neq m.val\}$ 
509  $\cup \{[val \mapsto m.val, bal \mapsto b]\})$ 
510  $\wedge maxBal' = [maxBal \text{ EXCEPT } ![self] = b]$ 
511  $\wedge \text{UNCHANGED } \langle maxVBal, maxVVal, knowsSent \rangle$ 
512  $\vee \wedge maxBal[self] \leq b$ 
513  $\wedge \exists v \in \{vv \in Value :$ 
514  $\exists Q \in ByzQuorum :$ 
515  $\forall aa \in Q :$ 
516  $\exists m \in sentMsgs("2av", b) : \wedge m.val = vv$ 
517  $\wedge m.acc = aa\} :$ 
518  $\wedge bmsgs' = (bmsgs \cup$ 
519  $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\})$ 
520  $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = v]$ 
521  $\wedge maxBal' = [maxBal \text{ EXCEPT } ![self] = b]$ 
522  $\wedge maxVBal' = [maxVBal \text{ EXCEPT } ![self] = b]$ 
523  $\wedge \text{UNCHANGED } \langle 2avSent, knowsSent \rangle$ 
524  $\vee \wedge \exists S \in \text{SUBSET } sentMsgs("1b", b) :$ 
525  $knowsSent' = [knowsSent \text{ EXCEPT } ![self] = knowsSent[self] \cup S]$ 
526  $\wedge \text{UNCHANGED } \langle maxBal, maxVBal, maxVVal, 2avSent, bmsgs \rangle$ 
528  $leader(self) \triangleq \wedge \vee \wedge bmsgs' = (bmsgs \cup \{[type \mapsto "1a", bal \mapsto self]\})$ 
529  $\vee \wedge \exists S \in \text{SUBSET } [type : \{"1c"\}, bal : \{self\}, val : Value] :$ 
530  $bmsgs' = (bmsgs \cup S)$ 
531  $\wedge \text{UNCHANGED } \langle maxBal, maxVBal, maxVVal, 2avSent, knowsSent \rangle$ 
533  $facceptor(self) \triangleq \wedge \exists m \in \{mm \in 1bMessage \cup 2avMessage \cup 2bMessage :$ 
534  $mm.acc = self\} :$ 
535  $bmsgs' = (bmsgs \cup \{m\})$ 
536  $\wedge \text{UNCHANGED } \langle maxBal, maxVBal, maxVVal, 2avSent,$ 
537  $knowsSent \rangle$ 
539  $Next \triangleq (\exists self \in Acceptor : acceptor(self))$ 
540  $\vee (\exists self \in Ballot : leader(self))$ 
541  $\vee (\exists self \in FakeAcceptor : facceptor(self))$ 

```

543 $Spec \triangleq Init \wedge \Box[Next]_{vars}$

545 **END TRANSLATION**

546

As in module *PConProof*, we now rewrite the next-state relation in a form more convenient for writing proofs.

551 $Phase1b(self, b) \triangleq$
 552 $\wedge (b > maxBal[self]) \wedge (sentMsgs("1a", b) \neq \{\})$
 553 $\wedge maxBal' = [maxBal \text{ EXCEPT } ![self] = b]$
 554 $\wedge bmsgs' = bmsgs \cup \{[type \mapsto "1b", bal \mapsto b, acc \mapsto self,$
 555 $m2av \mapsto 2avSent[self],$
 556 $mbal \mapsto maxVVal[self], mval \mapsto maxVVal[self]]\}$
 557 $\wedge \text{UNCHANGED } \langle maxVVal, maxVVal, 2avSent, knowsSent \rangle$

559 $Phase2av(self, b) \triangleq$
 560 $\wedge maxBal[self] \leq b$
 561 $\wedge \forall r \in 2avSent[self] : r.bal < b$
 562 $\wedge \exists m \in \{ms \in sentMsgs("1c", b) : KnowsSafeAt(self, b, ms.val)\} :$
 563 $\wedge bmsgs' = bmsgs \cup$
 564 $\{[type \mapsto "2av", bal \mapsto b, val \mapsto m.val, acc \mapsto self]\}$
 565 $\wedge 2avSent' = [2avSent \text{ EXCEPT}$
 566 $![self] = \{r \in 2avSent[self] : r.val \neq m.val\}$
 567 $\cup \{[val \mapsto m.val, bal \mapsto b]\}]$
 568 $\wedge maxBal' = [maxBal \text{ EXCEPT } ![self] = b]$
 569 $\wedge \text{UNCHANGED } \langle maxVVal, maxVVal, knowsSent \rangle$

571 $Phase2b(self, b) \triangleq$
 572 $\wedge maxBal[self] \leq b$
 573 $\wedge \exists v \in \{vv \in Value :$
 574 $\exists Q \in ByzQuorum :$
 575 $\forall a \in Q :$
 576 $\exists m \in sentMsgs("2av", b) : \wedge m.val = vv$
 577 $\wedge m.acc = a\} :$
 578 $\wedge bmsgs' = (bmsgs \cup$
 579 $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\})$
 580 $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = v]$
 581 $\wedge maxBal' = [maxBal \text{ EXCEPT } ![self] = b]$
 582 $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = b]$
 583 $\wedge \text{UNCHANGED } \langle 2avSent, knowsSent \rangle$

585 $LearnsSent(self, b) \triangleq$
 586 $\wedge \exists S \in \text{SUBSET } sentMsgs("1b", b) :$
 587 $knowsSent' = [knowsSent \text{ EXCEPT } ![self] = knowsSent[self] \cup S]$
 588 $\wedge \text{UNCHANGED } \langle maxBal, maxVVal, maxVVal, 2avSent, bmsgs \rangle$

590 $Phase1a(self) \triangleq$

591 $\wedge bmsgs' = (bmsgs \cup \{[type \mapsto "1a", bal \mapsto self]\})$
 592 $\wedge \text{UNCHANGED } \langle maxBal, maxVVal, maxVVal, 2avSent, knowsSent \rangle$
 594 $Phase1c(self) \triangleq$
 595 $\wedge \exists S \in \text{SUBSET } [type : \{ "1c" \}, bal : \{ self \}, val : Value] :$
 596 $bmsgs' = (bmsgs \cup S)$
 597 $\wedge \text{UNCHANGED } \langle maxBal, maxVVal, maxVVal, 2avSent, knowsSent \rangle$
 599 $FakingAcceptor(self) \triangleq$
 600 $\wedge \exists m \in \{ mm \in 1bMessage \cup 2avMessage \cup 2bMessage : mm.acc = self \} :$
 601 $bmsgs' = (bmsgs \cup \{ m \})$
 602 $\wedge \text{UNCHANGED } \langle maxBal, maxVVal, maxVVal, 2avSent, knowsSent \rangle$

603 |
 The following lemma describes how the next-state relation *Next* can be written in terms of the actions defined above.

608 LEMMA $NextDef \triangleq$
 609 $Next = \vee \exists self \in Acceptor :$
 610 $\quad \exists b \in Ballot : \vee Phase1b(self, b)$
 611 $\quad \vee Phase2av(self, b)$
 612 $\quad \vee Phase2b(self, b)$
 613 $\quad \vee LearnsSent(self, b)$
 614 $\vee \exists self \in Ballot : \vee Phase1a(self)$
 615 $\quad \vee Phase1c(self)$
 616 $\vee \exists self \in FakeAcceptor : FakingAcceptor(self)$
 617 $\langle 1 \rangle 1. \forall self : acceptor(self) = NextDef!2!1!(self)$
 618 BY DEF *acceptor*, *Phase1b*, *Phase2av*, *Phase2b*, *LearnsSent*
 619 $\langle 1 \rangle 2. \forall self : leader(self) = NextDef!2!2!(self)$
 620 BY DEF *leader*, *Phase1a*, *Phase1c*
 621 $\langle 1 \rangle 3. \forall self : facceptor(self) = NextDef!2!3!(self)$
 622 BY DEF *facceptor*, *FakingAcceptor*
 623 $\langle 1 \rangle 4. \text{QED}$
 624 BY $\langle 1 \rangle 1, \langle 1 \rangle 2, \langle 1 \rangle 3$
 625 DEF *Next*, *acceptor*, *leader*, *facceptor*

626 |
 THE REFINEMENT MAPPING

We define a quorum to be the set of acceptors in a *Byzantine* quorum. The quorum assumption *QA* of module *PConProof*, which we here call *QuorumTheorem*, follows easily from the definition and assumption *BQA*.

636 $Quorum \triangleq \{ S \cap Acceptor : S \in ByzQuorum \}$
 638 THEOREM $QuorumTheorem \triangleq$
 639 $\wedge \forall Q1, Q2 \in Quorum : Q1 \cap Q2 \neq \{ \}$
 640 $\wedge \forall Q \in Quorum : Q \subseteq Acceptor$
 641 $\langle 1 \rangle 1. QuorumTheorem!1$
 642 $\langle 2 \rangle 1. \text{SUFFICES ASSUME NEW } Q1 \in Quorum, \text{ NEW } Q2 \in Quorum$

```

643          PROVE  $Q1 \cap Q2 \neq \{\}$ 
644      OBVIOUS
645  ⟨2⟩2. PICK  $BQ1 \in ByzQuorum, BQ2 \in ByzQuorum :$ 
646           $\wedge Q1 = BQ1 \cap Acceptor$ 
647           $\wedge Q2 = BQ2 \cap Acceptor$ 
648      BY ⟨2⟩1 DEF Quorum
649  ⟨2⟩3.  $Q1 \cap Q2 = BQ1 \cap BQ2 \cap Acceptor$ 
650      BY ⟨2⟩2
651  ⟨2⟩4. QED
652      BY BQA, ⟨2⟩3
653  ⟨1⟩2. QuorumTheorem!2
654      BY DEF Quorum
655  ⟨1⟩3. QED
656      BY ⟨1⟩1, ⟨1⟩2

```

We now define refinement mapping under which our algorithm implements the algorithm of module *PConProof*. First, we define the set *msgs* that implements the variable of the same name in *PConProof*. There are two non-obvious parts of the definition.

1. The 1c messages in *msgs* should just be the ones that are legal—that is, messages whose value is safe at the indicated ballot. The obvious way to define legality is in terms of 1b messages that have been sent. However, this has the effect that sending a 1b message can add both that 1b message and one or more 1c messages to *msgs*. Proving implementation under this refinement mapping would require adding a stuttering variable. Instead, we define the 1c message to be legal if the set of 1b messages that some acceptor knows were sent confirms its legality. Thus, those 1c messages are added to *msgs* by the *LearnsSent* ation, which has no other effect on the refinement mapping.

2. A 2a message is added to *msgs* when a quorum of acceptors have reacted to it by sending a 2av message.

```

678   $msgsOfType(t) \triangleq \{m \in bmsgs : m.type = t\}$ 
680   $acceptorMsgsOfType(t) \triangleq \{m \in msgsOfType(t) : m.acc \in Acceptor\}$ 
682   $1bRestrict(m) \triangleq [type \mapsto "1b", acc \mapsto m.acc, bal \mapsto m.bal,$ 
683       $mbal \mapsto m.mbal, mval \mapsto m.mval]$ 
685   $1bmsgs \triangleq \{1bRestrict(m) : m \in acceptorMsgsOfType("1b")\}$ 
687   $1cmsgs \triangleq \{m \in msgsOfType("1c") :$ 
688       $\exists a \in Acceptor : KnowsSafeAt(a, m.bal, m.val)\}$ 
690   $2amsgs \triangleq \{m \in [type : \{"2a"\}, bal : Ballot, val : Value] :$ 
691       $\exists Q \in Quorum :$ 
692       $\forall a \in Q :$ 
693       $\exists m2av \in acceptorMsgsOfType("2av") :$ 
694       $\wedge m2av.acc = a$ 
695       $\wedge m2av.bal = m.bal$ 
696       $\wedge m2av.val = m.val\}$ 

```

698 $msgs \triangleq msgsOfType("1a") \cup 1bmsgs \cup 1cmsgs \cup 2amsgs$
699 $\cup acceptorMsgsOfType("2b")$

We now define $PmaxBal$, the state function with which we instantiate the variable $maxBal$ of $PConProof$. The reason we don't just instantiate it with the variable $maxBal$ is that $maxBal[a]$ can change when acceptor a performs a $Phase2av$ action, which does not correspond to any acceptor action of the $PConProof$ algorithm. We want $PmaxBal[a]$ to change only when a performs a $Phase1b$ or $Phase2b$ action—that is, when it sends a $1b$ or $2b$ message. Thus, we define $PmaxBal[a]$ to be the largest bal field of all $1b$ and $2b$ messages sent by a .

To define $PmaxBal$, we need to define an operator $MaxBallot$ so that $MaxBallot(S)$ is the largest element of S if S is non-empty a finite set consisting of ballot numbers and possibly the value -1 .

715 $MaxBallot(S) \triangleq$
716 IF $S = \{\}$ THEN -1
717 ELSE CHOOSE $mb \in S : \forall x \in S : mb \geq x$

To prove that the CHOOSE in this definition actually does choose a maximum of S when S is nonempty, we need the following trivial fact. It has been checked by *TLC* with $-5 \dots 5$ substituted for Int .

724 AXIOM $FiniteSetHasMax \triangleq$
725 $\forall S \in SUBSET Int :$
726 $IsFiniteSet(S) \wedge (S \neq \{\}) \Rightarrow \exists max \in S : \forall x \in S : max \geq x$

Our proofs use this property of $MaxBallot$.

731 THEOREM $MaxBallotProp \triangleq$
732 $\forall S \in SUBSET (Ballot \cup \{-1\}) :$
733 $IsFiniteSet(S) \Rightarrow$
734 IF $S = \{\}$ THEN $MaxBallot(S) = -1$
735 ELSE $\wedge MaxBallot(S) \in S$
736 $\wedge \forall x \in S : MaxBallot(S) \geq x$
737 $\langle 1 \rangle$ SUFFICES ASSUME NEW $S \in SUBSET (Ballot \cup \{-1\})$,
738 $IsFiniteSet(S)$
739 PROVE $MaxBallotProp!(S)!2$
740 OBVIOUS
741 $\langle 1 \rangle 1$. CASE $S = \{\}$
742 BY $\langle 1 \rangle 1$ DEF $MaxBallot$
743 $\langle 1 \rangle 2$. CASE $S \neq \{\}$
744 $\langle 2 \rangle 1$. $S \in SUBSET Int$
745 BY DEF $Ballot$ $\langle 2 \rangle 1$
746 $\langle 2 \rangle 2$. $\exists mb \in S : \forall x \in S : mb \geq x$
747 BY $\langle 2 \rangle 1, \langle 1 \rangle 2, FiniteSetHasMax$
749 $\langle 2 \rangle 3$. QED
750 BY $\langle 1 \rangle 2, \langle 2 \rangle 2$ DEF $MaxBallot$
751 $\langle 1 \rangle 3$. QED
752 BY $\langle 1 \rangle 1, \langle 1 \rangle 2$

We now prove a couple of lemmas about $MaxBallot$.

757 LEMMA *MaxBallotLemma1* \triangleq
758 $\forall S \in \text{SUBSET } (\text{Ballot} \cup \{-1\}) :$
759 $\text{IsFiniteSet}(S) \Rightarrow$
760 $\forall y \in S :$
761 $(\forall x \in S : y \geq x) \Rightarrow (y = \text{MaxBallot}(S))$
762 $\langle 1 \rangle 1.$ SUFFICES ASSUME NEW $S \in \text{SUBSET } (\text{Ballot} \cup \{-1\}),$
763 $\text{IsFiniteSet}(S),$
764 NEW $y \in S,$
765 $\forall x \in S : y \geq x$
766 PROVE $y = \text{MaxBallot}(S)$
767 OBVIOUS
768 $\langle 1 \rangle 2. \wedge \text{MaxBallot}(S) \in S$
769 $\wedge \forall x \in S : \text{MaxBallot}(S) \geq x$
770 BY $\langle 1 \rangle 1, \text{MaxBallotProp}$
771 $\langle 1 \rangle 3. \text{MaxBallot}(S) \geq y$
772 BY $\langle 1 \rangle 2$
773 $\langle 1 \rangle 4. y \in \text{Ballot} \cup \{-1\}$
774 OBVIOUS
775 $\langle 1 \rangle 5. y \geq \text{MaxBallot}(S)$
776 BY $\langle 1 \rangle 1, \langle 1 \rangle 2$
777 $\langle 1 \rangle 6. \forall mbs \in \text{Ballot} \cup \{-1\} :$
778 $mbs \geq y \wedge y \geq mbs \Rightarrow y = mbs$
779 BY $\langle 1 \rangle 4, \text{SimpleArithmetic}$ DEF *Ballot*
780 $\langle 1 \rangle 7. \text{MaxBallot}(S) \in \text{Ballot} \cup \{-1\}$
781 BY $\langle 1 \rangle 2$
782 $\langle 1 \rangle 8.$ QED
783 BY $\langle 1 \rangle 3, \langle 1 \rangle 5, \langle 1 \rangle 6, \langle 1 \rangle 7$

785 LEMMA *MaxBallotLemma2* \triangleq
786 $\forall S, T \in \text{SUBSET } (\text{Ballot} \cup \{-1\}) :$
787 $\text{IsFiniteSet}(S) \wedge \text{IsFiniteSet}(T) \Rightarrow$
788 $\text{MaxBallot}(S \cup T) = \text{IF } \text{MaxBallot}(S) \geq \text{MaxBallot}(T)$
789 $\text{THEN } \text{MaxBallot}(S)$
790 $\text{ELSE } \text{MaxBallot}(T)$
791 $\langle 1 \rangle 1. \forall S \in \text{SUBSET } (\text{Ballot} \cup \{-1\}) :$
792 $\text{IsFiniteSet}(S) \Rightarrow (\text{MaxBallot}(S) \in \text{Ballot} \cup \{-1\})$
793 BY *MaxBallotProp*
794 $\langle 1 \rangle 2.$ ASSUME NEW $S \in \text{SUBSET } (\text{Ballot} \cup \{-1\}),$
795 NEW $T \in \text{SUBSET } (\text{Ballot} \cup \{-1\}),$
796 $\text{IsFiniteSet}(S) \wedge \text{IsFiniteSet}(T),$
797 $\text{MaxBallot}(S) \geq \text{MaxBallot}(T)$
798 PROVE $\text{MaxBallot}(S \cup T) = \text{MaxBallot}(S)$
799 $\langle 2 \rangle 1.$ CASE $S = \{\}$
800 $\langle 3 \rangle 1.$ CASE $T = \{\}$
801 BY $\langle 3 \rangle 1$

802 $\langle 3 \rangle 2.$ CASE $T \neq \{\}$
803 $\langle 4 \rangle 1.$ $MaxBallot(S) = -1$
804 BY $\langle 1 \rangle 2, \langle 2 \rangle 1, MaxBallotProp$
805 $\langle 4 \rangle 2.$ $MaxBallot(T) = -1$
806 $\langle 5 \rangle 1.$ $\forall x \in Ballot \cup \{-1\} : -1 \geq x \Rightarrow x = -1$
807 BY *SimpleArithmetic* DEF *Ballot*
808 $\langle 5 \rangle 2.$ $MaxBallot(T) \in Ballot \cup \{-1\}$
809 BY $\langle 1 \rangle 2, \langle 1 \rangle 1$
810 $\langle 5 \rangle 3.$ QED
811 BY $\langle 5 \rangle 1, \langle 5 \rangle 2, \langle 4 \rangle 1, \langle 1 \rangle 2$
812 $\langle 4 \rangle 3.$ $-1 \in T \wedge \forall x \in T : -1 \geq x$
813 BY $\langle 4 \rangle 2, \langle 3 \rangle 2, \langle 1 \rangle 2, MaxBallotProp$
814 $\langle 4 \rangle 4.$ QED
815 BY $\langle 4 \rangle 1, \langle 4 \rangle 3, \langle 3 \rangle 2, \langle 2 \rangle 1, \langle 1 \rangle 2, MaxBallotLemma1$
816 $\langle 3 \rangle 3.$ QED
817 BY $\langle 3 \rangle 1, \langle 3 \rangle 2$
818 $\langle 2 \rangle 2.$ CASE $S \neq \{\}$
819 $\langle 3 \rangle 1.$ CASE $T = \{\}$
820 BY $\langle 3 \rangle 1$
821 $\langle 3 \rangle 2.$ CASE $T \neq \{\}$
822 $\langle 4 \rangle 1.$ $\wedge MaxBallot(S) \in S$
823 $\wedge \forall x \in S : MaxBallot(S) \geq x$
824 BY $\langle 2 \rangle 2, \langle 1 \rangle 2, MaxBallotProp$
825 $\langle 4 \rangle 2.$ $\wedge MaxBallot(T) \in T$
826 $\wedge \forall x \in T : MaxBallot(T) \geq x$
827 BY $\langle 3 \rangle 2, \langle 1 \rangle 2, MaxBallotProp$
828 $\langle 4 \rangle 3.$ $\forall x, y \in Ballot \cup \{-1\}, TT \in \text{SUBSET}(Ballot \cup \{-1\}) :$
829 $(x \geq y) \wedge (\forall z \in TT : y \geq z) \Rightarrow (\forall z \in TT : x \geq z)$
830 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $x \in Ballot \cup \{-1\},$ NEW $y \in Ballot \cup \{-1\},$
831 NEW $TT \in \text{SUBSET}(Ballot \cup \{-1\}),$
832 $(x \geq y), \forall z \in TT : y \geq z$
833 PROVE $(\forall z \in TT : x \geq z)$
834 OBVIOUS
835 $\langle 5 \rangle 2.$ SUFFICES ASSUME NEW $z \in TT$
836 PROVE $x \geq z$
837 OBVIOUS
838 $\langle 5 \rangle 3.$ $z \in Ballot \cup \{-1\}$
839 BY $\langle 5 \rangle 1, \langle 5 \rangle 2$
840 $\langle 5 \rangle 4.$ $y \geq z$
841 BY $\langle 5 \rangle 1$
842 $\langle 5 \rangle 5.$ QED
843 BY *SimpleArithmetic*, $\langle 5 \rangle 1, \langle 5 \rangle 3, \langle 5 \rangle 4$ DEF *Ballot*
845 $\langle 4 \rangle 4.$ $\wedge MaxBallot(S) \in Ballot \cup \{-1\}$
846 $\wedge MaxBallot(T) \in Ballot \cup \{-1\}$

847 BY $\langle 1 \rangle 1, \langle 1 \rangle 2$
 848 $\langle 4 \rangle 5. \forall x \in T : \text{MaxBallot}(S) \geq x$
 849 BY $\langle 1 \rangle 2, \langle 4 \rangle 2, \langle 4 \rangle 3, \langle 4 \rangle 4$
 850 $\langle 4 \rangle 6. \wedge \text{MaxBallot}(S) \in S \cup T$
 851 $\wedge \forall x \in S \cup T : \text{MaxBallot}(S) \geq x$
 852 BY $\langle 4 \rangle 1, \langle 4 \rangle 5$
 853 $\langle 4 \rangle 7. \text{IsFiniteSet}(S \cup T)$
 854 BY $\langle 1 \rangle 2, \text{UnionOfFiniteSetsFinite}$
 855 $\langle 4 \rangle 8. \text{QED}$
 856 BY $\langle 4 \rangle 6, \langle 4 \rangle 7, \text{MaxBallotLemma1}$
 857 $\langle 3 \rangle 3. \text{QED}$
 858 BY $\langle 3 \rangle 1, \langle 3 \rangle 2$
 859 $\langle 2 \rangle 3. \text{QED}$
 860 BY $\langle 2 \rangle 1, \langle 2 \rangle 2$
 861 $\langle 1 \rangle 3. \text{SUFFICES ASSUME NEW } S \in \text{SUBSET } (\text{Ballot} \cup \{-1\}),$
 862 $\text{NEW } T \in \text{SUBSET } (\text{Ballot} \cup \{-1\}),$
 863 $\text{IsFiniteSet}(S) \wedge \text{IsFiniteSet}(T)$
 864 $\text{PROVE } \text{MaxBallot}(S \cup T) = \text{IF } \text{MaxBallot}(S) \geq \text{MaxBallot}(T)$
 865 $\text{THEN } \text{MaxBallot}(S)$
 866 $\text{ELSE } \text{MaxBallot}(T)$
 867 OBVIOUS
 868 $\langle 1 \rangle 4. \text{CASE } \text{MaxBallot}(S) \geq \text{MaxBallot}(T)$
 869 $\langle 2 \rangle \text{SUFFICES } \text{MaxBallot}(S \cup T) = \text{MaxBallot}(S)$
 870 BY $\langle 1 \rangle 3, \langle 1 \rangle 4$
 871 $\langle 2 \rangle \text{QED}$
 872 BY $\langle 1 \rangle 2, \langle 1 \rangle 3, \langle 1 \rangle 4$ added $\langle 1 \rangle 3$ on 13 Nov 2010
 873 $\langle 1 \rangle 5. \text{CASE } \neg(\text{MaxBallot}(S) \geq \text{MaxBallot}(T))$
 874 $\langle 2 \rangle \text{SUFFICES } \text{MaxBallot}(T \cup S) = \text{MaxBallot}(T)$
 875 BY $\langle 1 \rangle 3, \langle 1 \rangle 5$
 876 $\langle 2 \rangle \text{MaxBallot}(T) \geq \text{MaxBallot}(S)$
 877 $\langle 3 \rangle 1. \forall x, y \in \text{Ballot} \cup \{-1\} : x \geq y \vee y \geq x$
 878 BY *SimpleArithmetic* DEF *Ballot*
 879 $\langle 3 \rangle 2. \wedge \text{MaxBallot}(S) \in \text{Ballot} \cup \{-1\}$
 880 $\wedge \text{MaxBallot}(T) \in \text{Ballot} \cup \{-1\}$
 881 BY $\langle 1 \rangle 1, \langle 1 \rangle 3$
 882 $\langle 3 \rangle 3. \text{QED}$
 883 BY $\langle 1 \rangle 5, \langle 3 \rangle 1, \langle 3 \rangle 2$
 884 $\langle 2 \rangle \text{QED}$
 885 BY $\langle 1 \rangle 2, \langle 1 \rangle 3, \langle 1 \rangle 5$
 886 $\langle 1 \rangle 6. \text{QED}$
 887 BY $\langle 1 \rangle 4, \langle 1 \rangle 5$

We finally come to our definition of *PmaxBal*, the state function substituted for variable *maxBal* of module *PConProof* by our refinement mapping. We also prove a couple of lemmas about *PmaxBal*.


```

896  $1bOr2bMsgs \triangleq \{m \in bmsgs : m.type \in \{"1b", "2b"\}\}$ 
898  $PmaxBal \triangleq [a \in Acceptor \mapsto$ 
899    $MaxBallot(\{m.bal : m \in \{ma \in 1bOr2bMsgs :$ 
900      $ma.acc = a\}\})]$ 
902 LEMMA  $PmaxBalLemma1 \triangleq$ 
903    $\forall m : \wedge bmsgs' = bmsgs \cup \{m\}$ 
904      $\wedge m.type \neq "1b" \wedge m.type \neq "2b"$ 
905      $\Rightarrow PmaxBal' = PmaxBal$ 
906  $\langle 1 \rangle$  SUFFICES ASSUME NEW  $m$ ,
907    $bmsgs' = bmsgs \cup \{m\}$ ,
908    $m.type \neq "1b" \wedge m.type \neq "2b"$ 
909   PROVE  $PmaxBal' = PmaxBal$ 
910   OBVIOUS
911  $\langle 1 \rangle 1$ . ASSUME NEW  $ma$ ,  $ma.type \in \{"1b", "2b"\}$ 
912   PROVE  $ma \in bmsgs' \equiv ma \in bmsgs$ 
913   BY  $\langle 1 \rangle 1$ 
914  $\langle 1 \rangle 2$ . QED
915   BY  $\langle 1 \rangle 1$  DEF  $PmaxBal, 1bOr2bMsgs$ 
917 LEMMA  $PmaxBalLemma2 \triangleq$ 
918    $\forall m : (bmsgs' = bmsgs \cup \{m\}) \Rightarrow$ 
919      $\forall a \in Acceptor : (m.acc \neq a \Rightarrow PmaxBal'[a] = PmaxBal[a])$ 
920  $\langle 1 \rangle$  SUFFICES ASSUME NEW  $m$ ,
921    $bmsgs' = bmsgs \cup \{m\}$ ,
922   NEW  $a \in Acceptor$ ,
923    $m.acc \neq a$ 
924   PROVE  $PmaxBal'[a] = PmaxBal[a]$ 
925   OBVIOUS
926  $\langle 1 \rangle 1$ . ASSUME NEW  $ma$ ,  $ma.acc \neq m.acc$ 
927   PROVE  $ma \in bmsgs' \equiv ma \in bmsgs$ 
928   BY  $\langle 1 \rangle 1$ 
929  $\langle 1 \rangle 2$ . QED
930   BY  $\langle 1 \rangle 1$  DEF  $PmaxBal, 1bOr2bMsgs$ 

```

Finally, we define the refinement mapping. As before, for any operator op defined in module $PConProof$, the following `INSTANCE` statement defines $P!op$ to be the operator obtained from op by the indicated substitutions, along with the implicit substitutions

```

Acceptor  $\leftarrow$  Acceptor,
Quorum  $\leftarrow$  Quorum
Value  $\leftarrow$  Value
maxVBal  $\leftarrow$  maxVBal
maxVVal  $\leftarrow$  maxVVal
msgs  $\leftarrow$  msgs

```

945 $P \triangleq \text{INSTANCE } PConProof \text{ WITH } maxBal \leftarrow PmaxBal$

946

We now define the inductive invariant Inv used in our proof. It is defined to be the conjunction of a number of separate invariants that we define first, starting with the ever-present type-correctness invariant.

953 $TypeOK \triangleq \wedge maxBal \in [Acceptor \rightarrow Ballot \cup \{-1\}]$
 954 $\wedge 2avSent \in [Acceptor \rightarrow \text{SUBSET } [val : Value, bal : Ballot]]$
 955 $\wedge maxVVal \in [Acceptor \rightarrow Ballot \cup \{-1\}]$
 956 $\wedge maxVVal \in [Acceptor \rightarrow Value \cup \{None\}]$
 957 $\wedge knowsSent \in [Acceptor \rightarrow \text{SUBSET } 1bMessage]$
 958 $\wedge bmsgs \subseteq BMessage$

To use the definition of $PmaxBal$, we need to know that the set of $1b$ and $2b$ messages in $bmsgs$ is finite. This is asserted by the following invariant. Note that the set $bmsgs$ is not necessarily finite because we allow a $Phase1c$ action to send an infinite number of $1c$ messages.

966 $bmsgsFinite \triangleq IsFiniteSet(1bOr2bMsgs)$

The following lemma is used to prove the invariance of $bmsgsFinite$.

971 LEMMA $FiniteMsgsLemma \triangleq$
 972 $\forall m : bmsgsFinite \wedge (bmsgs' = bmsgs \cup \{m\}) \Rightarrow bmsgsFinite'$
 973 $\langle 1 \rangle$ SUFFICES ASSUME NEW $m, bmsgsFinite, bmsgs' = bmsgs \cup \{m\}$
 974 PROVE $bmsgsFinite'$
 975 OBVIOUS
 976 $\langle 1 \rangle 1.$ CASE $(m.type \in \{"1b", "2b"\})$
 977 $\langle 2 \rangle 1.$ $1bOr2bMsgs' = 1bOr2bMsgs \cup \{m\}$
 978 BY $\langle 1 \rangle 1$ DEF $1bOr2bMsgs$
 979 $\langle 2 \rangle 2.$ QED
 980 BY $\langle 2 \rangle 1$, $SingletonSetFinite$, $UnionOfFiniteSetsFinite$ DEF $bmsgsFinite$
 981 $\langle 1 \rangle 2.$ CASE $m.type \notin \{"1b", "2b"\}$
 982 BY $\langle 1 \rangle 2$ DEF $bmsgsFinite, 1bOr2bMsgs$
 983 $\langle 1 \rangle 3.$ QED
 984 BY $\langle 1 \rangle 1, \langle 1 \rangle 2$

Invariant $1bInv1$ asserts that if (good) acceptor a has $mCBal[a] \neq -1$, then there is a $1c$ message for ballot $mCBal[a]$ and value $mCVal[a]$ in the emulated execution of $PaxosConsensus$.

991 $1bInv1 \triangleq \forall m \in bmsgs :$
 992 $\wedge m.type = "1b"$
 993 $\wedge m.acc \in Acceptor$
 994 $\Rightarrow \forall r \in m.m2av :$
 995 $[type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val] \in msgs$

Invariant $1bInv2$ asserts that an acceptor sends at most one $1b$ message for any ballot.

1001 $1bInv2 \triangleq \forall m1, m2 \in bmsgs :$
 1002 $\wedge m1.type = "1b"$
 1003 $\wedge m2.type = "1b"$
 1004 $\wedge m1.acc \in Acceptor$

1005 $\wedge m1.acc = m2.acc$
 1006 $\wedge m1.bal = m2.bal$
 1007 $\Rightarrow m1 = m2$

Invariant *2avInv1* asserts that an acceptor sends at most one *2av* message in any ballot.

1013 $2avInv1 \triangleq \forall m1, m2 \in bmsgs :$
 1014 $\quad \wedge m1.type = \text{"2av"}$
 1015 $\quad \wedge m2.type = \text{"2av"}$
 1016 $\quad \wedge m1.acc \in \text{Acceptor}$
 1017 $\quad \wedge m1.acc = m2.acc$
 1018 $\quad \wedge m1.bal = m2.bal$
 1019 $\quad \Rightarrow m1 = m2$

Invariant *2avInv2* follows easily from the meaning (and setting) of *2avSent*.

1025 $2avInv2 \triangleq \forall m \in bmsgs :$
 1026 $\quad \wedge m.type = \text{"2av"}$
 1027 $\quad \wedge m.acc \in \text{Acceptor}$
 1028 $\quad \Rightarrow \exists r \in 2avSent[m.acc] : \wedge r.val = m.val$
 1029 $\quad \quad \wedge r.bal \geq m.bal$

Invariant *2avInv3* asserts that an acceptor sends a *2av* message only if the required *1c* message exists in the emulated execution of *PaxosConsensus*.

1036 $2avInv3 \triangleq \forall m \in bmsgs :$
 1037 $\quad \wedge m.type = \text{"2av"}$
 1038 $\quad \wedge m.acc \in \text{Acceptor}$
 1039 $\quad \Rightarrow [type \mapsto \text{"1c"}, bal \mapsto m.bal, val \mapsto m.val] \in msgs$

Invariant *maxBalInv* is a simple consequence of the fact that an acceptor *a* sets *maxBal[a]* to *b* whenever it sends a *1b*, *2av*, or *2b* message in ballot *b*.

1046 $maxBalInv \triangleq \forall m \in bmsgs :$
 1047 $\quad \wedge m.type \in \{\text{"1b"}, \text{"2av"}, \text{"2b"}\}$
 1048 $\quad \wedge m.acc \in \text{Acceptor}$
 1049 $\quad \Rightarrow m.bal \leq maxBal[m.acc]$

Invariant *accInv* asserts some simple relations between the variables local to an acceptor, as well as the fact that acceptor *a* sets *maxCBal[a]* to *b* and *maxCVal[a]* to *v* only if there is a ballot-*b* *1c* message for value *c* in the simulated execution of the *PaxosConsensus* algorithm.

1058 $accInv \triangleq \forall a \in \text{Acceptor} :$
 1059 $\quad \forall r \in 2avSent[a] :$
 1060 $\quad \quad \wedge r.bal \leq maxBal[a]$
 1061 $\quad \quad \wedge [type \mapsto \text{"1c"}, bal \mapsto r.bal, val \mapsto r.val] \in msgs$

Invariant *knowsSentInv* simply asserts that for any acceptor *a*, *knowsSent[a]* is a set of *1b* messages that have actually been sent.

1067 $knowsSentInv \triangleq \forall a \in \text{Acceptor} : knowsSent[a] \subseteq msgsOfType(\text{"1b"})$
 1069 $Inv \triangleq$

1070 $TypeOK \wedge bmsgsFinite \wedge 1bInv1 \wedge 1bInv2 \wedge maxBalInv \wedge 2avInv1 \wedge 2avInv2$
 1071 $\wedge 2avInv3 \wedge accInv \wedge knowsSentInv$

1072

We now prove some simple lemmas that are useful for reasoning about $PmaxBal$.

1077 LEMMA $PMaBalLemma3 \triangleq$
 1078 ASSUME $TypeOK$,
 1079 $bmsgsFinite$,
 1080 NEW $a \in Acceptor$
 1081 PROVE LET $S \triangleq \{m.bal : m \in \{ma \in bmsgs :$
 1082 $\wedge ma.type \in \{“1b”, “2b”\}$
 1083 $\wedge ma.acc = a\}\}$
 1084 IN $\wedge IsFiniteSet(S)$
 1085 $\wedge S \in SUBSET Ballot$
 1086 $\langle 1 \rangle$ DEFINE $T \triangleq \{ma \in bmsgs : \wedge ma.type \in \{“1b”, “2b”\}$
 1087 $\wedge ma.acc = a\}$
 1088 $S \triangleq \{m.bal : m \in T\}$
 1089 $\langle 1 \rangle 1. IsFiniteSet(S)$
 1090 $\langle 2 \rangle 1. IsFiniteSet(T)$
 1091 BY $SubsetOfFiniteSetFinite$ DEF $bmsgsFinite, 1bOr2bMsgs$
 1092 $\langle 2 \rangle$ DEFINE $f[m \in T] \triangleq m.bal$
 1093 $\langle 2 \rangle 2. IsFiniteSet(\{f[m] : m \in T\})$
 1094 BY $\langle 2 \rangle 1, ImageOfFiniteSetFinite$
 1095 $\langle 2 \rangle 3. QED$
 1096 BY $\langle 2 \rangle 2$
 1097 $\langle 1 \rangle 2. ASSUME NEW b \in S$
 1098 PROVE $b \in Ballot$
 1099 $\langle 2 \rangle 1. PICK m \in bmsgs : b = m.bal \wedge m.type \in \{“1b”, “2b”\}$
 1100 OBVIOUS
 1101 $\langle 2 \rangle 2. CASE m.type = “1b”$
 1102 $\langle 3 \rangle 1. m \in 1bMessage$
 1103 BY $\langle 2 \rangle 2, BMessageLemma$ DEF $TypeOK$
 1104 $\langle 3 \rangle 2. QED$
 1105 BY $\langle 3 \rangle 1, \langle 2 \rangle 1$ DEF $1bMessage$
 1106 $\langle 2 \rangle 3. CASE m.type = “2b”$
 1107 $\langle 3 \rangle 1. m \in 2bMessage$
 1108 BY $\langle 2 \rangle 3, BMessageLemma$ DEF $TypeOK$
 1109 $\langle 3 \rangle 2. QED$
 1110 BY $\langle 3 \rangle 1, \langle 2 \rangle 1$ DEF $2bMessage$
 1111 $\langle 2 \rangle 4. QED$
 1112 BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3$
 1113 $\langle 1 \rangle 3. QED$
 1114 BY $\langle 1 \rangle 1, \langle 1 \rangle 2$
 1116 LEMMA $PMaBalLemma4 \triangleq$
 1117 $TypeOK \wedge maxBalInv \wedge bmsgsFinite \Rightarrow$

1118 $\forall a \in \text{Acceptor} : PmaxBal[a] \leq maxBal[a]$
1119 $\langle 1 \rangle$ SUFFICES ASSUME $TypeOK$,
1120 $maxBalInv$,
1121 $bmsgsFinite$,
1122 NEW $a \in \text{Acceptor}$
1123 PROVE $PmaxBal[a] \leq maxBal[a]$
1124 OBVIOUS
1125 $\langle 1 \rangle$ DEFINE $SM \triangleq \{ma \in bmsgs : \wedge ma.type \in \{\text{"1b"}, \text{"2b"}\}$
1126 $\wedge ma.acc = a\}$
1127 $S \triangleq \{ma.bal : ma \in SM\}$
1128 $\langle 1 \rangle 1. PmaxBal[a] = MaxBallot(S)$
1129 BY DEF $PmaxBal, 1bOr2bMsgs$
1130 $\langle 1 \rangle 2. \wedge IsFiniteSet(S)$
1131 $\wedge S \in \text{SUBSET} (Ballot \cup \{-1\})$
1132 BY $PMaxBalLemma3$
1133 $\langle 1 \rangle 3. \forall b \in S : b \leq maxBal[a]$
1134 BY DEF $maxBalInv$
1135 $\langle 1 \rangle 4.$ CASE $S = \{\}$
1136 $\langle 2 \rangle 1. PmaxBal[a] = -1$
1137 BY $\langle 1 \rangle 2, \langle 1 \rangle 1, \langle 1 \rangle 4, MaxBallotProp$
1138 $\langle 2 \rangle 2. maxBal[a] \in \{-1\} \cup Ballot$
1139 BY DEF $TypeOK$
1140 $\langle 2 \rangle 3. \forall b \in \{-1\} \cup Ballot : -1 \leq b$
1141 BY $SimpleArithmetic$ DEF $Ballot$
1142 $\langle 2 \rangle 4.$ QED
1143 BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3$
1144 $\langle 1 \rangle 5.$ CASE $S \neq \{\}$
1145 $\langle 2 \rangle 1. MaxBallot(S) \in S$
1146 BY $\langle 1 \rangle 2, \langle 1 \rangle 5, MaxBallotProp$
1147 $\langle 2 \rangle 2.$ QED
1148 BY $\langle 1 \rangle 1, \langle 1 \rangle 3, \langle 2 \rangle 1$
1149 $\langle 1 \rangle 6.$ QED
1150 BY $\langle 1 \rangle 4, \langle 1 \rangle 5$

1152 LEMMA $PmaxBalLemma5 \triangleq$
1153 $TypeOK \wedge bmsgsFinite \Rightarrow$
1154 $\forall a \in \text{Acceptor} : PmaxBal[a] \in Ballot \cup \{-1\}$
1155 $\langle 1 \rangle$ SUFFICES ASSUME $TypeOK, bmsgsFinite$, NEW $a \in \text{Acceptor}$
1156 PROVE $PmaxBal[a] \in Ballot \cup \{-1\}$
1157 OBVIOUS
1158 $\langle 1 \rangle$ DEFINE $S \triangleq \{m.bal : m \in \{ma \in bmsgs : \wedge ma.type \in \{\text{"1b"}, \text{"2b"}\}$
1159 $\wedge ma.acc = a\}\}$
1160 $\langle 1 \rangle 1. \wedge S \subseteq (Ballot \cup \{-1\})$
1161 $\wedge IsFiniteSet(S)$
1162 $\langle 2 \rangle$ DEFINE $M \triangleq \{ma \in bmsgs : \wedge ma.type \in \{\text{"1b"}, \text{"2b"}\}$

```

1163                                      $\wedge ma.acc = a\}$ 
1164  $\langle 2 \rangle 1. IsFiniteSet(M)$ 
1165 BY SubsetOfFiniteSetFinite DEF bmsgsFinite, 1bOr2bMsgs
1166  $\langle 2 \rangle 2. IsFiniteSet(S)$ 
1167  $\langle 3 \rangle$  DEFINE  $f[x \in M] \triangleq x.bal$ 
1168  $\langle 3 \rangle 1. S = \{f[x] : x \in M\}$ 
1169 OBVIOUS
1170  $\langle 3 \rangle$  HIDE DEF  $f, S, M$ 
1171  $\langle 3 \rangle 2$  QED
1172 BY  $\langle 2 \rangle 1, \langle 3 \rangle 1, ImageOfFiniteSetFinite$ 
1173  $\langle 2 \rangle 3. \forall m \in M : m.bal \in Ballot \cup \{-1\}$ 
1174  $\langle 3 \rangle$  SUFFICES ASSUME NEW  $m \in M$ 
1175 PROVE  $m.bal \in Ballot \cup \{-1\}$ 
1176 OBVIOUS
1177  $\langle 3 \rangle 1. m \in bmsgs \wedge m.type \in \{"1b", "2b"\}$ 
1178 OBVIOUS
1179  $\langle 3 \rangle 2. CASE\ m.type = "1b"$ 
1180 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2, BMessageLemma$  DEF TypeOK, 1bMessage
1181  $\langle 3 \rangle 3. CASE\ m.type = "2b"$ 
1182 BY  $\langle 3 \rangle 1, \langle 3 \rangle 3, BMessageLemma$  DEF TypeOK, 2bMessage
1183  $\langle 3 \rangle 4. QED$ 
1184 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3$ 
1185  $\langle 2 \rangle$  QED
1186 BY  $\langle 2 \rangle 2, \langle 2 \rangle 3$ 
1187  $\langle 1 \rangle 2. QED$ 
1188 BY  $\langle 1 \rangle 1, \langle 1 \rangle 2, MaxBallotProp$  DEF PmaxBal, 1bOr2bMsgs

```

Now comes a bunch of useful lemmas.

We first prove that $P!NextDef$ is a valid theorem and give it the name $PNextDef$. This requires proving that the assumptions of module *PConProof* are satisfied by the refinement mapping. Note that $P!NextDef!$ is an abbreviation for the statement of theorem $P!NextDef$ – that is, for the statement of theorem *NextDef* of module *PConProof* under the substitutions of the refinement mapping.

```

1203 LEMMA  $PNextDef \triangleq P!NextDef!$  :
1204  $\langle 1 \rangle 1. P!QA$ 
1205 BY QuorumTheorem
1206  $\langle 1 \rangle 2. P!BallotAssump$ 
1207 BY BallotAssump DEF Ballot, P!Ballot, ByzAcceptor
1208  $\langle 1 \rangle 3. QED$ 
1209 BY  $P!NextDef, \langle 1 \rangle 1, \langle 1 \rangle 2, NoSetContainsEverything$ 

```

The provers have a hard time dealing with all the quantifiers inside the definition of *KnowsSafeAt*. To help them, we define some formulas that allow us to break it into pieces.

1216 $KSet(a, b) \triangleq \{m \in knowsSent[a] : m.bal = b\}$
1217 $KS11a(a, S) \triangleq \exists m \in S : \wedge m.acc = a$
1218 $\wedge m.mbal = -1$
1219 $KS11(BQ, S) \triangleq \forall a \in BQ : KS11a(a, S)$
1220 $KS1(S) \triangleq \exists BQ \in ByzQuorum : KS11(BQ, S)$
1221 $KS21BQa(v, c, a, S) \triangleq \exists m \in S : \wedge m.acc = a$
1222 $\wedge m.mbal \leq c$
1223 $\wedge (m.mbal = c) \Rightarrow (m.mval = v)$
1224 $KS21BQ(v, c, BQ, S) \triangleq \forall a \in BQ : KS21BQa(v, c, a, S)$
1225 $KS21(v, c, S) \triangleq \exists BQ \in ByzQuorum : KS21BQ(v, c, BQ, S)$
1226 $KS22WQa(v, c, a, S) \triangleq \exists m \in S : \wedge m.acc = a$
1227 $\wedge \exists r \in m.m2av : \wedge r.bal \geq c$
1228 $\wedge r.val = v$
1229 $KS22WQ(v, c, WQ, S) \triangleq \forall a \in WQ : KS22WQa(v, c, a, S)$
1230 $KS22(v, c, S) \triangleq \exists WQ \in WeakQuorum : KS22WQ(v, c, WQ, S)$
1231 $KS2(v, b, S) \triangleq \exists c \in 0 \dots (b-1) : \wedge KS21(v, c, S)$
1232 $\wedge KS22(v, c, S)$

The following lemma asserts the obvious relation between *KnowsSafeAt* and the top-level definitions *KS1*, *KS2*, and *KSet*. The second conjunct is, of course, the primed version of the first. To understand why it is needed, see the discussion of *MsgsTypeLemmaPrime* below.

1240 LEMMA *KnowsSafeAtDef* \triangleq
1241 $\forall a, b, v :$
1242 $\wedge KnowsSafeAt(a, b, v) = (KS1(KSet(a, b)) \vee KS2(v, b, KSet(a, b)))$
1243 $\wedge KnowsSafeAt(a, b, v)' = (KS1(KSet(a, b)') \vee KS2(v, b, KSet(a, b)'))$
1244 BY DEF *KnowsSafeAt*, *KSet*, *KS11a*, *KS11*, *KS1*, *KS21BQa*,
1245 *KS21BQ*, *KS21*, *KS22WQa*, *KS22WQ*, *KS22*, *KS2*
1247 LEMMA *MsgsTypeLemma* \triangleq
1248 $\forall m \in msgs : \wedge (m.type = "1a") \equiv (m \in msgsOfType("1a"))$
1249 $\wedge (m.type = "1b") \equiv (m \in 1bmsgs)$
1250 $\wedge (m.type = "1c") \equiv (m \in 1cmsgs)$
1251 $\wedge (m.type = "2a") \equiv (m \in 2amsgs)$
1252 $\wedge (m.type = "2b") \equiv (m \in acceptorMsgsOfType("2b"))$
1253 $\langle 1 \rangle$ SUFFICES ASSUME NEW $m \in msgs$
1254 PROVE *MsgsTypeLemma*!(m)
1255 OBVIOUS
1256 $\langle 1 \rangle 1. (m \in msgsOfType("1a")) \Rightarrow (m.type = "1a")$
1257 BY DEF *msgsOfType*
1258 $\langle 1 \rangle 2. (m \in 1bmsgs) \Rightarrow (m.type = "1b")$
1259 $\langle 2 \rangle \forall mm : [type \mapsto "1b", acc \mapsto mm.acc, bal \mapsto mm.bal,$
1260 $mbal \mapsto mm.mbal, mval \mapsto mm.mval].type = "1b"$
1261 OBVIOUS
1262 $\langle 2 \rangle$ QED
1263 BY DEF *1bmsgs*, *1bRestrict*
1264 $\langle 1 \rangle 3. (m \in 1cmsgs) \Rightarrow (m.type = "1c")$

1265 BY DEF $1cmsgs, msgsOfType$
 1266 $\langle 1 \rangle 4. (m \in 2amsgs) \Rightarrow (m.type = "2a")$
 1267 BY DEF $2amsgs$
 1268 $\langle 1 \rangle 5. (m \in acceptorMsgsOfType("2b")) \Rightarrow (m.type = "2b")$
 1269 BY DEF $acceptorMsgsOfType, msgsOfType$
 1270 $\langle 1 \rangle 6.$ QED
 1271 BY $\langle 1 \rangle 1, \langle 1 \rangle 2, \langle 1 \rangle 3, \langle 1 \rangle 4, \langle 1 \rangle 5$ DEF $msgs$

The following lemma is the primed version of *MsgsTypeLemma*. That is, its statement is just the statement of *MsgsTypeLemma* primed. It follows from *MsgsTypeLemma* by the meta-theorem that if we can prove a state-predicate F as a (top-level) theorem, then we can deduce F' . A more general meta-theorem says that if we can prove a state predicate F that does not appear within the proof of an ASSUME /PROVE, then we can deduce F' . We expect this meta-theorem will be enshrined in a proof rule when temporal-logic reasoning is implemented in *TLAPS*. Until then, we must prove F' separately from F .

1284 LEMMA $MsgsTypeLemmaPrime \triangleq$
 1285 $\forall m \in msgs' : \wedge (m.type = "1a") \equiv (m \in msgsOfType("1a"))'$
 1286 $\wedge (m.type = "1b") \equiv (m \in 1bmsgs')$
 1287 $\wedge (m.type = "1c") \equiv (m \in 1cmsgs')$
 1288 $\wedge (m.type = "2a") \equiv (m \in 2amsgs')$
 1289 $\wedge (m.type = "2b") \equiv (m \in acceptorMsgsOfType("2b"))'$
 1290 $\langle 1 \rangle$ SUFFICES ASSUME NEW $m \in msgs'$
 1291 PROVE $MsgsTypeLemmaPrime!(m)$
 1292 OBVIOUS
 1293 $\langle 1 \rangle 1. (m \in msgsOfType("1a"))' \Rightarrow (m.type = "1a")$
 1294 BY DEF $msgsOfType$
 1295 $\langle 1 \rangle 2. (m \in 1bmsgs') \Rightarrow (m.type = "1b")$
 1296 $\langle 2 \rangle \forall mm : [type \mapsto "1b", acc \mapsto mm.acc, bal \mapsto mm.bal,$
 1297 $mbal \mapsto mm.mbal, mval \mapsto mm.mval].type = "1b"$
 1298 OBVIOUS
 1299 $\langle 2 \rangle$ QED
 1300 BY DEF $1bmsgs, 1bRestrict$
 1301 $\langle 1 \rangle 3. (m \in 1cmsgs') \Rightarrow (m.type = "1c")$
 1302 BY DEF $1cmsgs, msgsOfType$
 1303 $\langle 1 \rangle 4. (m \in 2amsgs') \Rightarrow (m.type = "2a")$
 1304 BY DEF $2amsgs$
 1305 $\langle 1 \rangle 5. (m \in acceptorMsgsOfType("2b"))' \Rightarrow (m.type = "2b")$
 1306 BY DEF $acceptorMsgsOfType, msgsOfType$
 1307 $\langle 1 \rangle 6.$ QED
 1308 BY $\langle 1 \rangle 1, \langle 1 \rangle 2, \langle 1 \rangle 3, \langle 1 \rangle 4, \langle 1 \rangle 5$ DEF $msgs$

The following lemma describes how $msgs$ is changed by the actions of the algorithm.

1314 LEMMA $MsgsLemma \triangleq$
 1315 $TypeOK \Rightarrow$
 1316 $\wedge \forall self \in Acceptor, b \in Ballot :$
 1317 $Phase1b(self, b) \Rightarrow$

1318 $msgs' = msgs \cup$
1319 $\{[type \mapsto "1b", acc \mapsto self, bal \mapsto b,$
1320 $mbal \mapsto maxVBal[self], mval \mapsto maxVVal[self]]\}$
1321 $\wedge \forall self \in Acceptor, b \in Ballot :$
1322 $Phase2av(self, b) \Rightarrow$
1323 $\vee msgs' = msgs$
1324 $\vee \exists v \in Value :$
1325 $\wedge [type \mapsto "1c", bal \mapsto b, val \mapsto v] \in msgs$
1326 $\wedge msgs' = msgs \cup \{[type \mapsto "2a", bal \mapsto b, val \mapsto v]\}$
1327 $\wedge \forall self \in Acceptor, b \in Ballot :$
1328 $Phase2b(self, b) \Rightarrow$
1329 $\exists v \in Value :$
1330 $\wedge \exists Q \in ByzQuorum :$
1331 $\forall a \in Q :$
1332 $\exists m \in sentMsgs("2av", b) : \wedge m.val = v$
1333 $\wedge m.acc = a$
1334 $\wedge msgs' = msgs \cup$
1335 $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\}$
1336 $\wedge bmsgs' = bmsgs \cup$
1337 $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\}$
1338 $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = v]$
1339 $\wedge \forall self \in Acceptor, b \in Ballot :$
1340 $LearnsSent(self, b) \Rightarrow$
1341 $\exists S \in \text{SUBSET } \{m \in msgsOfType("1c") : m.bal = b\} :$
1342 $msgs' = msgs \cup S$
1343 $\wedge \forall self \in Ballot :$
1344 $Phase1a(self) \Rightarrow$
1345 $msgs' = msgs \cup \{[type \mapsto "1a", bal \mapsto self]\}$
1346 $\wedge \forall self \in Ballot :$
1347 $Phase1c(self) \Rightarrow$
1348 $\exists S \in \text{SUBSET } [type : \{ "1c" \}, bal : \{ self \}, val : Value] :$
1349 $\wedge \forall m \in S :$
1350 $\exists a \in Acceptor : KnowsSafeAt(a, m.bal, m.val)$
1351 $\wedge msgs' = msgs \cup S$
1352 $\wedge \forall self \in FakeAcceptor : FakingAcceptor(self) \Rightarrow msgs' = msgs$
1353 $\langle 1 \rangle a. \text{ ASSUME NEW } S, bmsgs' = bmsgs \cup S$
1354 $\text{ PROVE } (\forall m \in S : m.type \neq "1a") \Rightarrow$
1355 $(msgsOfType("1a")' = msgsOfType("1a"))$
1356 $\text{ BY } \langle 1 \rangle a \text{ DEF } msgsOfType$
1357 $\langle 1 \rangle b. \text{ ASSUME NEW } S, bmsgs' = bmsgs \cup S$
1358 $\text{ PROVE } (\forall m \in S : m.type \neq "1b") \Rightarrow (1bmsgs' = 1bmsgs)$
1359 $\text{ BY } \langle 1 \rangle b \text{ DEF } 1bmsgs, 1bRestrict, acceptorMsgsOfType, msgsOfType$
1360 $\langle 1 \rangle c. \text{ ASSUME NEW } S, bmsgs' = bmsgs \cup S$
1361 $\text{ PROVE } (\forall m \in S : m.type \neq "1c") \wedge (knowsSent' = knowsSent)$
1362 $\Rightarrow (1cmsgs' = 1cmsgs)$

1363 $\langle 2 \rangle 1. (knowsSent' = knowsSent) \Rightarrow$
1364 $\quad \forall a \in \text{Acceptor} :$
1365 $\quad \forall b, v : KnowsSafeAt(a, b, v)' = KnowsSafeAt(a, b, v)$
1366 BY DEF *KnowsSafeAt*
1367 $\langle 2 \rangle 2. (knowsSent' = knowsSent) \Rightarrow$
1368 $\quad \forall b, v : (\exists a \in \text{Acceptor} : KnowsSafeAt(a, b, v))' \equiv$
1369 $\quad (\exists a \in \text{Acceptor} : KnowsSafeAt(a, b, v))$
1370 BY $\langle 2 \rangle 1$
1371 $\langle 2 \rangle 3. (\forall m \in S : m.type \neq "1c") \Rightarrow msgsOfType("1c")' = msgsOfType("1c")$
1372 BY $\langle 1 \rangle c, \langle 2 \rangle 3$ DEF *msgsOfType*
1373 $\langle 2 \rangle 4.$ QED
1374 BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3$ DEF *1cmsgs, KnowsSafeAt*
1375 $\langle 1 \rangle d.$ ASSUME NEW *S*, $bmsgs' = bmsgs \cup S$
1376 PROVE $(\forall m \in S : m.type \neq "2av") \Rightarrow (2amsgs' = 2amsgs)$
1377 $\langle 3 \rangle$ SUFFICES ASSUME $\forall m \in S : m.type \neq "2av"$
1378 PROVE $2amsgs' = 2amsgs$
1379 OBVIOUS
1380 $\langle 3 \rangle 1. \text{acceptorMsgsOfType}("2av")' = \text{acceptorMsgsOfType}("2av")$
1381 BY $\langle 1 \rangle d$ DEF *acceptorMsgsOfType, msgsOfType*
1382 $\langle 3 \rangle 2.$ QED
1383 BY $\langle 3 \rangle 1$ DEF *2amsgs*
1384 $\langle 1 \rangle e.$ ASSUME NEW *S*, $bmsgs' = bmsgs \cup S$
1385 PROVE $(\forall m \in S : m.type \neq "2b") \Rightarrow$
1386 $\quad (\text{acceptorMsgsOfType}("2b")' = \text{acceptorMsgsOfType}("2b"))$
1387 BY $\langle 1 \rangle e$ DEF *acceptorMsgsOfType, msgsOfType*
1388 $\langle 1 \rangle$ HAVE *TypeOK*
1389 $\langle 1 \rangle 1.$ ASSUME NEW *self* $\in \text{Acceptor}$, NEW *b* $\in \text{Ballot}$
1390 PROVE $\text{Phase1b}(\text{self}, b) \Rightarrow$
1391 $\quad msgs' = msgs \cup$
1392 $\quad \{[type \mapsto "1b", acc \mapsto \text{self}, bal \mapsto b,$
1393 $\quad \quad mbal \mapsto \text{maxVBal}[\text{self}], mval \mapsto \text{maxVVal}[\text{self}]]\}$
1394 $\langle 2 \rangle$ DEFINE $m \triangleq [type \mapsto "1b", acc \mapsto \text{self}, bal \mapsto b,$
1395 $\quad m2av \mapsto 2avSent[\text{self}],$
1396 $\quad mbal \mapsto \text{maxVBal}[\text{self}], mval \mapsto \text{maxVVal}[\text{self}]]$
1397 $\langle 2 \rangle$ SUFFICES ASSUME $\text{Phase1b}(\text{self}, b)$
1398 PROVE $msgs' = msgs \cup \{1bRestrict(m)\}$
1399 BY DEF *1bRestrict*
1400 $\langle 2 \rangle 1. bmsgs' = bmsgs \cup \{m\}$
1401 $\langle 3 \rangle 1. [type \mapsto "1b", bal \mapsto b, acc \mapsto \text{self}, m2av \mapsto 2avSent[\text{self}],$
1402 $\quad mbal \mapsto \text{maxVBal}[\text{self}], mval \mapsto \text{maxVVal}[\text{self}]]$
1403 $\quad = m$
1404 The provers seem to be really bad at equality of records,
1405 so I had to jump through hoops to get it to prove this
1406 trivial result.
1407 $\langle 4 \rangle$ DEFINE $a0 \triangleq "1b"$

1408 $a1 \triangleq 2avSent[self]$
1409 $a3 \triangleq maxVBal[self]$
1410 $a4 \triangleq maxVVal[self]$
1411 $a5 \triangleq b$
1412 $a6 \triangleq self$
1413 $\langle 4 \rangle$ HIDE DEF $a0, a1, a3, a4, a5, a6$
1414 $\langle 4 \rangle 1.$ $[type \mapsto a0, bal \mapsto a5, acc \mapsto a6,$
1415 $m2av \mapsto a1, mbal \mapsto a3, mval \mapsto a4]$
1416 $=$
1417 $[type \mapsto a0, acc \mapsto a6, bal \mapsto a5,$
1418 $m2av \mapsto a1, mbal \mapsto a3, mval \mapsto a4]$
1419 OBVIOUS It takes Isabelle 1 – 1/2 minutes to prove this.
1420 $\langle 4 \rangle$ USE DEF $a0, a1, a3, a4, a5, a6$
1421 $\langle 4 \rangle 2.$ QED
1422 BY $\langle 4 \rangle 1$
1423 $\langle 3 \rangle$ HIDE DEF m
1424 $\langle 3 \rangle 2.$ QED
1425 BY $\langle 3 \rangle 1$ DEF $Phase1b$
1426 $\langle 2 \rangle 2. \wedge m.type = "1b"$
1427 $\wedge m.acc = self$
1428 OBVIOUS
1429 $\langle 2 \rangle$ HIDE DEF m
1430 $\langle 2 \rangle 3.$ $acceptorMsgsOfType("1b")' = acceptorMsgsOfType("1b") \cup \{m\}$
1431 BY $\langle 2 \rangle 1, \langle 2 \rangle 2$ DEF $acceptorMsgsOfType, msgsOfType$
1432 $\langle 2 \rangle 4.$ $1bmsgs' = 1bmsgs \cup \{1bRestrict(m)\}$
1433 BY $\langle 2 \rangle 3$ DEF $1bmsgs$
1434 $\langle 2 \rangle 5.$ $knowsSent' = knowsSent$
1435 BY DEF $Phase1b$
1436 $\langle 2 \rangle 6. \wedge msgsOfType("1a")' = msgsOfType("1a")$
1437 $\wedge 1cmsgs' = 1cmsgs$
1438 $\wedge 2ams' = 2ams$
1439 $\wedge acceptorMsgsOfType("2b")' = acceptorMsgsOfType("2b")$
1440 $\langle 3 \rangle$ DEFINE $S \triangleq \{m\}$
1441 $\langle 3 \rangle \wedge bmsgs' = bmsgs \cup S$
1442 $\wedge \forall mm \in S : mm.type = "1b"$
1443 BY $\langle 2 \rangle 1, \langle 2 \rangle 2$
1444 $\langle 3 \rangle$ HIDE DEF S
1445 $\langle 3 \rangle$ QED
1446 BY $\langle 2 \rangle 5, \langle 1 \rangle a, \langle 1 \rangle c, \langle 1 \rangle d, \langle 1 \rangle e$
1447 $\langle 2 \rangle 7.$ QED
1448 BY $\langle 2 \rangle 4, \langle 2 \rangle 6$ DEF $msgs$
1450 $\langle 1 \rangle 2.$ ASSUME NEW $self \in Acceptor$, NEW $b \in Ballot$
1451 PROVE $Phase2av(self, b) \Rightarrow$
1452 $\vee msgs' = msgs$

```

1453       $\vee \exists v \in \text{Value} :$ 
1454       $\wedge [type \mapsto "1c", bal \mapsto b, val \mapsto v] \in msgs$ 
1455       $\wedge msgs' = msgs \cup$ 
1456       $\{[type \mapsto "2a", bal \mapsto b, val \mapsto v]\}$ 
1457   $\langle 2 \rangle$  HAVE Phase2av(self, b)
1458   $\langle 2 \rangle$  1. PICK  $m \in \text{sentMsgs}("1c", b) :$ 
1459       $\wedge \text{KnowsSafeAt}(\text{self}, b, m.val)$ 
1460       $\wedge bmsgs' = bmsgs \cup$ 
1461       $\{[type \mapsto "2av", bal \mapsto b, val \mapsto m.val, acc \mapsto self]\}$ 
1462      BY DEF Phase2av
1463   $\langle 2 \rangle$  2.  $m = [type \mapsto "1c", bal \mapsto b, val \mapsto m.val]$ 
1464   $\langle 3 \rangle$  1.  $\wedge m \in bmsgs$ 
1465       $\wedge m.type = "1c"$ 
1466       $\wedge m.bal = b$ 
1467      BY DEF sentMsgs
1468   $\langle 3 \rangle$  2.  $m \in BMessage$ 
1469      BY  $\langle 3 \rangle$  1 DEF TypeOK
1470   $\langle 3 \rangle$  3.  $m \in 1cMessage$ 
1471      BY  $\langle 3 \rangle$  1,  $\langle 3 \rangle$  2, BMessageLemma
1472   $\langle 3 \rangle$  4.  $m = [type \mapsto m.type, bal \mapsto m.bal, val \mapsto m.val]$ 
1473      BY  $\langle 3 \rangle$  3 DEF 1cMessage
1474   $\langle 3 \rangle$  5. QED
1475      BY  $\langle 3 \rangle$  1,  $\langle 3 \rangle$  4

1477   $\langle 2 \rangle$  DEFINE  $ma \triangleq [type \mapsto "2a", bal \mapsto b, val \mapsto m.val]$ 
1478   $\langle 2 \rangle$  3. SUFFICES ASSUME  $msgs' \neq msgs$ 
1479      PROVE  $\wedge m \in msgs$ 
1480       $\wedge msgs' = msgs \cup \{ma\}$ 
1481   $\langle 3 \rangle$  1.  $m.val \in \text{Value}$ 
1482   $\langle 4 \rangle$  1.  $\wedge m \in bmsgs$ 
1483       $\wedge m.type = "1c"$ 
1484      BY DEF sentMsgs
1485   $\langle 4 \rangle$  2.  $m \in BMessage$ 
1486      BY  $\langle 4 \rangle$  1 DEF TypeOK
1487   $\langle 4 \rangle$  3.  $m \in 1cMessage$ 
1488      BY  $\langle 4 \rangle$  1,  $\langle 4 \rangle$  2, BMessageLemma
1489   $\langle 4 \rangle$  4. QED
1490      BY  $\langle 4 \rangle$  3 DEF 1cMessage
1491   $\langle 3 \rangle$  2. QED
1492      BY  $\langle 3 \rangle$  1,  $\langle 2 \rangle$  2

1494   $\langle 2 \rangle$  4.  $m \in msgs$ 
1495   $\langle 3 \rangle$  1.  $\wedge m \in bmsgs$ 
1496       $\wedge m.type = "1c"$ 
1497       $\wedge m.bal = b$ 

```

```

1498     BY DEF sentMsgs
1499     ⟨3⟩2.  $m \in \text{msgsOfType}(\text{"1c"})$ 
1500     BY ⟨3⟩1 DEF msgsOfType
1501     ⟨3⟩3.  $\text{KnowsSafeAt}(\text{self}, m.\text{bal}, m.\text{val})$ 
1502     BY ⟨2⟩1, ⟨3⟩1
1503     ⟨3⟩4.  $\exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.\text{bal}, m.\text{val})$ 
1504     BY ⟨3⟩3
1505     ⟨3⟩5.  $m \in \text{1cmsgs}$ 
1506     BY ⟨2⟩2, ⟨3⟩1, ⟨3⟩2, ⟨3⟩4 DEF 1cmsgs
1507     ⟨3⟩6. QED
1508     BY ⟨3⟩5 DEF msgs
1509     ⟨2⟩5.  $\text{msgs}' = \text{msgs} \cup \{ma\}$ 
1510     ⟨3⟩ DEFINE  $mb \triangleq [\text{type} \mapsto \text{"2av"}, \text{bal} \mapsto b, \text{val} \mapsto m.\text{val}, \text{acc} \mapsto \text{self}]$ 
1511            $S \triangleq \{mb\}$ 
1512     ⟨3⟩1.  $\wedge \text{bmsgs}' = \text{bmsgs} \cup S$ 
1513            $\wedge \forall mm \in S : mm.\text{type} = \text{"2av"}$ 
1514     BY ⟨2⟩1
1515     ⟨3⟩2.  $\text{knowsSent}' = \text{knowsSent}$ 
1516     BY DEF Phase2av
1517     ⟨3⟩3.  $\wedge \text{msgsOfType}(\text{"1a"})' = \text{msgsOfType}(\text{"1a"})$ 
1518            $\wedge \text{1bmsgs}' = \text{1bmsgs}$ 
1519            $\wedge \text{1cmsgs}' = \text{1cmsgs}$ 
1520            $\wedge \text{acceptorMsgsOfType}(\text{"2b"})' = \text{acceptorMsgsOfType}(\text{"2b"})$ 
1521     ⟨4⟩ HIDE DEF S
1522     ⟨4⟩ QED
1523     BY ⟨3⟩1, ⟨3⟩2, ⟨1⟩a, ⟨1⟩b, ⟨1⟩c, ⟨1⟩e
1524     ⟨3⟩4.  $2\text{amsgs} \subseteq 2\text{amsgs}'$ 
1525     ⟨4⟩1. SUFFICES ASSUME NEW  $m1 \in [\text{type} : \{\text{"2a"}\}, \text{bal} : \text{Ballot}, \text{val} : \text{Value}]$ ,
1526            $\exists Q \in \text{Quorum} :$ 
1527            $\forall a \in Q :$ 
1528            $\exists m2av \in \text{acceptorMsgsOfType}(\text{"2av"}) :$ 
1529            $\wedge m2av.\text{acc} = a$ 
1530            $\wedge m2av.\text{bal} = m1.\text{bal}$ 
1531            $\wedge m2av.\text{val} = m1.\text{val}$ 
1532     PROVE  $\exists Q \in \text{Quorum} :$ 
1533            $\forall a \in Q :$ 
1534            $\exists m2av \in \text{acceptorMsgsOfType}(\text{"2av"})' :$ 
1535            $\wedge m2av.\text{acc} = a$ 
1536            $\wedge m2av.\text{bal} = m1.\text{bal}$ 
1537            $\wedge m2av.\text{val} = m1.\text{val}$ 
1538     BY DEF 2amsgs
1539     ⟨4⟩2. PICK  $Q \in \text{Quorum} :$ 
1540            $\forall a \in Q :$ 
1541            $\exists m2av \in \text{acceptorMsgsOfType}(\text{"2av"}) :$ 
1542            $\wedge m2av.\text{acc} = a$ 

```

1543 $\wedge m2av.bal = m1.bal$
1544 $\wedge m2av.val = m1.val$
1545 BY $\langle 4 \rangle 1$
1546 $\langle 4 \rangle$ SUFFICES ASSUME NEW $a \in Q$
1547 PROVE $\exists m2av \in \text{acceptorMsgsOfType}("2av")'$:
1548 $\wedge m2av.acc = a$
1549 $\wedge m2av.bal = m1.bal$
1550 $\wedge m2av.val = m1.val$
1551 OBVIOUS
1552 $\langle 4 \rangle 3. \exists m2av \in \text{acceptorMsgsOfType}("2av")'$:
1553 $\wedge m2av.acc = a$
1554 $\wedge m2av.bal = m1.bal$
1555 $\wedge m2av.val = m1.val$
1556 BY $\langle 4 \rangle 2$
1557 $\langle 4 \rangle 4. \text{acceptorMsgsOfType}("2av") \subseteq \text{acceptorMsgsOfType}("2av")'$
1558 $\langle 5 \rangle 1. \text{msgsOfType}("2av") \subseteq \text{msgsOfType}("2av")'$
1559 BY $\langle 3 \rangle 1$ DEF msgsOfType
1560 $\langle 5 \rangle 2.$ QED
1561 BY $\langle 5 \rangle 1$ DEF $\text{acceptorMsgsOfType}$
1562 $\langle 4 \rangle 5.$ QED
1563 BY $\langle 4 \rangle 3, \langle 4 \rangle 4$
1564 $\langle 3 \rangle 5. \text{msgs} \subseteq \text{msgs}'$
1565 BY $\langle 3 \rangle 3, \langle 3 \rangle 4$ DEF msgs
1566 $\langle 3 \rangle 6.$ ASSUME NEW $mp \in \text{msgs}', mp \notin \text{msgs}$
1567 PROVE $mp = ma$
1568 $\langle 4 \rangle 1. mp \in 2\text{amsgs}' \wedge mp \notin 2\text{amsgs}$
1569 BY $\langle 3 \rangle 3, \langle 3 \rangle 6$ DEF msgs
1570 $\langle 4 \rangle 2.$ PICK $Q \in \text{Quorum}$:
1571 $\forall a \in Q$:
1572 $\exists m2av \in \text{acceptorMsgsOfType}("2av")'$:
1573 $\wedge m2av.acc = a$
1574 $\wedge m2av.bal = mp.bal$
1575 $\wedge m2av.val = mp.val$
1576 BY $\langle 4 \rangle 1$ DEF 2amsgs
1577 $\langle 4 \rangle 3. \neg \forall a \in Q$:
1578 $\exists m2av \in \text{acceptorMsgsOfType}("2av")'$:
1579 $\wedge m2av.acc = a$
1580 $\wedge m2av.bal = mp.bal$
1581 $\wedge m2av.val = mp.val$
1582 BY $\langle 4 \rangle 1$ DEF 2amsgs
1583 $\langle 4 \rangle 4.$ PICK $a \in Q$:
1584 $\neg \exists m2av \in \text{acceptorMsgsOfType}("2av")'$:
1585 $\wedge m2av.acc = a$
1586 $\wedge m2av.bal = mp.bal$
1587 $\wedge m2av.val = mp.val$

1588 BY $\langle 4 \rangle 3$
1589 $\langle 4 \rangle 5$. PICK $m2av \in \text{acceptorMsgsOfType}(\text{"2a"})'$:
1590 $\wedge m2av.\text{acc} = a$
1591 $\wedge m2av.\text{bal} = mp.\text{bal}$
1592 $\wedge m2av.\text{val} = mp.\text{val}$
1593 BY $\langle 4 \rangle 2$
1594 $\langle 4 \rangle 6$. $m2av \notin \text{acceptorMsgsOfType}(\text{"2a"})$
1595 BY $\langle 4 \rangle 5$, $\langle 4 \rangle 4$
1596 $\langle 4 \rangle 7$. $m2av = mb$
1597 $\langle 5 \rangle 1$. $\text{acceptorMsgsOfType}(\text{"2a"})' = \text{acceptorMsgsOfType}(\text{"2a"}) \cup \{mb\}$
1598 BY $\langle 3 \rangle 1$, $mb.\text{type} = \text{"2a"}$ DEF $\text{acceptorMsgsOfType}$, msgsOfType
1599 $\langle 5 \rangle 2$. QED
1600 BY $\langle 4 \rangle 6$, $\langle 5 \rangle 1$
1601 $\langle 4 \rangle 8$. $mp = [type \mapsto \text{"2a"}, bal \mapsto mp.bal, val \mapsto mp.val]$
1602 $\langle 5 \rangle 1$. $mp \in [type : \{\text{"2a"}\}, bal : \text{Ballot}, val : \text{Value}]$
1603 BY $\langle 4 \rangle 1$ DEF 2amsgs
1604 $\langle 5 \rangle 2$. QED
1605 BY $\langle 5 \rangle 1$
1606 $\langle 4 \rangle 9$. QED
1607 BY $\langle 4 \rangle 8$, $\langle 4 \rangle 7$, $\langle 4 \rangle 5$
1608 $\langle 3 \rangle 7$. QED
1609 BY $\langle 2 \rangle 3$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$
1610 $\langle 2 \rangle 6$. QED
1611 BY $\langle 2 \rangle 4$, $\langle 2 \rangle 5$

1613 $\langle 1 \rangle 3$. ASSUME NEW $self \in \text{Acceptor}$, NEW $b \in \text{Ballot}$
1614 PROVE $\text{Phase2b}(self, b) \Rightarrow$
1615 $\exists v \in \text{Value} :$
1616 $\wedge \exists Q \in \text{ByzQuorum} :$
1617 $\forall a \in Q :$
1618 $\exists m \in \text{sentMsgs}(\text{"2a"}, b) : \wedge m.\text{val} = v$
1619 $\wedge m.\text{acc} = a$
1620 $\wedge \text{msgs}' = \text{msgs} \cup$
1621 $\{[type \mapsto \text{"2b"}, acc \mapsto self, bal \mapsto b,$
1622 $val \mapsto v]$
1623 $\}$
1624 $\wedge \text{bmsgs}' = \text{bmsgs} \cup$
1625 $\{[type \mapsto \text{"2b"}, acc \mapsto self, bal \mapsto b, val \mapsto v]\}$
1626 $\wedge \text{maxVVal}' = [\text{maxVVal} \text{ EXCEPT } ![self] = v]$
1627 $\langle 2 \rangle$ HAVE $\text{Phase2b}(self, b)$
1628 $\langle 2 \rangle 1$. PICK $v \in \text{Value} :$
1629 $\wedge \exists Q \in \text{ByzQuorum} :$
1630 $\forall a \in Q :$
1631 $\exists m \in \text{sentMsgs}(\text{"2a"}, b) : \wedge m.\text{val} = v$
1632 $\wedge m.\text{acc} = a$

```

1633       $\wedge bmsgs' =$ 
1634       $bmsgs \cup$ 
1635       $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\}$ 
1636       $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = v]$ 
1637      BY DEF Phase2b
1638       $\langle 2 \rangle$  DEFINE  $bm \triangleq [type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]$ 
1639       $\langle 2 \rangle 2. \wedge msgsOfType("1a")' = msgsOfType("1a")$ 
1640       $\wedge 1bmsgs' = 1bmsgs$ 
1641       $\wedge 1cmsgs' = 1cmsgs$ 
1642       $\wedge 2amsgs' = 2amsgs$ 
1643       $\langle 3 \rangle$  DEFINE  $S \triangleq \{bm\}$ 
1644       $\langle 3 \rangle \wedge bmsgs' = bmsgs \cup S$ 
1645       $\wedge \forall m \in S : m.type = "2b"$ 
1646      BY  $\langle 2 \rangle 1, bm.type = "2b"$ 
1647       $\langle 3 \rangle$  HIDE DEF  $S$ 
1648       $\langle 3 \rangle$  QED
1649      BY  $\langle 1 \rangle a, \langle 1 \rangle b, knowsSent' = knowsSent, \langle 1 \rangle c, \langle 1 \rangle d$  DEF Phase2b
1650       $\langle 2 \rangle 3. acceptorMsgsOfType("2b")' = acceptorMsgsOfType("2b") \cup \{bm\}$ 
1651       $\langle 3 \rangle 0. acceptorMsgsOfType("2b") \subseteq acceptorMsgsOfType("2b")'$ 
1652      BY  $\langle 2 \rangle 1$  DEF acceptorMsgsOfType, msgsOfType
1653       $\langle 3 \rangle 1. bm \in acceptorMsgsOfType("2b")'$ 
1654      BY  $\langle 2 \rangle 1$  DEF acceptorMsgsOfType, msgsOfType
1655       $\langle 3 \rangle 3. \text{ASSUME NEW } m \in acceptorMsgsOfType("2b")', m \neq bm$ 
1656      PROVE  $m \in acceptorMsgsOfType("2b")$ 
1657       $\langle 4 \rangle 1. \wedge m \in bmsgs'$ 
1658       $\wedge m.type = "2b"$ 
1659       $\wedge m.acc \in Acceptor$ 
1660      BY DEF acceptorMsgsOfType, msgsOfType
1661       $\langle 4 \rangle a. bmsgs' = bmsgs \cup \{bm\}$ 
1662      BY  $\langle 2 \rangle 1$ 
1663       $\langle 4 \rangle 2. m \in bmsgs$ 
1664      BY  $\langle 4 \rangle 1, \langle 2 \rangle 1, bmsgs' = bmsgs \cup \{bm\}, \langle 3 \rangle 3$ 
1665       $\langle 4 \rangle 3. \text{QED}$ 
1666      BY  $\langle 4 \rangle 1, \langle 4 \rangle 2$  DEF acceptorMsgsOfType, msgsOfType
1667       $\langle 3 \rangle 5. \text{QED}$ 
1668      BY  $\langle 3 \rangle 0, \langle 3 \rangle 1, \langle 3 \rangle 3$ 

1670       $\langle 2 \rangle 4. msgs' = msgs \cup \{bm\}$ 
1671      BY  $\langle 2 \rangle 2, \langle 2 \rangle 3$  DEF msgs
1672       $\langle 2 \rangle 5. \text{QED}$ 
1673      BY  $\langle 2 \rangle 1, \langle 2 \rangle 4, \langle 2 \rangle 5$ 

1675       $\langle 1 \rangle 4. \text{ASSUME NEW } self \in Acceptor, \text{NEW } b \in Ballot$ 
1676      PROVE  $LearnsSent(self, b) \Rightarrow$ 
1677       $\exists S \in \text{SUBSET } \{m \in msgsOfType("1c") : m.bal = b\} :$ 

```



```

1678                                      $msgs' = msgs \cup S$ 
1679  $\langle 2 \rangle$  HAVE LearnsSent(self, b)
1680  $\langle 2 \rangle 1.$   $\wedge msgsOfType("1a")' = msgsOfType("1a")$ 
1681            $\wedge 1bmsgs' = 1bmsgs$ 
1682            $\wedge 2amsgs' = 2amsgs$ 
1683            $\wedge acceptorMsgsOfType("2b")' = acceptorMsgsOfType("2b")$ 
1684  $\langle 3 \rangle 1.$   $\wedge bmsgs' = bmsgs \cup \{ \}$ 
1685            $\wedge \forall m \in \{ \} : m.type = "x"$ 
1686       BY DEF LearnsSent
1687  $\langle 3 \rangle 2. \langle 2 \rangle 1!1$ 
1688       BY  $\langle 3 \rangle 1, \langle 1 \rangle a$ 
1689  $\langle 3 \rangle 3. \langle 2 \rangle 1!2$ 
1690       BY  $\langle 3 \rangle 1, \langle 1 \rangle b$ 
1691  $\langle 3 \rangle 4. \langle 2 \rangle 1!3$ 
1692       BY  $\langle 3 \rangle 1, \langle 1 \rangle d$ 
1693  $\langle 3 \rangle 5. \langle 2 \rangle 1!4$ 
1694       BY  $\langle 3 \rangle 1, \langle 1 \rangle e$ 
1695  $\langle 3 \rangle 6.$  QED
1696       BY  $\langle 3 \rangle 2, \langle 3 \rangle 3, \langle 3 \rangle 4, \langle 3 \rangle 5$ 
1697  $\langle 2 \rangle 2. \wedge 1cmsgs \subseteq 1cmsgs'$ 
1698            $\wedge \forall m \in 1cmsgs' \setminus 1cmsgs :$ 
1699              $m \in msgsOfType("1c") \wedge m.bal = b$ 
1700  $\langle 3 \rangle 1.$   $bmsgs' = bmsgs$ 
1701       BY DEF LearnsSent
1702  $\langle 3 \rangle 2.$  PICK  $S \in \text{SUBSET } sentMsgs("1b", b) :$ 
1703            $knowsSent' = [knowsSent \text{ EXCEPT } ![self] = knowsSent[self] \cup S]$ 
1704       BY DEF LearnsSent
1705  $\langle 3 \rangle 3.$  ASSUME NEW  $m \in 1cmsgs$ 
1706           PROVE  $m \in 1cmsgs'$ 
1707        $\langle 4 \rangle 1. \forall a \in \text{Acceptor} : knowsSent[a] \subseteq knowsSent'[a]$ 
1708       BY  $\langle 3 \rangle 2$  DEF TypeOK
1709        $\langle 4 \rangle 2. \forall a \in \text{Acceptor} :$ 
1710            $\forall bb, v : KnowsSafeAt(a, bb, v) \Rightarrow KnowsSafeAt(a, bb, v)'$ 
1711        $\langle 5 \rangle$  SUFFICES ASSUME NEW  $a \in \text{Acceptor}$ , NEW  $bb$ , NEW  $v$ ,
1712            $KnowsSafeAt(a, bb, v)$ 
1713           PROVE  $KnowsSafeAt(a, bb, v)'$ 
1714       OBVIOUS
1715        $\langle 5 \rangle 1. \forall T, U : (T \subseteq U) \Rightarrow \wedge KS1(T) \Rightarrow KS1(U)$ 
1716            $\wedge KS2(v, bb, T) \Rightarrow KS2(v, bb, U)$ 
1717        $\langle 6 \rangle$  SUFFICES ASSUME NEW  $T$ , NEW  $U$ ,  $T \subseteq U$ 
1718           PROVE  $\langle 5 \rangle 1!(T, U)!2$ 
1719       OBVIOUS
1720        $\langle 6 \rangle 1. \langle 5 \rangle 1!(T, U)!2!1$ 
1721        $\langle 7 \rangle$  SUFFICES ASSUME NEW  $BQ$ 
1722           PROVE  $KS11(BQ, T) \Rightarrow KS11(BQ, U)$ 

```

```

1723         BY DEF KS1
1724     ⟨7⟩ SUFFICES ASSUME NEW ac
1725         PROVE  $KS11a(ac, T) \Rightarrow KS11a(ac, U)$ 
1726         BY DEF KS11
1727     ⟨7⟩ QED
1728         BY DEF KS11a
1729     ⟨6⟩2.⟨5⟩1!(T, U)!2
1730     ⟨7⟩1 ASSUME NEW c
1731         PROVE  $KS21(v, c, T) \Rightarrow KS21(v, c, U)$ 
1732     ⟨8⟩ SUFFICES ASSUME NEW BQ
1733         PROVE  $KS21BQ(v, c, BQ, T) \Rightarrow KS21BQ(v, c, BQ, U)$ 
1734         BY DEF KS21
1735     ⟨8⟩ SUFFICES ASSUME NEW ac
1736         PROVE  $KS21BQa(v, c, ac, T) \Rightarrow KS21BQa(v, c, ac, U)$ 
1737         BY DEF KS21BQ
1738     ⟨8⟩ QED
1739         BY DEF KS21BQa
1740     ⟨7⟩2 ASSUME NEW c
1741         PROVE  $KS22(v, c, T) \Rightarrow KS22(v, c, U)$ 
1742     ⟨8⟩ SUFFICES ASSUME NEW WQ
1743         PROVE  $KS22WQ(v, c, WQ, T) \Rightarrow KS22WQ(v, c, WQ, U)$ 
1744         BY DEF KS22
1745     ⟨8⟩ SUFFICES ASSUME NEW ac
1746         PROVE  $KS22WQa(v, c, ac, T) \Rightarrow KS22WQa(v, c, ac, U)$ 
1747         BY DEF KS22WQ
1748     ⟨8⟩ QED
1749         BY DEF KS22WQa
1750     ⟨7⟩3. QED
1751         BY ⟨7⟩1, ⟨7⟩2 DEF KS2
1752     ⟨6⟩3. QED
1753         BY ⟨6⟩1, ⟨6⟩2
1754     ⟨5⟩2.  $KSet(a, bb) \subseteq KSet(a, bb)'$ 
1755         BY ⟨4⟩1 DEF KSet
1756     ⟨5⟩3. QED
1757         BY ⟨5⟩1, ⟨5⟩2, KnowsSafeAtDef
1758     ⟨4⟩3.  $msgsOfType("1c")' = msgsOfType("1c")$ 
1759         BY DEF msgsOfType, LearnsSent
1760     ⟨4⟩4. QED
1761         BY ⟨4⟩2, ⟨4⟩3 DEF 1cmsgs
1762     ⟨3⟩4. ASSUME NEW  $m \in 1cmsgs', m \notin 1cmsgs$ 
1763         PROVE  $m \in msgsOfType("1c") \wedge m.bal = b$ 
1764     ⟨4⟩1.  $m \in msgsOfType("1c")$ 
1765         BY DEF 1cmsgs, msgsOfType, LearnsSent
1766     ⟨4⟩2. PICK  $a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)'$ 
1767         BY DEF 1cmsgs

```

1768 $\langle 4 \rangle 3. \neg \text{KnowsSafeAt}(a, m.\text{bal}, m.\text{val})$
1769 BY $\langle 3 \rangle 4, \langle 4 \rangle 1$ DEF 1cmsgs
1770 $\langle 4 \rangle 4. \forall aa \in \text{Acceptor}, bb \in \text{Ballot} :$
1771 $\quad \forall mm \in \text{KSet}(aa, bb)' :$
1772 $\quad \quad mm \notin \text{KSet}(aa, bb) \Rightarrow bb = b$
1773 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $aa \in \text{Acceptor},$
1774 $\quad \quad \quad \text{NEW } bb \in \text{Ballot},$
1775 $\quad \quad \quad \text{NEW } mm \in \text{KSet}(aa, bb)',$
1776 $\quad \quad \quad mm \notin \text{KSet}(aa, bb)$
1777 PROVE $bb = b$
1778 OBVIOUS
1779 $\langle 5 \rangle 2.$ ASSUME NEW $m1 \in \text{knowsSent}[aa]', m1 \notin \text{knowsSent}[aa]$
1780 PROVE $m1.\text{bal} = b$
1781 $\langle 6 \rangle 1. \text{knowsSent}' = [\text{knowsSent} \text{ EXCEPT } ![self] = \text{knowsSent}[self] \cup S]$
1782 BY DEF LearnsSent
1783 $\langle 6 \rangle 2.$ CASE $aa \neq self$
1784 BY $\langle 6 \rangle 2, \langle 5 \rangle 2$ DEF $\text{TypeOK}, \text{LearnsSent}$
1785 $\langle 6 \rangle 3.$ CASE $aa = self$
1786 BY $\langle 6 \rangle 1, \langle 6 \rangle 3, \langle 5 \rangle 2$ DEF $\text{TypeOK}, \text{sentMsgs}$
1787 $\langle 6 \rangle 4.$ QED
1788 BY $\langle 6 \rangle 2, \langle 6 \rangle 3$
1789 $\langle 5 \rangle 3.$ QED
1790 BY $\langle 5 \rangle 1, \langle 5 \rangle 2$ DEF KSet
1791 $\langle 4 \rangle 5. m.\text{bal} \in \text{Ballot}$
1792 BY $\langle 4 \rangle 1, \text{BMessageLemma}$ DEF $1\text{cMessage}, \text{msgsOfType}, \text{TypeOK}$
1793 $\langle 4 \rangle 7.$ CASE $\text{KS1}(\text{KSet}(a, m.\text{bal})') \wedge \neg \text{KS1}(\text{KSet}(a, m.\text{bal}))$
1794 $\langle 5 \rangle 1.$ PICK $BQ \in \text{ByzQuorum} : \text{KS11}(BQ, \text{KSet}(a, m.\text{bal})')$
1795 BY $\langle 4 \rangle 7$ DEF KS1
1796 $\langle 5 \rangle 2. \neg \text{KS11}(BQ, \text{KSet}(a, m.\text{bal}))$
1797 BY $\langle 4 \rangle 7$ DEF KS1
1798 $\langle 5 \rangle 3.$ PICK $aa \in BQ : \neg \text{KS11a}(aa, \text{KSet}(a, m.\text{bal}))$
1799 BY $\langle 5 \rangle 2$ DEF KS11
1800 $\langle 5 \rangle 4. \text{KS11a}(aa, \text{KSet}(a, m.\text{bal})')$
1801 BY $\langle 5 \rangle 1$ DEF KS11
1802 $\langle 5 \rangle 5.$ PICK $mm \in \text{KSet}(a, m.\text{bal})' : mm.\text{acc} = aa \wedge mm.\text{mbal} = -1$
1803 BY $\langle 5 \rangle 4$ DEF KS11a
1804 $\langle 5 \rangle 6. mm \notin \text{KSet}(a, m.\text{bal})$
1805 BY $\langle 5 \rangle 5, \langle 5 \rangle 3$ DEF KS11a
1806 $\langle 5 \rangle 7. m.\text{bal} = b$
1807 BY $\langle 4 \rangle 4, \langle 4 \rangle 5, \langle 5 \rangle 5, \langle 5 \rangle 6$
1808 $\langle 5 \rangle 8.$ QED
1809 BY $\langle 4 \rangle 1, \langle 5 \rangle 7$
1810 $\langle 4 \rangle 8.$ CASE $\text{KS2}(m.\text{val}, m.\text{bal}, \text{KSet}(a, m.\text{bal})') \wedge \neg \text{KS2}(m.\text{val}, m.\text{bal}, \text{KSet}(a, m.\text{bal}))$
1811 $\langle 5 \rangle 1.$ PICK $c \in 0 \dots (m.\text{bal} - 1) : \wedge \text{KS21}(m.\text{val}, c, \text{KSet}(a, m.\text{bal}))'$
1812 $\quad \quad \quad \wedge \text{KS22}(m.\text{val}, c, \text{KSet}(a, m.\text{bal}))'$

1813 BY $\langle 4 \rangle 8$ DEF $KS2$
 1814 $\langle 5 \rangle 2$. CASE $\neg KS21(m.val, c, KSet(a, m.bal))$
 1815 $\langle 6 \rangle 1$. PICK $BQ \in ByzQuorum : KS21BQ(m.val, c, BQ, KSet(a, m.bal))'$
 1816 BY $\langle 5 \rangle 1$ DEF $KS21$
 1817 $\langle 6 \rangle 2$. PICK $aa \in BQ :$
 1818 $\neg \exists mm \in KSet(a, m.bal) : \wedge mm.acc = aa$
 1819 $\wedge mm.mbal \leq c$
 1820 $\wedge (mm.mbal = c) \Rightarrow (mm.mval = m.val)$
 1821 BY $\langle 5 \rangle 2$ DEF $KS21, KS21BQ, KS21BQa$
 1822 $\langle 6 \rangle 3$. PICK $mm \in KSet(a, m.bal)' : \wedge mm.acc = aa$
 1823 $\wedge mm.mbal \leq c$
 1824 $\wedge (mm.mbal = c) \Rightarrow (mm.mval = m.val)$
 1825 BY $\langle 6 \rangle 1$ DEF $KS21BQ, KS21BQa$
 1826 $\langle 6 \rangle 4$. $mm \notin KSet(a, m.bal)$
 1827 BY $\langle 6 \rangle 2, \langle 6 \rangle 3$
 1828 $\langle 6 \rangle 5$. $mm.bal = m.bal$
 1829 BY DEF $KSet$
 1830 $\langle 6 \rangle 6$. QED
 1831 BY $\langle 6 \rangle 4, \langle 6 \rangle 5, \langle 4 \rangle 4, \langle 4 \rangle 5, \langle 4 \rangle 1$
 1832 $\langle 5 \rangle 3$. CASE $\neg KS22(m.val, c, KSet(a, m.bal))$
 1833 $\langle 6 \rangle 1$. PICK $WQ \in WeakQuorum : KS22WQ(m.val, c, WQ, KSet(a, m.bal))'$
 1834 BY $\langle 5 \rangle 1$ DEF $KS22$
 1835 $\langle 6 \rangle 2$. PICK $aa \in WQ :$
 1836 $\neg \exists mm \in KSet(a, m.bal) : \wedge mm.acc = aa$
 1837 $\wedge \exists r \in mm.m2av :$
 1838 $\wedge r.bal \geq c$
 1839 $\wedge r.val = m.val$
 1840 $\langle 7 \rangle 1$. $\neg(\forall aa \in WQ :$
 1841 $\exists m_1 \in KSet(a, m.bal) :$
 1842 $\wedge m_1.acc = aa$
 1843 $\wedge \exists r \in m_1.m2av : \wedge r.bal \geq c$
 1844 $\wedge r.val = m.val)$
 1845 BY $\langle 5 \rangle 3$ DEF $KS22, KS22WQ, KS22WQa$
 1846 $\langle 7 \rangle 2$. QED
 1847 BY $\langle 7 \rangle 1$
 1848 $\langle 6 \rangle 3$. PICK $mm \in KSet(a, m.bal)' : \wedge mm.acc = aa$
 1849 $\wedge \exists r \in mm.m2av :$
 1850 $\wedge r.bal \geq c$
 1851 $\wedge r.val = m.val$
 1852 BY $\langle 6 \rangle 1$ DEF $KS22WQ, KS22WQa$
 1853 $\langle 6 \rangle 4$. $mm \notin KSet(a, m.bal)$
 1854 BY $\langle 6 \rangle 2, \langle 6 \rangle 3$
 1855 $\langle 6 \rangle 5$. $mm.bal = m.bal$
 1856 BY DEF $KSet$
 1857 $\langle 6 \rangle 6$. QED

1858 BY $\langle 6 \rangle 4, \langle 6 \rangle 5, \langle 4 \rangle 4, \langle 4 \rangle 5, \langle 4 \rangle 1$
1859 $\langle 5 \rangle 4$. QED
1860 BY $\langle 5 \rangle 2, \langle 5 \rangle 3, \langle 4 \rangle 8$ DEF $KS2$
1861 $\langle 4 \rangle$ QED
1862 $\langle 5 \rangle 1$. $KS1(KSet(a, m.bal)') \vee KS2(m.val, m.bal, KSet(a, m.bal)')$
1863 $\langle 6 \rangle$ $KnowsSafeAt(a, m.bal, m.val)' = (KS1(KSet(a, m.bal)') \vee KS2(m.val, m.bal, KSet(a, m.bal)'))$
1864 BY $KnowsSafeAtDef$
1865 $\langle 6 \rangle$ QED
1866 BY $\langle 4 \rangle 2$
1867 $\langle 5 \rangle 2$. $(\neg KS1(KSet(a, m.bal))) \wedge (\neg KS2(m.val, m.bal, KSet(a, m.bal)))$
1868 BY $\langle 4 \rangle 3, KnowsSafeAtDef$
1869 $\langle 5 \rangle 3$. QED
1870 BY $\langle 4 \rangle 7, \langle 4 \rangle 8, \langle 5 \rangle 1, \langle 5 \rangle 2$
1871 $\langle 3 \rangle 5$. QED
1872 BY $\langle 3 \rangle 3, \langle 3 \rangle 4$
1873 $\langle 2 \rangle 3$. QED
1874 $\langle 3 \rangle$ DEFINE $S \triangleq 1cmsgs' \setminus 1cmsgs$
1875 $\langle 3 \rangle 1$. $1cmsgs' = 1cmsgs \cup S$
1876 BY $\langle 2 \rangle 2$
1877 $\langle 3 \rangle 2$. $S \in \text{SUBSET } \{m \in msgsOfType("1c") : m.bal = b\}$
1878 BY $\langle 2 \rangle 2$
1879 $\langle 3 \rangle$ HIDE DEF S
1880 $\langle 3 \rangle 3$. $msgs' = msgs \cup S$
1881 BY $\langle 3 \rangle 1, \langle 2 \rangle 1$ DEF $msgs$
1882 $\langle 3 \rangle 4$. QED
1883 BY $\langle 3 \rangle 3, \langle 3 \rangle 2$
1884 $\langle 1 \rangle 5$. ASSUME NEW $self \in Ballot$
1885 PROVE $Phase1a(self) \Rightarrow$
1886 $msgs' = msgs \cup \{[type \mapsto "1a", bal \mapsto self]\}$
1887 $\langle 2 \rangle$ DEFINE $m \triangleq [type \mapsto "1a", bal \mapsto self]$
1888 $\langle 2 \rangle$ SUFFICES ASSUME $Phase1a(self)$
1889 PROVE $msgs' = msgs \cup \{m\}$
1890 BY $\langle 1 \rangle 5$
1891 $\langle 2 \rangle 1$. $\wedge bmsgs' = bmsgs \cup \{m\}$
1892 $\wedge m.type = "1a"$
1893 BY DEF $Phase1a$
1894 $\langle 2 \rangle 2$. $\wedge 1bmsgs' = 1bmsgs$
1895 $\wedge 1cmsgs' = 1cmsgs$
1896 $\wedge 2ams' = 2ams$
1897 $\wedge acceptorMsgsOfType("2b")' = acceptorMsgsOfType("2b")$
1898 $\langle 3 \rangle$ DEFINE $S \triangleq \{m\}$
1899 $\langle 3 \rangle$ $\wedge bmsgs' = bmsgs \cup S$
1900 $\wedge \forall mm \in S : mm.type = "1a"$
1901 $\wedge knowsSent' = knowsSent$
1902 BY $\langle 2 \rangle 1$ DEF $Phase1a$

```

1903   ⟨3⟩ HIDE DEF  $S$ 
1904   ⟨3⟩ QED
1905   BY ⟨1⟩b, ⟨1⟩c, ⟨1⟩d, ⟨1⟩e
1906   ⟨2⟩3.  $msgsOfType("1a")' = msgsOfType("1a") \cup \{m\}$ 
1907   BY ⟨2⟩1 DEF  $msgsOfType$ 
1908   ⟨2⟩4. QED
1909   BY ⟨2⟩2, ⟨2⟩3 DEF  $msgs$ 
1910   ⟨1⟩6. ASSUME NEW  $self \in Ballot$ 
1911   PROVE  $Phase1c(self) \Rightarrow$ 
1912      $\exists S \in \text{SUBSET } [type : \{ "1c" \}, bal : \{ self \}, val : Value] :$ 
1913      $\wedge \forall m \in S :$ 
1914      $\exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)$ 
1915      $\wedge msgs' = msgs \cup S$ 
1916   ⟨2⟩1. SUFFICES ASSUME NEW  $S \in \text{SUBSET } [type : \{ "1c" \}, bal : \{ self \}, val : Value],$ 
1917      $bmsgs' = (bmsgs \cup S),$ 
1918      $knowsSent' = knowsSent$ 
1919   PROVE ⟨1⟩6!2!2
1920   BY DEF  $Phase1c$ 
1921   ⟨2⟩ DEFINE  $SS \triangleq \{m \in S : \exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)\}$ 
1922   ⟨2⟩ SUFFICES  $msgs' = msgs \cup SS$ 
1923   BY ⟨2⟩1
1924   ⟨2⟩2.  $\forall m \in S : m.type = "1c"$ 
1925   BY ⟨2⟩1
1926   ⟨2⟩3.  $\wedge msgsOfType("1a")' = msgsOfType("1a")$ 
1927      $\wedge 1bmsgs' = 1bmsgs$ 
1928      $\wedge 2ams' = 2ams$ 
1929      $\wedge \text{acceptorMsgsOfType}("2b")' = \text{acceptorMsgsOfType}("2b")$ 
1930   BY ⟨2⟩1, ⟨2⟩2, ⟨1⟩a, ⟨1⟩b, ⟨1⟩d, ⟨1⟩e
1931   ⟨2⟩4.  $1cmsgs' = 1cmsgs \cup SS$ 
1932   ⟨3⟩1.  $msgsOfType("1c")' = msgsOfType("1c") \cup S$ 
1933   BY ⟨2⟩1 DEF  $msgsOfType$ 
1934   ⟨3⟩2.  $1cmsgs' =$ 
1935      $\{m \in msgsOfType("1c") :$ 
1936        $\exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)\}'$ 
1937      $\cup$ 
1938      $\{m \in S : \exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)\}'$ 
1939   BY ⟨3⟩1 DEF  $1cmsgs$ 
1940   ⟨3⟩3.  $\forall m : \forall a \in \text{Acceptor} :$ 
1941      $\text{KnowsSafeAt}(a, m.bal, m.val)' = \text{KnowsSafeAt}(a, m.bal, m.val)$ 
1942   BY ⟨2⟩1 DEF  $\text{KnowsSafeAt}$ 
1943   ⟨3⟩4.  $1cmsgs' =$ 
1944      $\{m \in msgsOfType("1c") :$ 
1945        $\exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)\}'$ 
1946      $\cup$ 
1947      $\{m \in S : \exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)\}'$ 

```

1948 BY $\langle 2 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3$
1949 $\langle 3 \rangle 5$. QED
1950 BY $\langle 3 \rangle 4$ DEF $1cmsgs$
1951 $\langle 2 \rangle 5$. QED
1952 BY $\langle 2 \rangle 3, \langle 2 \rangle 4$ DEF $msgs$

1954 $\langle 1 \rangle 7$. ASSUME NEW $self \in FakeAcceptor$
1955 PROVE $FakingAcceptor(self) \Rightarrow msgs' = msgs$
1956 $\langle 2 \rangle$ SUFFICES ASSUME $FakingAcceptor(self)$
1957 PROVE $msgs' = msgs$
1958 OBVIOUS
1959 $\langle 2 \rangle 1$. PICK $m \in 1bMessage \cup 2avMessage \cup 2bMessage :$
1960 $\wedge m.acc = self$
1961 $\wedge bmsgs' = bmsgs \cup \{m\}$
1962 BY DEF $FakingAcceptor$
1963 $\langle 2 \rangle 2$. $m.type \in \{ "1b", "2av", "2b" \}$
1964 BY DEF $1bMessage, 2avMessage, 2bMessage$
1965 $\langle 2 \rangle 3$. $\wedge msgsOfType("1a")' = msgsOfType("1a")$
1966 $\wedge 1cmsgs' = 1cmsgs$
1967 $\langle 3 \rangle S \triangleq \{m\}$
1968 $\langle 3 \rangle 1$. $bmsgs' = bmsgs \cup S$
1969 BY $\langle 2 \rangle 1$
1970 $\langle 3 \rangle 2$. $\wedge \forall mm \in S : mm.type \neq "1a"$
1971 $\wedge \forall mm \in S : mm.type \neq "1c"$
1972 BY $\langle 2 \rangle 1, \langle 2 \rangle 2$
1973 $\langle 3 \rangle$ HIDE DEF S
1974 $\langle 3 \rangle 3$. $knowsSent' = knowsSent$
1975 BY DEF $FakingAcceptor$
1976 $\langle 3 \rangle 4$. QED
1977 BY $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3, \langle 1 \rangle a, \langle 1 \rangle c$
1978 $\langle 2 \rangle 4$. $m.acc \notin Acceptor$
1979 BY $\langle 2 \rangle 1, BQA$
1980 $\langle 2 \rangle 5$. $1bmsgs' = 1bmsgs$
1981 $\langle 3 \rangle 1$. $acceptorMsgsOfType("1b")' = acceptorMsgsOfType("1b")$
1982 BY $\langle 2 \rangle 1, \langle 2 \rangle 4$ DEF $acceptorMsgsOfType, msgsOfType$
1983 $\langle 3 \rangle 2$. QED
1984 BY $\langle 3 \rangle 1$ DEF $1bmsgs$
1985 $\langle 2 \rangle 6$. $2ams' = 2ams$
1986 $\langle 3 \rangle 1$. $acceptorMsgsOfType("2av")' = acceptorMsgsOfType("2av")$
1987 BY $\langle 2 \rangle 1, \langle 2 \rangle 4$ DEF $acceptorMsgsOfType, msgsOfType$
1988 $\langle 3 \rangle 2$. QED
1989 BY $\langle 3 \rangle 1$ DEF $2ams$
1990 $\langle 2 \rangle 7$. $acceptorMsgsOfType("2b")' = acceptorMsgsOfType("2b")$
1991 BY $\langle 2 \rangle 1, \langle 2 \rangle 4$ DEF $acceptorMsgsOfType, msgsOfType$
1992 $\langle 2 \rangle 8$. QED

1993 BY $\langle 2 \rangle 3, \langle 2 \rangle 5, \langle 2 \rangle 6, \langle 2 \rangle 7$ DEF *msgs*
 1994 $\langle 1 \rangle 9$. QED
 1995 BY $\langle 1 \rangle 1, \langle 1 \rangle 2, \langle 1 \rangle 3, \langle 1 \rangle 4, \langle 1 \rangle 5, \langle 1 \rangle 6, \langle 1 \rangle 7$
 1996 |

Finally, we come to the proof of invariance of our inductive invariant *Inv*. Because *TLAPS* does not yet do temporal reasoning, we omit the proofs of the obviously true temporal-logic steps.

2002 THEOREM $Spec \Rightarrow \Box Inv$
 2003 $\langle 1 \rangle 1$. $Init \Rightarrow Inv$
 2004 $\langle 2 \rangle$ SUFFICES ASSUME *Init*
 2005 PROVE *Inv*
 2006 OBVIOUS
 2007 $\langle 2 \rangle$ USE DEF *Init*
 2008 $\langle 2 \rangle 1$. *TypeOK*
 2009 BY DEF *TypeOK*
 2010 $\langle 2 \rangle 2$. *bmsgsFinite*
 2011 BY *EmptySetFinite* DEF *bmsgsFinite*, *1bOr2bMsgs*
 2012 $\langle 2 \rangle 3$. *1bInv1*
 2013 BY DEF *1bInv1*
 2014 $\langle 2 \rangle 4$. *1bInv2*
 2015 BY DEF *1bInv2*
 2016 $\langle 2 \rangle 5$. *maxBalInv*
 2017 BY DEF *maxBalInv*
 2018 $\langle 2 \rangle 6$. *2avInv1*
 2019 BY DEF *2avInv1*
 2020 $\langle 2 \rangle 7$. *2avInv2*
 2021 BY DEF *2avInv2*
 2022 $\langle 2 \rangle 8$. *2avInv3*
 2023 BY DEF *2avInv3*
 2024 $\langle 2 \rangle 9$. *accInv*
 2025 BY DEF *accInv*
 2026 $\langle 2 \rangle 10$. *knowsSentInv*
 2027 BY DEF *knowsSentInv*
 2028 $\langle 2 \rangle 11$. QED
 2029 BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3, \langle 2 \rangle 4, \langle 2 \rangle 5, \langle 2 \rangle 6, \langle 2 \rangle 7, \langle 2 \rangle 8, \langle 2 \rangle 9, \langle 2 \rangle 10$
 2030 DEF *Inv*

2032 $\langle 1 \rangle 2$. $Inv \wedge [Next]_{vars} \Rightarrow Inv'$
 2033 $\langle 2 \rangle$ SUFFICES ASSUME *Inv*, $[Next]_{vars}$
 2034 PROVE *Inv'*
 2035 OBVIOUS
 2036 $\langle 2 \rangle 1$. ASSUME NEW *self* \in *Acceptor*,
 2037 NEW *b* \in *Ballot*,
 2038 $\vee Phase1b(self, b)$
 2039 $\vee Phase2av(self, b)$
 2040 $\vee Phase2b(self, b)$

2041 $\vee \text{LearnsSent}(\text{self}, b)$
 2042 PROVE Inv'
 2043 $\langle 3 \rangle 1. \text{CASE } \text{Phase1b}(\text{self}, b)$
 2044 $\langle 4 \rangle \text{USE } \text{Phase1b}(\text{self}, b)$
 2045 $\langle 4 \rangle \text{DEFINE } mb \triangleq [\text{type} \mapsto \text{"1b"}, \text{bal} \mapsto b, \text{acc} \mapsto \text{self},$
 2046 $\text{m2av} \mapsto \text{2avSent}[\text{self}],$
 2047 $\text{mbal} \mapsto \text{maxVVal}[\text{self}], \text{mval} \mapsto \text{maxVVal}[\text{self}]]$
 2048 $mc \triangleq [\text{type} \mapsto \text{"1b"}, \text{acc} \mapsto \text{self}, \text{bal} \mapsto b,$
 2049 $\text{mbal} \mapsto \text{maxVVal}[\text{self}], \text{mval} \mapsto \text{maxVVal}[\text{self}]]$
 2050 $\langle 4 \rangle 1. \text{msgs}' = \text{msgs} \cup \{mc\}$
 2051 BY MsgsLemma DEF Inv
 2052 $\langle 4 \rangle 2. \text{TypeOK}'$
 2053 $\langle 5 \rangle 1. mb \in \text{BMessage}$
 2054 BY DEF $\text{Inv}, \text{TypeOK}, \text{BMessage}, \text{1bMessage}, \text{ByzAcceptor}$
 2055 $\langle 5 \rangle 2. \text{QED}$
 2056 BY $\langle 5 \rangle 1$ DEF $\text{TypeOK}, \text{Inv}, \text{Phase1b}$
 2057 $\langle 4 \rangle 3. \text{bmsgsFinite}'$
 2058 BY FiniteMsgsLemma DEF $\text{Inv}, \text{bmsgsFinite}, \text{Phase1b}$
 2059 $\langle 4 \rangle 4. \text{1bInv1}'$
 2060 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m \in \text{bmsgs}',$
 2061 $\text{NEW } r \in m.\text{m2av},$
 2062 $\text{1bInv1}!(m)!1$
 2063 PROVE $[\text{type} \mapsto \text{"1c"},$
 2064 $\text{bal} \mapsto r.\text{bal}, \text{val} \mapsto r.\text{val}] \in \text{msgs}'$
 2065 BY DEF 1bInv1
 2066 $\langle 5 \rangle 2. \text{CASE } m = mb$
 2067 BY $\langle 4 \rangle 1, \langle 5 \rangle 1, \langle 5 \rangle 2$ DEF $\text{Inv}, \text{accInv}$
 2068 $\langle 5 \rangle 3. \text{CASE } m \in \text{bmsgs}$
 2069 BY $\langle 5 \rangle 1, \langle 5 \rangle 3, \langle 4 \rangle 1$ DEF $\text{Inv}, \text{1bInv1}$
 2070 $\langle 5 \rangle 4. \text{QED}$
 2071 BY $\langle 5 \rangle 2, \langle 5 \rangle 3$ DEF Phase1b
 2072 $\langle 4 \rangle 5. \text{1bInv2}'$
 2073 $\langle 5 \rangle 1. \text{ASSUME NEW } m1 \in \text{bmsgs}, \text{NEW } m2 \in \text{bmsgs},$
 2074 $\text{1bInv2}!(m1, m2)!1$
 2075 PROVE $m1 = m2$
 2076 BY $\langle 5 \rangle 1$ DEF $\text{Inv}, \text{1bInv2}$
 2077 $\langle 5 \rangle 2. \text{ASSUME NEW } m1 \in \text{bmsgs}',$
 2078 $\text{1bInv2}!(m1, mb)!1$
 2079 PROVE $m1 = mb$
 2080 $\langle 6 \rangle 1. \text{SUFFICES ASSUME } m1 \neq mb$
 2081 PROVE FALSE
 2082 OBVIOUS
 2083 $\langle 6 \rangle 2. m1 \in \text{bmsgs}$
 2084 BY $\langle 6 \rangle 1$ DEF Phase1b
 2085 $\langle 6 \rangle 3. m1.\text{bal} \leq \text{maxBal}[\text{self}]$

2086 BY $\langle 5 \rangle 2, \langle 6 \rangle 2$ DEF *Inv*, *maxBalInv*
 2087 $\langle 6 \rangle 4. b > \text{maxBal}[\text{self}]$
 2088 BY DEF *Phase1b*
 2089 $\langle 6 \rangle 5. m1.bal \in \text{Ballot} \cup \{-1\}$
 2090 BY $\langle 5 \rangle 2, \langle 6 \rangle 2$ DEF *Inv*, *TypeOK*, *1bMessage*
 2091 $\langle 6 \rangle 6. \text{maxBal}[\text{self}] \in \text{Ballot} \cup \{-1\}$
 2092 BY DEF *Inv*, *TypeOK*
 2093 $\langle 6 \rangle 7. \forall m1bal, \text{maxbalsel}f \in \text{Ballot} \cup \{-1\} :$
 2094 $b > \text{maxbalsel}f \wedge m1bal \leq \text{maxbalsel}f \Rightarrow m1bal \neq b$
 2095 BY *SimpleArithmetic* DEF *Ballot*
 2096 $\langle 6 \rangle 8. m1.bal \neq b$
 2097 BY $\langle 6 \rangle 3, \langle 6 \rangle 4, \langle 6 \rangle 5, \langle 6 \rangle 6, \langle 6 \rangle 7$
 2098 $\langle 6 \rangle 9.$ QED
 2099 BY $\langle 5 \rangle 2, \langle 6 \rangle 1, \langle 6 \rangle 8$
 2100 $\langle 5 \rangle 3.$ QED
 2101 $\langle 6 \rangle$ SUFFICES ASSUME NEW $m1 \in \text{bmsgs}'$, NEW $m2 \in \text{bmsgs}'$,
 2102 $1b\text{Inv}2!(m1, m2)!1$
 2103 PROVE $m1 = m2$
 2104 BY DEF *1bInv2*
 2105 $\langle 6 \rangle 1.$ CASE $m1 \neq mb \wedge m2 \neq mb$
 2106 BY $\langle 6 \rangle 1, \langle 5 \rangle 1$ DEF *Phase1b*
 2107 $\langle 6 \rangle 2.$ CASE $m1 = mb$
 2108 BY $\langle 5 \rangle 2, \langle 6 \rangle 2$
 2109 $\langle 6 \rangle 3.$ CASE $m2 = mb$
 2110 BY $\langle 5 \rangle 2, \langle 6 \rangle 3$
 2111 $\langle 6 \rangle 4.$ QED
 2112 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 6 \rangle 3$
 2113 $\langle 4 \rangle 6. \text{maxBalInv}'$
 2114 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m \in \text{bmsgs}'$,
 2115 $m.type \in \{\text{"1b"}, \text{"2av"}, \text{"2b"}\}$,
 2116 $m.acc \in \text{Acceptor}$
 2117 PROVE $m.bal \leq \text{maxBal}'[m.acc]$
 2118 BY DEF *maxBalInv*
 2119 $\langle 5 \rangle 2. \wedge \forall x \in \text{Ballot} \cup \{-1\} :$
 2120 $(b > x) \Rightarrow (x \leq b)$
 2121 $\wedge \forall x, y, z \in \text{Ballot} \cup \{-1\} :$
 2122 $(x \leq y) \wedge (y \leq z) \Rightarrow (x \leq z)$
 2123 $\wedge \forall x \in \text{Ballot} \cup \{-1\} : x \leq x$
 2124 BY *SimpleArithmetic* DEF *Ballot*
 2125 $\langle 5 \rangle 3.$ ASSUME NEW $a \in \text{Acceptor}$
 2126 PROVE $\wedge \text{maxBal}[a] \leq \text{maxBal}'[a]$
 2127 $\wedge \text{maxBal}[a] \in \text{Ballot} \cup \{-1\}$
 2128 $\wedge \text{maxBal}'[a] \in \text{Ballot} \cup \{-1\}$
 2129 $\langle 6 \rangle 1. \langle 5 \rangle 3!2!2 \wedge \langle 5 \rangle 3!2!3$
 2130 BY $\langle 4 \rangle 2$ DEF *Inv*, *TypeOK*

2131 $\langle 6 \rangle 2. \maxBal[a] \leq \maxBal'[a]$
 2132 $\langle 7 \rangle 1. \text{CASE } a = self$
 2133 BY $\langle 5 \rangle 2, \langle 6 \rangle 1, \langle 7 \rangle 1$ DEF *Phase1b, Inv, TypeOK*
 2134 $\langle 7 \rangle 2. \text{CASE } a \neq self$
 2135 BY $\langle 5 \rangle 2, \langle 7 \rangle 2, \langle 5 \rangle 3$ DEF *Phase1b, Inv, TypeOK*
 2136 $\langle 7 \rangle 3. \text{QED}$
 2137 BY $\langle 7 \rangle 1, \langle 7 \rangle 2$
 2138 $\langle 6 \rangle 3. \text{QED}$
 2139 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2140 $\langle 5 \rangle 4. \text{CASE } m \in bmsgs$
 2141 $\langle 6 \rangle 1. m.bal \leq \maxBal[m.acc]$
 2142 BY $\langle 5 \rangle 1, \langle 5 \rangle 4$ DEF *Inv, maxBalInv*
 2143 $\langle 6 \rangle 2. m.bal \in Ballot \cup \{-1\}$
 2144 $\langle 7 \rangle 1. \text{CASE } m.type = "1b"$
 2145 BY $\langle 5 \rangle 4, \langle 7 \rangle 1, BMessageLemma$ DEF *Inv, TypeOK, 1bMessage*
 2146 $\langle 7 \rangle 2. \text{CASE } m.type = "2av"$
 2147 BY $\langle 5 \rangle 4, \langle 7 \rangle 2, BMessageLemma$ DEF *Inv, TypeOK, 2avMessage*
 2148 $\langle 7 \rangle 3. \text{CASE } m.type = "2b"$
 2149 BY $\langle 5 \rangle 4, \langle 7 \rangle 3, BMessageLemma$ DEF *Inv, TypeOK, 2bMessage*
 2150 $\langle 7 \rangle 4. \text{QED}$
 2151 BY $\langle 7 \rangle 1, \langle 7 \rangle 2, \langle 7 \rangle 3, \langle 5 \rangle 1$
 2152 $\langle 6 \rangle 3. \text{QED}$
 2153 $\langle 7 \rangle 1. \wedge \maxBal[m.acc] \leq \maxBal'[m.acc]$
 2154 $\wedge \maxBal[m.acc] \in Ballot \cup \{-1\}$
 2155 $\wedge \maxBal'[m.acc] \in Ballot \cup \{-1\}$
 2156 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$
 2157 $\langle 7 \rangle 2. \text{QED}$
 2158 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 7 \rangle 1, \langle 5 \rangle 2$
 2159 $\langle 5 \rangle 5. \text{CASE } m = mb$
 2160 BY $\langle 5 \rangle 2, \langle 5 \rangle 5$ DEF *Inv, TypeOK, Phase1b*
 2161 $\langle 5 \rangle 6. \text{QED}$
 2162 BY $\langle 5 \rangle 4, \langle 5 \rangle 5$ DEF *Phase1b*
 2163 $\langle 4 \rangle 7. 2avInv1'$
 2164 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m1 \in bmsgs', \text{ NEW } m2 \in bmsgs',$
 2165 $2avInv1!(m1, m2)!1$
 2166 PROVE $2avInv1!(m1, m2)!2'$
 2167 BY DEF *2avInv1*
 2168 $\langle 5 \rangle 2. m1 \neq mb \wedge m2 \neq mb$
 2169 BY $\langle 5 \rangle 1, mb.type = "1b"$
 2170 $\langle 5 \rangle 3. m1 \in bmsgs \wedge m2 \in bmsgs$
 2171 BY $\langle 5 \rangle 2$ DEF *Phase1b*
 2172 $\langle 5 \rangle 4. \text{QED}$
 2173 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$ DEF *Inv, 2avInv1*
 2174 $\langle 4 \rangle 8. 2avInv2'$
 2175 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m \in bmsgs',$

2176 $2avInv2!(m)!1$
 2177 PROVE $\exists r \in 2avSent'[m.acc] :$
 2178 $\wedge r.val = m.val$
 2179 $\wedge r.bal \geq m.bal$
 2180 BY DEF $2avInv2$
 2181 $\langle 5 \rangle 2. m \neq mb$
 2182 BY $\langle 5 \rangle 1, mb.type = "1b"$
 2183 $\langle 5 \rangle 3. m \in bmsgs$
 2184 BY $\langle 5 \rangle 2$ DEF $Phase1b$
 2185 $\langle 5 \rangle 4.$ QED
 2186 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$ DEF $Phase1b, Inv, 2avInv2$
 2187 $\langle 4 \rangle 9. 2avInv3'$
 2188 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m \in bmsgs'$,
 2189 $2avInv3!(m)!1$
 2190 PROVE $2avInv3!(m)!2'$
 2191 BY DEF $2avInv3$
 2192 $\langle 5 \rangle 2. m \neq mb$
 2193 BY $\langle 5 \rangle 1, mb.type = "1b"$
 2194 $\langle 5 \rangle 3. m \in bmsgs$
 2195 BY $\langle 5 \rangle 2$ DEF $Phase1b$
 2196 $\langle 5 \rangle 4.$ QED
 2197 BY $\langle 5 \rangle 1, \langle 5 \rangle 3, \langle 4 \rangle 1$ DEF $Phase1b, Inv, 2avInv3$
 2198 $\langle 4 \rangle 10. accInv'$
 2199 $\langle 5 \rangle$ SUFFICES ASSUME NEW $a \in Acceptor$,
 2200 NEW $r \in 2avSent[a]$
 2201 PROVE $\wedge r.bal \leq maxBal'[a]$
 2202 $\wedge [type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val]$
 2203 $\in msgs'$
 2204 BY DEF $accInv, Phase1b$
 2205 $\langle 5 \rangle 1. \wedge r.bal \leq maxBal[a]$
 2206 $\wedge [type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val] \in msgs$
 2207 BY DEF $Inv, accInv$
 2208 $\langle 5 \rangle 2. [type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val] \in msgs'$
 2209 BY $\langle 5 \rangle 1, MsgsLemma$ DEF Inv
 2210 $\langle 5 \rangle 3. maxBal[a] \leq maxBal'[a]$
 2211 $\langle 6 \rangle 1.$ CASE $a = self$
 2212 $\langle 7 \rangle 1. \forall maxbal \in Ballot \cup \{-1\} :$
 2213 $b > maxbal \Rightarrow maxbal \leq b$
 2214 BY $SimpleArithmetic$ DEF $Ballot$
 2215 $\langle 7 \rangle 2.$ QED
 2216 BY $\langle 6 \rangle 1, \langle 7 \rangle 1$ DEF $Phase1b, Inv, TypeOK$
 2217 $\langle 6 \rangle 2.$ CASE $a \neq self$
 2218 $\langle 7 \rangle 1. \forall maxbal \in Ballot \cup \{-1\} : maxbal \leq maxbal$
 2219 BY $SimpleArithmetic$ DEF $Ballot$
 2220 $\langle 7 \rangle 2.$ QED

2221 BY $\langle 5 \rangle 3, \langle 6 \rangle 2, \langle 7 \rangle 1$ DEF *Phase1b*, *Inv*, *TypeOK*
 2222 $\langle 6 \rangle 3$. QED
 2223 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2224 $\langle 5 \rangle 4$. $r.bal \leq \max Bal'[a]$
 2225 $\langle 6 \rangle 1$. $\forall rbal, maxb, maxbp \in Ballot \cup \{-1\}$:
 2226 $rbal \leq maxb \wedge maxb \leq maxbp \Rightarrow rbal \leq maxbp$
 2227 BY *SimpleArithmetic* DEF *Ballot*
 2228 $\langle 6 \rangle 2$. $r.bal \in Ballot$
 2229 $\langle 7 \rangle 1$. $2avSent[a] \in \text{SUBSET } [val : Value, bal : Ballot]$
 2230 BY DEF *Inv*, *TypeOK*
 2231 $\langle 7 \rangle 2$. $r \in [val : Value, bal : Ballot]$
 2232 BY $\langle 7 \rangle 1$
 2233 $\langle 7 \rangle 3$. QED
 2234 BY $\langle 7 \rangle 2$
 2235 $\langle 6 \rangle 3$. $\wedge \max Bal[a] \in Ballot \cup \{-1\}$
 2236 $\wedge \max Bal'[a] \in Ballot \cup \{-1\}$
 2237 BY $\langle 4 \rangle 2$ DEF *Inv*, *TypeOK*
 2238 $\langle 6 \rangle 4$. QED
 2239 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 6 \rangle 3, \langle 5 \rangle 1, \langle 5 \rangle 3$
 2240 $\langle 5 \rangle 5$. QED
 2241 BY $\langle 5 \rangle 2, \langle 5 \rangle 4$
 2242 $\langle 4 \rangle 11$. *knowsSentInv'*
 2243 $\langle 5 \rangle 1$. $msgsOfType("1b") \subseteq msgsOfType("1b")'$
 2244 BY DEF *Phase1b*, *msgsOfType*
 2245 $\langle 5 \rangle 2$. QED
 2246 BY $\langle 5 \rangle 1$ DEF *Inv*, *knowsSentInv*, *Phase1b*
 2247 $\langle 4 \rangle 12$. QED
 2248 BY $\langle 4 \rangle 2, \langle 4 \rangle 3, \langle 4 \rangle 4, \langle 4 \rangle 5, \langle 4 \rangle 6, \langle 4 \rangle 7, \langle 4 \rangle 8, \langle 4 \rangle 9,$
 2249 $\langle 4 \rangle 10, \langle 4 \rangle 11$ DEF *Inv*
 2250 $\langle 3 \rangle 2$. CASE *Phase2av*(*self*, *b*)
 2251 $\langle 4 \rangle$ USE *Phase2av*(*self*, *b*)
 2252 $\langle 4 \rangle 1$. PICK $mc \in sentMsgs("1c", b)$:
 2253 $\wedge KnowsSafeAt(self, b, mc.val)$
 2254 $\wedge bmsgs' = bmsgs \cup$
 2255 $\{[type \mapsto "2av", bal \mapsto b,$
 2256 $val \mapsto mc.val, acc \mapsto self]\}$
 2257 $\wedge 2avSent' = [2avSent \text{ EXCEPT}$
 2258 $![self] = \{r \in 2avSent[self] : r.val \neq mc.val\}$
 2259 $\cup \{[val \mapsto mc.val, bal \mapsto b]\}$
 2260 BY DEF *Phase2av*
 2261 $\langle 4 \rangle 2$. $mc = [type \mapsto "1c", bal \mapsto mc.bal, val \mapsto mc.val]$
 2262 Follows from $\langle 4 \rangle 1$ and def of *sentMsgs* (domain of *mc*).
 2263 but provers are unable to prove this easily.
 2264 $\langle 5 \rangle 1$. $\wedge mc \in [type : \{"1c"\}, bal : Ballot, val : Value]$
 2265 $\wedge mc.type = "1c"$

2266 BY $\langle 4 \rangle 1$, *BMessageLemma* DEF *sentMsgs*, *Inv*, *TypeOK*, *1cMessage*
 2267 $\langle 5 \rangle$ DEFINE $mcx \triangleq [type \mapsto \text{"1c"}, bal \mapsto mc.bal, val \mapsto mc.val]$
 2268 $\langle 5 \rangle 2. \wedge mc = [i \in \{\text{"type"}, \text{"bal"}, \text{"val"}\} \mapsto mc[i]]$
 2269 $\wedge mcx = [i \in \{\text{"type"}, \text{"bal"}, \text{"val"}\} \mapsto mcx[i]]$
 2270 BY $\langle 5 \rangle 1$
 2271 $\langle 5 \rangle 3. \forall i \in \{\text{"type"}, \text{"bal"}, \text{"val"}\} : mc[i] = mcx[i]$
 2272 $\langle 6 \rangle$ SUFFICES ASSUME NEW $i \in \{\text{"type"}, \text{"bal"}, \text{"val"}\}$
 2273 PROVE $mc[i] = mcx[i]$
 2274 OBVIOUS
 2275 $\langle 6 \rangle 1$. CASE $i = \text{"type"}$
 2276 BY $\langle 5 \rangle 1$, $\langle 6 \rangle 1$
 2277 $\langle 6 \rangle 2$. CASE $i = \text{"bal"}$
 2278 BY $\langle 6 \rangle 2$
 2279 $\langle 6 \rangle 3$. CASE $i = \text{"val"}$
 2280 BY $\langle 6 \rangle 3$
 2281 $\langle 6 \rangle 4$. QED
 2282 BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$
 2283 $\langle 5 \rangle 4$. QED
 2284 BY $\langle 5 \rangle 2$, $\langle 5 \rangle 3$
 2285 $\langle 4 \rangle$ DEFINE $mb \triangleq [type \mapsto \text{"2av"}, bal \mapsto b,$
 2286 $val \mapsto mc.val, acc \mapsto self]$
 2287 $mmc(v) \triangleq [type \mapsto \text{"1c"}, bal \mapsto b, val \mapsto v]$
 2288 $ma(v) \triangleq [type \mapsto \text{"2a"}, bal \mapsto b, val \mapsto v]$
 2289 $\langle 4 \rangle 3. \forall msgs' = msgs$
 2290 $\forall \exists v \in Value :$
 2291 $\wedge mmc(v) \in msgs$
 2292 $\wedge msgs' = msgs \cup \{ma(v)\}$
 2293 $\langle 5 \rangle 1$. *MsgsLemma*!2!2
 2294 BY *MsgsLemma* DEF *Inv*
 2295 $\langle 5 \rangle 2$. QED
 2296 BY $\langle 5 \rangle 1$
 2297 $\langle 4 \rangle 4. msgs \subseteq msgs'$
 2298 BY $\langle 4 \rangle 3$
 2299 $\langle 4 \rangle 5$. *TypeOK'*
 2300 $\langle 5 \rangle 1. mc \in 1cMessage$
 2301 BY $mc.type = \text{"1c"}$, *BMessageLemma* DEF *sentMsgs*, *Inv*, *TypeOK*
 2303 $\langle 5 \rangle 2. mb.val \in Value$
 2304 $\langle 6 \rangle 2$. QED
 2305 BY $\langle 5 \rangle 1$ DEF *1cMessage*
 2306 $\langle 5 \rangle 3$. *TypeOK*!1'
 2307 BY DEF *Inv*, *TypeOK*, *Phase2av*
 2308 $\langle 5 \rangle 4$. *TypeOK*!2'
 2309 $\langle 6 \rangle 1. 2avSent[self] \in \text{SUBSET } [val : Value, bal : Ballot]$
 2310 BY DEF *Inv*, *TypeOK*

2311 $\langle 6 \rangle 2. \{r \in 2avSent[self] : r.val \neq mc.val\}$
2312 $\cup \{[val \mapsto mc.val, bal \mapsto b]\}$
2313 $\in \text{SUBSET } [val : Value, bal : Ballot]$
2314 BY $\langle 6 \rangle 1, \langle 5 \rangle 1, mc.val \in Value$ DEF $1cMessage$
2315 $\langle 6 \rangle 3. \text{QED}$
2316 BY $\langle 4 \rangle 1, \langle 6 \rangle 2$ DEF $Inv, TypeOK$
2317 $\langle 5 \rangle 5. TypeOK!3' \wedge TypeOK!4' \wedge TypeOK!5'$
2318 BY DEF $Inv, TypeOK, Phase2av$
2319 $\langle 5 \rangle 6. TypeOK!6'$
2320 $\langle 6 \rangle 1. mb \in 2avMessage$
2321 BY $\langle 5 \rangle 2$ DEF $2avMessage, ByzAcceptor$
2322 $\langle 6 \rangle 2. \text{QED}$
2323 BY $\langle 4 \rangle 1, \langle 6 \rangle 1$ DEF $Inv, TypeOK, BMessage$
2324 $\langle 5 \rangle 7. \text{QED}$
2325 BY $\langle 5 \rangle 3, \langle 5 \rangle 4, \langle 5 \rangle 5, \langle 5 \rangle 6$ DEF $TypeOK$
2326 $\langle 4 \rangle 6. bmsgsFinite'$
2327 BY $\langle 4 \rangle 1, FiniteMsgsLemma$ DEF $Inv, bmsgsFinite$
2328 $\langle 4 \rangle 7. 1bInv1'$
2329 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m \in bmsgs',$
2330 $1bInv1!(m)!1$
2331 PROVE $1bInv1!(m)!2'$
2332 BY DEF $1bInv1$
2333 $\langle 5 \rangle 2. m \neq mb$
2334 BY $\langle 5 \rangle 1, mb.type = "2av"$
2335 $\langle 5 \rangle 3. m \in bmsgs$
2336 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$ DEF $Phase2av$
2337 $\langle 5 \rangle 4. \text{QED}$
2338 BY $\langle 5 \rangle 1, \langle 5 \rangle 3, \langle 4 \rangle 4$ DEF $Phase2av, Inv, 1bInv1$
2339 $\langle 4 \rangle 8. 1bInv2'$
2340 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m1 \in bmsgs', \text{ NEW } m2 \in bmsgs',$
2341 $1bInv2!(m1, m2)!1$
2342 PROVE $1bInv2!(m1, m2)!2'$
2343 BY DEF $1bInv2$
2344 $\langle 5 \rangle 2. m1 \neq mb \wedge m2 \neq mb$
2345 BY $\langle 5 \rangle 1, mb.type = "2av"$
2346 $\langle 5 \rangle 3. m1 \in bmsgs \wedge m2 \in bmsgs$
2347 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$
2348 $\langle 5 \rangle 4. \text{QED}$
2349 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$ DEF $Inv, 1bInv2$
2350 $\langle 4 \rangle 9. maxBalInv'$
2351 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m \in bmsgs',$
2352 $m.type \in \{"1b", "2av", "2b"\},$
2353 $m.acc \in Acceptor$
2354 PROVE $m.bal \leq maxBal'[m.acc]$
2355 BY DEF $maxBalInv$

2356 $\langle 5 \rangle 2. \wedge \forall x, y, z \in \text{Ballot} \cup \{-1\} :$
 2357 $(x \leq y) \wedge (y \leq z) \Rightarrow (x \leq z)$
 2358 $\wedge \forall x \in \text{Ballot} \cup \{-1\} : x \leq x$
 2359 BY *SimpleArithmetic* DEF *Ballot*
 2360 $\langle 5 \rangle 3. \text{ASSUME NEW } a \in \text{Acceptor}$
 2361 PROVE $\wedge \text{maxBal}[a] \leq \text{maxBal}'[a]$
 2362 $\wedge \text{maxBal}[a] \in \text{Ballot} \cup \{-1\}$
 2363 $\wedge \text{maxBal}'[a] \in \text{Ballot} \cup \{-1\}$
 2364 $\langle 6 \rangle 1. \langle 5 \rangle 3!2!2 \wedge \langle 5 \rangle 3!2!3$
 2365 BY DEF *Inv*, *TypeOK*, *Phase2av*
 2366 $\langle 6 \rangle 2. \text{maxBal}[a] \leq \text{maxBal}'[a]$
 2367 $\langle 7 \rangle 1. \text{CASE } a = \text{self}$
 2368 BY $\langle 6 \rangle 1, \langle 7 \rangle 1$ DEF *Phase2av*, *Inv*, *TypeOK*
 2369 $\langle 7 \rangle 2. \text{CASE } a \neq \text{self}$
 2370 BY $\langle 5 \rangle 2, \langle 7 \rangle 2, \langle 6 \rangle 1$ DEF *Phase2av*, *Inv*, *TypeOK*
 2371 $\langle 7 \rangle 3. \text{QED}$
 2372 BY $\langle 7 \rangle 1, \langle 7 \rangle 2$
 2373 $\langle 6 \rangle 3. \text{QED}$
 2374 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2375 $\langle 5 \rangle 4. \text{CASE } m \in \text{bmsgs}$
 2376 $\langle 6 \rangle 1. m.\text{bal} \leq \text{maxBal}[m.\text{acc}]$
 2377 BY $\langle 5 \rangle 1, \langle 5 \rangle 4$ DEF *Inv*, *maxBalInv*
 2378 $\langle 6 \rangle 2. m.\text{bal} \in \text{Ballot} \cup \{-1\}$
 2379 $\langle 7 \rangle 1. \text{CASE } m.\text{type} = \text{"1b"}$
 2380 BY $\langle 5 \rangle 4, \langle 7 \rangle 1, \text{BMessageLemma}$ DEF *Inv*, *TypeOK*, *1bMessage*
 2381 $\langle 7 \rangle 2. \text{CASE } m.\text{type} = \text{"2av"}$
 2382 BY $\langle 5 \rangle 4, \langle 7 \rangle 2, \text{BMessageLemma}$ DEF *Inv*, *TypeOK*, *2avMessage*
 2383 $\langle 7 \rangle 3. \text{CASE } m.\text{type} = \text{"2b"}$
 2384 BY $\langle 5 \rangle 4, \langle 7 \rangle 3, \text{BMessageLemma}$ DEF *Inv*, *TypeOK*, *2bMessage*
 2385 $\langle 7 \rangle 4. \text{QED}$
 2386 BY $\langle 7 \rangle 1, \langle 7 \rangle 2, \langle 7 \rangle 3, \langle 5 \rangle 1$
 2387 $\langle 6 \rangle 3. \text{QED}$
 2388 $\langle 7 \rangle 1. \wedge \text{maxBal}[m.\text{acc}] \leq \text{maxBal}'[m.\text{acc}]$
 2389 $\wedge \text{maxBal}[m.\text{acc}] \in \text{Ballot} \cup \{-1\}$
 2390 $\wedge \text{maxBal}'[m.\text{acc}] \in \text{Ballot} \cup \{-1\}$
 2391 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$
 2392 $\langle 7 \rangle 2. \text{QED}$
 2393 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 7 \rangle 1, \langle 5 \rangle 2$
 2394 $\langle 5 \rangle 5. \text{CASE } m = mb$
 2395 $\langle 6 \rangle 1. b \leq b$
 2396 BY *SimpleArithmetic* DEF *Ballot*
 2397 $\langle 6 \rangle 2. \text{QED}$
 2398 $\langle 7 \rangle 1. m.\text{bal} = b \wedge m.\text{acc} = \text{self}$
 2399 BY $\langle 5 \rangle 5$
 2400 $\langle 7 \rangle 2. \text{maxBal}'[\text{self}] = b$

2401 BY DEF *Inv*, *TypeOK*, *Phase2av*
 2402 $\langle 7 \rangle 3$. QED
 2403 BY $\langle 6 \rangle 1$, $\langle 7 \rangle 1$, $\langle 7 \rangle 2$ DEF *Inv*, *TypeOK*, *Phase2av*
 2404 $\langle 5 \rangle 6$. QED
 2405 BY $\langle 5 \rangle 4$, $\langle 5 \rangle 5$, $\langle 4 \rangle 1$
 2406 $\langle 4 \rangle 10$. $2avInv1'$
 2407 $\langle 5 \rangle 1$. ASSUME NEW $m1 \in bmsgs$, NEW $m2 \in bmsgs$,
 2408 $2avInv1!(m1, m2)!1$
 2409 PROVE $m1 = m2$
 2410 BY $\langle 5 \rangle 1$ DEF *Inv*, $2avInv1$
 2411 $\langle 5 \rangle 2$. ASSUME NEW $m1 \in bmsgs'$,
 2412 $2avInv1!(m1, mb)!1$
 2413 PROVE $m1 = mb$
 2414 $\langle 6 \rangle 1$. SUFFICES ASSUME $m1 \neq mb$
 2415 PROVE FALSE
 2416 OBVIOUS
 2417 $\langle 6 \rangle 2$. $m1 \in bmsgs$
 2418 BY $\langle 6 \rangle 1$, $\langle 4 \rangle 1$
 2419 $\langle 6 \rangle 3$. PICK $r \in 2avSent[self] : r.bal \geq m1.bal$
 2420 BY $\langle 5 \rangle 2$, $\langle 6 \rangle 2$ DEF *Inv*, $2avInv2$
 2421 $\langle 6 \rangle 4$. $r.bal < b$
 2422 BY DEF *Phase2av*
 2423 $\langle 6 \rangle 5$. $m1.bal \in Ballot \cup \{-1\}$
 2424 BY $\langle 5 \rangle 2$, $\langle 6 \rangle 2$ DEF *Inv*, *TypeOK*, $1bMessage$
 2425 $\langle 6 \rangle 6$. $r \in [val : Value, bal : Ballot]$
 2426 BY DEF *Inv*, *TypeOK*
 2427 $\langle 6 \rangle 7$. $r.bal \in Ballot$
 2428 BY $\langle 6 \rangle 6$ DEF *Inv*, *TypeOK*
 2429 $\langle 6 \rangle 8$. $\forall m1bal, maxcbalself \in Ballot \cup \{-1\} :$
 2430 $maxcbalself < b \wedge maxcbalself \geq m1bal$
 2431 $\Rightarrow m1bal \neq b$
 2432 BY *SimpleArithmetic* DEF *Ballot*
 2433 $\langle 6 \rangle 9$. $m1.bal \neq b$
 2434 BY $\langle 6 \rangle 3$, $\langle 6 \rangle 4$, $\langle 6 \rangle 5$, $\langle 6 \rangle 7$, $\langle 6 \rangle 8$
 2435 $\langle 6 \rangle 10$. QED
 2436 BY $\langle 5 \rangle 2$, $\langle 6 \rangle 9$
 2437 $\langle 5 \rangle 3$. QED
 2438 $\langle 6 \rangle$ SUFFICES ASSUME NEW $m1 \in bmsgs'$, NEW $m2 \in bmsgs'$,
 2439 $2avInv1!(m1, m2)!1$
 2440 PROVE $m1 = m2$
 2441 BY DEF $2avInv1$
 2442 $\langle 6 \rangle 1$. CASE $m1 \neq mb \wedge m2 \neq mb$
 2443 BY $\langle 6 \rangle 1$, $\langle 5 \rangle 1$, $\langle 4 \rangle 1$ DEF *Phase2av*
 2444 $\langle 6 \rangle 2$. CASE $m1 = mb$
 2445 BY $\langle 5 \rangle 2$, $\langle 6 \rangle 2$

2446 $\langle 6 \rangle 3.$ CASE $m2 = mb$
 2447 BY $\langle 5 \rangle 2, \langle 6 \rangle 3$
 2448 $\langle 6 \rangle 4.$ QED
 2449 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 6 \rangle 3$
 2450 $\langle 4 \rangle 11.$ $2avInv2'$
 2451 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m \in bmsgs'$,
 2452 $2avInv2!(m)!1$
 2453 PROVE $\exists r \in 2avSent'[m.acc] : \wedge r.val = m.val$
 2454 $\wedge r.bal \geq m.bal$
 2455 BY DEF $2avInv2$
 2456 $\langle 5 \rangle 2.$ CASE $m.acc = self$
 2457 $\langle 6 \rangle 1.$ CASE $m = mb$
 2458 $\langle 7 \rangle$ DEFINE $r \triangleq [val \mapsto mc.val, bal \mapsto b]$
 2459 $\langle 7 \rangle 1.$ $r \in 2avSent'[self]$
 2460 BY $\langle 4 \rangle 1$ DEF $Inv, TypeOK$
 2461 $\langle 7 \rangle 2.$ $b \geq b$
 2462 BY *SimpleArithmetic* DEF *Ballot*
 2463 $\langle 7 \rangle 3.$ QED
 2464 BY $\langle 7 \rangle 1, \langle 6 \rangle 1, mb.bal = b, \langle 7 \rangle 2$
 2465 $\langle 6 \rangle 2.$ CASE $m \neq mb$
 2466 $\langle 7 \rangle 1.$ $m \in bmsgs$
 2467 BY $\langle 4 \rangle 1, \langle 6 \rangle 2$
 2468 $\langle 7 \rangle 2.$ PICK $r \in 2avSent[m.acc] : \wedge r.val = m.val$
 2469 $\wedge r.bal \geq m.bal$
 2470 BY $\langle 5 \rangle 1, \langle 7 \rangle 1$ DEF $Inv, 2avInv2$
 2471 $\langle 7 \rangle 3.$ CASE $r.val = mc.val$
 2472 $\langle 8 \rangle 1.$ $r.bal \leq maxBal[self]$
 2473 BY $\langle 5 \rangle 2$ DEF $Inv, accInv$
 2474 $\langle 8 \rangle 2.$ $b \geq m.bal$
 2475 $\langle 9 \rangle 1.$ $\forall rbal, mbal, maxbal \in Ballot \cup \{-1\} :$
 2476 $rbal \geq mbal \wedge rbal \leq maxbal \wedge maxbal \leq b$
 2477 $\Rightarrow b \geq mbal$
 2478 BY *SimpleArithmetic* DEF *Ballot*
 2479 $\langle 9 \rangle 2.$ $r.bal \in Ballot$
 2480 $\langle 10 \rangle 1.$ $r \in [val : Value, bal : Ballot]$
 2481 BY $\langle 5 \rangle 2$ DEF $Inv, TypeOK$
 2482 $\langle 10 \rangle 2.$ QED
 2483 BY $\langle 10 \rangle 1$
 2484 $\langle 9 \rangle 3.$ $maxBal[self] \in Ballot \cup \{-1\}$
 2485 BY DEF $Inv, TypeOK$
 2486 $\langle 9 \rangle 4.$ $m.bal \in Ballot$
 2487 BY $\langle 5 \rangle 1, \langle 5 \rangle 2, \langle 7 \rangle 1, BMessageLemma$ DEF $Inv, TypeOK, 2avMessage$
 2488 $\langle 9 \rangle 5.$ QED
 2489 BY $\langle 9 \rangle 1, \langle 9 \rangle 2, \langle 9 \rangle 3, \langle 9 \rangle 4, \langle 7 \rangle 2, \langle 8 \rangle 1$ DEF *Phase2av*
 2490 $\langle 8 \rangle$ DEFINE $rr \triangleq [val \mapsto mc.val, bal \mapsto b]$

2491 $\langle 8 \rangle rr \in 2avSent'[m.acc]$
 2492 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$ DEF *Inv*, *TypeOK*
 2493 $\langle 8 \rangle 3$. WITNESS $rr \in 2avSent'[m.acc]$
 2494 $\langle 8 \rangle 4$. QED
 2495 BY $\langle 8 \rangle 2, \langle 7 \rangle 2, \langle 7 \rangle 3$
 2496 $\langle 7 \rangle 4$. CASE $r.val \neq mc.val$
 2497 BY $\langle 7 \rangle 2, \langle 4 \rangle 1, \langle 5 \rangle 2, \langle 7 \rangle 4$ DEF *Inv*, *TypeOK*
 2498 $\langle 7 \rangle 5$. QED
 2499 BY $\langle 7 \rangle 3, \langle 7 \rangle 4$
 2500 $\langle 6 \rangle 3$. QED
 2501 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2502 $\langle 5 \rangle 3$. CASE $m.acc \neq self$
 2503 $\langle 6 \rangle 1$. $m \in bmsgs$
 2504 BY $\langle 5 \rangle 3, mb.acc = self, \langle 4 \rangle 1$
 2505 $\langle 6 \rangle 2$. $m.acc \in Acceptor$
 2506 BY *BMessageLemma*, $\langle 6 \rangle 1, \langle 5 \rangle 1$ DEF *Inv*, *TypeOK*, *2avMessage*
 2507 $\langle 6 \rangle 3$. $2avSent'[m.acc] = 2avSent[m.acc]$
 2508 BY $\langle 6 \rangle 2, \langle 4 \rangle 1, \langle 5 \rangle 3$ DEF *Inv*, *TypeOK*
 2509 $\langle 6 \rangle 4$. PICK $r \in 2avSent[m.acc] : \wedge r.val = m.val$
 2510 $\wedge r.bal \geq m.bal$
 2511 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 5 \rangle 1$ DEF *Inv*, *2avInv2*
 2512 $\langle 6 \rangle 5$. QED
 2513 BY $\langle 6 \rangle 3, \langle 6 \rangle 4$
 2514 $\langle 5 \rangle 4$. QED
 2515 BY $\langle 5 \rangle 2, \langle 5 \rangle 3$
 2516 $\langle 4 \rangle 12$. *2avInv3'*
 2517 $\langle 5 \rangle 1$. SUFFICES ASSUME NEW $m \in bmsgs'$,
 2518 $2avInv3!(m)!1$
 2519 PROVE $2avInv3!(m)!2'$
 2520 BY DEF *2avInv3*
 2521 $\langle 5 \rangle 2$. CASE $m \in bmsgs$
 2522 BY $\langle 5 \rangle 1, \langle 5 \rangle 2, \langle 4 \rangle 4$ DEF *Inv*, *2avInv3*
 2523 $\langle 5 \rangle 3$. CASE $m = mb$
 2524 $\langle 6 \rangle 1$. $mc \in msgs$
 2525 BY $\langle 4 \rangle 1$ DEF *sentMsgs*, *msgs*, *1cmsgs*, *msgsOfType*
 2526 $\langle 6 \rangle 2$. $mc \in msgs'$
 2527 BY $\langle 6 \rangle 1, \langle 4 \rangle 4$
 2528 $\langle 6 \rangle 3$. $mc.bal = m.bal \wedge mc.val = m.val$
 2529 BY $\langle 5 \rangle 3$ DEF *sentMsgs*
 2530 $\langle 6 \rangle 4$. $mc = [type \mapsto "1c", bal \mapsto m.bal, val \mapsto m.val]$
 2531 BY $\langle 4 \rangle 2, \langle 6 \rangle 3$
 2532 $\langle 6 \rangle 5$. QED
 2533 BY $\langle 6 \rangle 1, \langle 6 \rangle 4, \langle 4 \rangle 4$
 2534 $\langle 5 \rangle 4$. QED
 2535 BY $\langle 5 \rangle 2, \langle 5 \rangle 3, \langle 4 \rangle 1$

2536 $\langle 4 \rangle 13. accInv'$
 2537 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } a \in \text{Acceptor},$
 2538 $\text{NEW } r \in 2avSent'[a]$
 2539 $\text{PROVE } \wedge r.bal \leq maxBal'[a]$
 2540 $\wedge [type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val]$
 2541 $\in msgs'$
 2542 $\text{BY DEF } accInv$
 2543 $\langle 5 \rangle 2. maxBal[a] \leq maxBal'[a]$
 2544 $\langle 6 \rangle 1. \text{CASE } a = self$
 2545 $\text{BY } \langle 6 \rangle 1 \text{ DEF } Inv, TypeOK, Phase2av$
 2546 $\langle 6 \rangle 2. \text{CASE } a \neq self$
 2547 $\langle 7 \rangle 1. \forall mbal \in Ballot \cup \{-1\} : mbal \leq mbal$
 2548 $\text{BY SimpleArithmetic DEF Ballot}$
 2549 $\langle 7 \rangle 2. \text{QED}$
 2550 $\text{BY } \langle 6 \rangle 2, \langle 7 \rangle 1 \text{ DEF } Inv, TypeOK, Phase2av$
 2551 $\langle 6 \rangle 3. \text{QED}$
 2552 $\text{BY } \langle 6 \rangle 1, \langle 6 \rangle 2$
 2553 $\langle 5 \rangle 3. \text{CASE } r \in 2avSent[a]$
 2554 $\langle 6 \rangle 1. \wedge r.bal \leq maxBal[a]$
 2555 $\wedge [type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val] \in msgs'$
 2556 $\text{BY } \langle 5 \rangle 3, \langle 4 \rangle 4 \text{ DEF } Inv, accInv$
 2557 $\langle 6 \rangle 2. \forall rbal, maxbal, maxbalp \in Ballot \cup \{-1\} :$
 2558 $rbal \leq maxbal \wedge maxbal \leq maxbalp \Rightarrow rbal \leq maxbalp$
 2559 $\text{BY SimpleArithmetic DEF Ballot}$
 2560 $\langle 6 \rangle 3. r.bal \in Ballot$
 2561 $\langle 7 \rangle 1. r \in [val : Value, bal : Ballot]$
 2562 $\text{BY } \langle 5 \rangle 3 \text{ DEF } Inv, TypeOK$
 2563 $\langle 7 \rangle 2. \text{QED}$
 2564 $\text{BY } \langle 7 \rangle 1$
 2565 $\langle 6 \rangle 4. \wedge maxBal[a] \in Ballot \cup \{-1\}$
 2566 $\wedge maxBal'[a] \in Ballot \cup \{-1\}$
 2567 $\text{BY } \langle 4 \rangle 5 \text{ DEF } Inv, TypeOK$
 2568 $\langle 6 \rangle 5. r.bal \leq maxBal'[a]$
 2569 $\text{BY } \langle 6 \rangle 1, \langle 6 \rangle 2, \langle 6 \rangle 3, \langle 6 \rangle 4, \langle 5 \rangle 2$
 2570 $\langle 6 \rangle 6. \text{QED}$
 2571 $\text{BY } \langle 6 \rangle 1, \langle 6 \rangle 5$
 2572 $\langle 5 \rangle 4. \text{CASE } r \notin 2avSent[a]$
 2573 $\langle 6 \rangle 1. a = self$
 2574 $\langle 7 \rangle 1. 2avSent'[a] \neq 2avSent[a]$
 2575 $\text{BY } \langle 5 \rangle 4$
 2576 $\langle 7 \rangle 2. \text{QED}$
 2577 $\text{BY } \langle 4 \rangle 1, \langle 7 \rangle 1 \text{ DEF } Inv, TypeOK$
 2578 $\langle 6 \rangle 2. r = [val \mapsto mc.val, bal \mapsto b]$
 2579 $\text{BY } \langle 6 \rangle 1, \langle 5 \rangle 4, \langle 4 \rangle 1 \text{ DEF } Inv, TypeOK$

2581 $\langle 6 \rangle 3. [type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val] \in msgs'$
 2582 $\langle 7 \rangle 1. \wedge mc \in msgsOfType("1c")$
 2583 $\wedge mc.bal = b$
 2584 $\wedge KnowsSafeAt(self, mc.bal, mc.val)$
 2585 BY $\langle 4 \rangle 1$ DEF $sentMsgs, msgsOfType$
 2586 $\langle 7 \rangle 2. mc \in msgs'$
 2587 BY $\langle 7 \rangle 1, \langle 4 \rangle 4$ DEF $msgs, lcmsgs$
 2588 $\langle 7 \rangle 3. mc = \langle 6 \rangle 3!1$
 2589 BY $\langle 4 \rangle 2, \langle 6 \rangle 2, \langle 4 \rangle 1$ DEF $sentMsgs$ $\langle 7 \rangle 4$
 2590 $\langle 7 \rangle 4.$ QED
 2591 BY $\langle 7 \rangle 2, \langle 7 \rangle 3$
 2592 $\langle 6 \rangle 4. \wedge maxBal'[a] = b$
 2593 $\wedge r.bal = b$
 2594 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$ DEF $Phase2av, Inv, TypeOK$
 2595 $\langle 6 \rangle 5. b \leq b$
 2596 BY $SimpleArithmetic$ DEF $Ballot$
 2597 $\langle 6 \rangle 6.$ QED
 2598 BY $\langle 6 \rangle 3, \langle 6 \rangle 4, \langle 6 \rangle 5$
 2599 $\langle 5 \rangle 5.$ QED
 2600 BY $\langle 5 \rangle 3, \langle 5 \rangle 4$
 2601 $\langle 4 \rangle 14. knowsSentInv'$
 2602 $\langle 5 \rangle 1. msgsOfType("1b")' = msgsOfType("1b")$
 2603 $\langle 6 \rangle 1. \text{ASSUME NEW } m \in msgsOfType("1b")$
 2604 $\text{PROVE } m \in msgsOfType("1b")'$
 2605 BY $\langle 4 \rangle 1$ DEF $msgsOfType$
 2606 $\langle 6 \rangle 2. \text{ASSUME NEW } m \in msgsOfType("1b")'$
 2607 $\text{PROVE } m \in msgsOfType("1b")$
 2608 BY $m.type = "1b", mb.type = "2av", \langle 4 \rangle 1$ DEF $msgsOfType$
 2609 $\langle 6 \rangle 3.$ QED
 2610 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2611 $\langle 5 \rangle 2.$ QED
 2612 BY $\langle 5 \rangle 1$ DEF $Phase2av, Inv, knowsSentInv, msgsOfType$
 2613 $\langle 4 \rangle 15.$ QED
 2614 BY $\langle 4 \rangle 5, \langle 4 \rangle 6, \langle 4 \rangle 7, \langle 4 \rangle 8, \langle 4 \rangle 9, \langle 4 \rangle 10, \langle 4 \rangle 11, \langle 4 \rangle 12,$
 2615 $\langle 4 \rangle 13, \langle 4 \rangle 14$ DEF Inv
 2616 $\langle 3 \rangle 3. \text{CASE } Phase2b(self, b)$
 2617 $\langle 4 \rangle \text{ USE } Phase2b(self, b)$
 2618 $\langle 4 \rangle 1. \text{PICK } v \in Value :$
 2619 $\wedge \exists Q \in ByzQuorum :$
 2620 $\forall a \in Q :$
 2621 $\exists m \in sentMsgs("2av", b) : \wedge m.val = v$
 2622 $\wedge m.acc = a$
 2623 $\wedge msgs' = msgs \cup$
 2624 $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\}$
 2625 $\wedge bmsgs' = (bmsgs \cup$

2626 $\{[type \mapsto \text{"2b"}, acc \mapsto self, bal \mapsto b, val \mapsto v]\}$
 2627 $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = v]$
 2628 $\langle 5 \rangle 1. MsgsLemma!2!3$
 2629 BY *MsgsLemma* DEF *Inv*
 2630 $\langle 5 \rangle 2. MsgsLemma!2!3!(self, b)$
 2631 BY $\langle 5 \rangle 1$
 2632 $\langle 5 \rangle$ DEFINE $exp(v) \triangleq MsgsLemma!2!3!(self, b)!2!(v)$
 2633 $\langle 5 \rangle 3.$ SUFFICES $\exists v \in Value : exp(v)$
 2634 OBVIOUS
 2635 $\langle 5 \rangle 4.$ QED
 2636 BY $\langle 5 \rangle 2$
 2637 $\langle 4 \rangle$ DEFINE $mb \triangleq [type \mapsto \text{"2b"}, acc \mapsto self, bal \mapsto b, val \mapsto v]$
 2638 $\langle 4 \rangle 2. TypeOK'$
 2639 $\langle 5 \rangle 1. TypeOK!1' \wedge TypeOK!3' \wedge TypeOK!5'$
 2640 BY DEF *Phase2b*, *Inv*, *TypeOK*
 2641 $\langle 5 \rangle 2. TypeOK!2'$
 2642 BY DEF *Inv*, *TypeOK*, *Phase2b*
 2643 $\langle 5 \rangle 3. TypeOK!4'$
 2644 BY $\langle 4 \rangle 1$ DEF *Inv*, *TypeOK*
 2645 $\langle 5 \rangle 4. bmsgs' \subseteq BMessage$
 2646 BY $\langle 4 \rangle 1$ DEF *Inv*, *TypeOK*, *BMessage*, *2bMessage*, *ByzAcceptor*
 2647 $\langle 5 \rangle 5.$ QED
 2648 BY $\langle 5 \rangle 1, \langle 5 \rangle 2, \langle 5 \rangle 3, \langle 5 \rangle 4$ DEF *TypeOK*
 2649 $\langle 4 \rangle 3. bmsgsFinite'$
 2650 BY $\langle 4 \rangle 1$, *FiniteMsgsLemma* DEF *Inv*, *bmsgsFinite*
 2651 $\langle 4 \rangle 4. 1bInv1'$
 2652 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m \in bmsgs'$,
 2653 $1bInv1!(m)!1$
 2654 PROVE $1bInv1!(m)!2'$
 2655 BY DEF *1bInv1*
 2656 $\langle 5 \rangle 2. m \neq mb$
 2657 BY $\langle 5 \rangle 1$, $mb.type = \text{"2b"}$
 2658 $\langle 5 \rangle 3. m \in bmsgs$
 2659 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$
 2660 $\langle 5 \rangle 4.$ QED
 2661 BY $\langle 4 \rangle 1, \langle 5 \rangle 1, \langle 5 \rangle 3, \langle 4 \rangle 4$ DEF *Inv*, *1bInv1*
 2662 $\langle 4 \rangle 5. 1bInv2'$
 2663 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m1 \in bmsgs'$, NEW $m2 \in bmsgs'$,
 2664 $1bInv2!(m1, m2)!1$
 2665 PROVE $1bInv2!(m1, m2)!2'$
 2666 BY DEF *1bInv2*
 2667 $\langle 5 \rangle 2. m1 \neq mb \wedge m2 \neq mb$
 2668 BY $\langle 5 \rangle 1$, $mb.type = \text{"2b"}$
 2669 $\langle 5 \rangle 3. m1 \in bmsgs \wedge m2 \in bmsgs$
 2670 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$

2671 $\langle 5 \rangle 4.$ QED
 2672 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$ DEF $Inv, 1bInv2$
 2673 $\langle 4 \rangle 6.$ $maxBalInv'$
 2674 The following copied almost exactly from proof
 2675 for $Phase2b(self, b)$
 2676 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m \in bmsgs'$,
 2677 $m.type \in \{ "1b", "2av", "2b" \},$
 2678 $m.acc \in Acceptor$
 2679 PROVE $m.bal \leq maxBal'[m.acc]$
 2680 BY DEF $maxBalInv$
 2681 $\langle 5 \rangle 2.$ $\wedge \forall x, y, z \in Ballot \cup \{ -1 \} :$
 2682 $(x \leq y) \wedge (y \leq z) \Rightarrow (x \leq z)$
 2683 $\wedge \forall x \in Ballot \cup \{ -1 \} : x \leq x$
 2684 BY $SimpleArithmetic$ DEF $Ballot$
 2685 $\langle 5 \rangle 3.$ ASSUME NEW $a \in Acceptor$
 2686 PROVE $\wedge maxBal[a] \leq maxBal'[a]$
 2687 $\wedge maxBal[a] \in Ballot \cup \{ -1 \}$
 2688 $\wedge maxBal'[a] \in Ballot \cup \{ -1 \}$
 2689 $\langle 6 \rangle 1. \langle 5 \rangle 3!2!2 \wedge \langle 5 \rangle 3!2!3$
 2690 BY $\langle 4 \rangle 2$ DEF $Inv, TypeOK, Phase2b$
 2691 $\langle 6 \rangle 2.$ $maxBal[a] \leq maxBal'[a]$
 2692 $\langle 7 \rangle 1.$ CASE $a = self$
 2693 BY $\langle 6 \rangle 1, \langle 7 \rangle 1$ DEF $Phase2b, Inv, TypeOK$
 2694 $\langle 7 \rangle 2.$ CASE $a \neq self$
 2695 BY $\langle 5 \rangle 2, \langle 7 \rangle 2, \langle 6 \rangle 1$ DEF $Phase2b, Inv, TypeOK$
 2696 $\langle 7 \rangle 3.$ QED
 2697 BY $\langle 7 \rangle 1, \langle 7 \rangle 2$
 2698 $\langle 6 \rangle 3.$ QED
 2699 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2700 $\langle 5 \rangle 4.$ CASE $m \in bmsgs$
 2701 $\langle 6 \rangle 1.$ $m.bal \leq maxBal[m.acc]$
 2702 BY $\langle 5 \rangle 1, \langle 5 \rangle 4$ DEF $Inv, maxBalInv$
 2703 $\langle 6 \rangle 2.$ $m.bal \in Ballot \cup \{ -1 \}$
 2704 $\langle 7 \rangle 1.$ CASE $m.type = "1b"$
 2705 BY $\langle 5 \rangle 4, \langle 7 \rangle 1, BMessageLemma$ DEF $Inv, TypeOK, 1bMessage$
 2706 $\langle 7 \rangle 2.$ CASE $m.type = "2av"$
 2707 BY $\langle 5 \rangle 4, \langle 7 \rangle 2, BMessageLemma$ DEF $Inv, TypeOK, 2avMessage$
 2708 $\langle 7 \rangle 3.$ CASE $m.type = "2b"$
 2709 BY $\langle 5 \rangle 4, \langle 7 \rangle 3, BMessageLemma$ DEF $Inv, TypeOK, 2bMessage$
 2710 $\langle 7 \rangle 4.$ QED
 2711 BY $\langle 7 \rangle 1, \langle 7 \rangle 2, \langle 7 \rangle 3, \langle 5 \rangle 1$
 2712 $\langle 6 \rangle 3.$ QED
 2713 $\langle 7 \rangle 1.$ $\wedge maxBal[m.acc] \leq maxBal'[m.acc]$
 2714 $\wedge maxBal[m.acc] \in Ballot \cup \{ -1 \}$
 2715 $\wedge maxBal'[m.acc] \in Ballot \cup \{ -1 \}$

2716 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$
 2717 $\langle 7 \rangle 2$. QED
 2718 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 7 \rangle 1, \langle 5 \rangle 2$
 2719 $\langle 5 \rangle 5$. CASE $m = mb$
 2720 $\langle 6 \rangle 1$. $b \leq b$
 2721 BY *SimpleArithmetic* DEF *Ballot*
 2722 $\langle 6 \rangle 2$. QED
 2723 $\langle 7 \rangle 1$. $m.bal = b \wedge m.acc = self$
 2724 BY $\langle 5 \rangle 5$
 2725 $\langle 7 \rangle 2$. $maxBal'[self] = b$
 2726 BY DEF *Inv*, *TypeOK*, *Phase2b*
 2727 $\langle 7 \rangle 3$. QED
 2728 BY $\langle 6 \rangle 1, \langle 7 \rangle 1, \langle 7 \rangle 2$ DEF *Inv*, *TypeOK*, *Phase2b*
 2729 $\langle 5 \rangle 6$. QED
 2730 BY $\langle 5 \rangle 4, \langle 5 \rangle 5, \langle 4 \rangle 1$
 2731 $\langle 4 \rangle 7$. $2avInv1'$
 2732 $\langle 5 \rangle 1$. SUFFICES ASSUME NEW $m1 \in bmsgs'$, NEW $m2 \in bmsgs'$,
 2733 $2avInv1!(m1, m2)!1$
 2734 PROVE $2avInv1!(m1, m2)!2'$
 2735 BY DEF $2avInv1$
 2736 $\langle 5 \rangle 2$. $m1 \neq mb \wedge m2 \neq mb$
 2737 BY $\langle 5 \rangle 1, mb.type = "2b"$
 2738 $\langle 5 \rangle 3$. $m1 \in bmsgs \wedge m2 \in bmsgs$
 2739 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$
 2740 $\langle 5 \rangle 4$. QED
 2741 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$ DEF *Inv*, $2avInv1$
 2742 $\langle 4 \rangle 8$. $2avInv2'$
 2743 $\langle 5 \rangle 1$. SUFFICES ASSUME NEW $m \in bmsgs'$,
 2744 $2avInv2!(m)!1$
 2745 PROVE $\exists r \in 2avSent'[m.acc] : \wedge r.val = m.val$
 2746 $\wedge r.bal \geq m.bal$
 2747 BY DEF $2avInv2$, *Phase2b*, *Inv*, *TypeOK*
 2748 $\langle 5 \rangle 2$. $m \neq mb$
 2749 BY $\langle 5 \rangle 1, mb.type = "2b"$
 2750 $\langle 5 \rangle 3$. $m \in bmsgs$
 2751 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$
 2752 $\langle 5 \rangle 4$. $2avSent'[m.acc] = 2avSent[m.acc]$
 2753 BY $\langle 5 \rangle 1$ DEF *Inv*, *TypeOK*, *Phase2b*
 2754 $\langle 5 \rangle 5$. QED
 2755 BY $\langle 5 \rangle 1, \langle 5 \rangle 3, \langle 5 \rangle 4$ DEF *Inv*, $2avInv2$ BY $\langle 5 \rangle 4, \langle 5 \rangle 5$
 2756 $\langle 4 \rangle 9$. $2avInv3'$
 2757 $\langle 5 \rangle 1$. SUFFICES ASSUME NEW $m \in bmsgs'$,
 2758 $2avInv3!(m)!1$
 2759 PROVE $2avInv3!(m)!2'$
 2760 BY DEF $2avInv3$

2761 $\langle 5 \rangle 2. m \neq mb$
 2762 BY $\langle 5 \rangle 1, mb.type = \text{"2b"}$
 2763 $\langle 5 \rangle 3. m \in bmsgs$
 2764 BY $\langle 4 \rangle 1, \langle 5 \rangle 2$
 2765 $\langle 5 \rangle 4. \text{QED}$
 2766 BY $\langle 5 \rangle 1, \langle 5 \rangle 3, \langle 4 \rangle 1$ DEF $Inv, 2avInv3$
 2767 $\langle 4 \rangle 10. accInv'$
 2768 Proof copied with a few changes from that of *Phase1b*
 2769 $\langle 5 \rangle$ SUFFICES ASSUME NEW $a \in Acceptor$,
 2770 NEW $r \in 2avSent[a]$
 2771 PROVE $\wedge r.bal \leq maxBal'[a]$
 2772 $\wedge [type \mapsto \text{"1c"}, bal \mapsto r.bal, val \mapsto r.val]$
 2773 $\in msgs'$
 2774 BY DEF $accInv, Phase2b$
 2775 $\langle 5 \rangle 1. \wedge r.bal \leq maxBal[a]$
 2776 $\wedge [type \mapsto \text{"1c"}, bal \mapsto r.bal, val \mapsto r.val] \in msgs$
 2777 BY DEF $Inv, accInv$
 2778 $\langle 5 \rangle 2. [type \mapsto \text{"1c"}, bal \mapsto r.bal, val \mapsto r.val] \in msgs'$
 2779 BY $\langle 5 \rangle 1, MsgsLemma$ DEF Inv
 2780 $\langle 5 \rangle 3. maxBal[a] \leq maxBal'[a]$
 2781 $\langle 6 \rangle 1. \text{CASE } a = self$
 2782 $\langle 7 \rangle 1. \forall maxbal \in Ballot \cup \{-1\} :$
 2783 $b > maxbal \Rightarrow maxbal \leq b$
 2784 BY *SimpleArithmetic* DEF *Ballot*
 2785 $\langle 7 \rangle 2. \text{QED}$
 2786 BY $\langle 6 \rangle 1, \langle 7 \rangle 1$ DEF *Phase2b, Inv, TypeOK*
 2787 $\langle 6 \rangle 2. \text{CASE } a \neq self$
 2788 $\langle 7 \rangle 1. \forall maxbal \in Ballot \cup \{-1\} : maxbal \leq maxbal$
 2789 BY *SimpleArithmetic* DEF *Ballot*
 2790 $\langle 7 \rangle 2. maxBal'[a] = maxBal[a]$
 2791 BY $\langle 6 \rangle 2$ DEF *Phase2b, Inv, TypeOK*
 2792 $\langle 7 \rangle 3. \text{QED}$
 2793 BY $\langle 7 \rangle 1, \langle 7 \rangle 2$ DEF *Phase2b, Inv, TypeOK*
 2794 $\langle 6 \rangle 3. \text{QED}$
 2795 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2796 $\langle 5 \rangle 4. r.bal \leq maxBal'[a]$
 2797 $\langle 6 \rangle 1. \forall rbal, maxb, maxbp \in Ballot \cup \{-1\} :$
 2798 $rbal \leq maxb \wedge maxb \leq maxbp \Rightarrow rbal \leq maxbp$
 2799 BY *SimpleArithmetic* DEF *Ballot*
 2800 $\langle 6 \rangle 2. r.bal \in Ballot$
 2801 $\langle 7 \rangle 1. 2avSent[a] \in \text{SUBSET } [val : Value, bal : Ballot]$
 2802 BY DEF *Inv, TypeOK*
 2803 $\langle 7 \rangle 2. r \in [val : Value, bal : Ballot]$
 2804 BY $\langle 7 \rangle 1$
 2805 $\langle 7 \rangle 3. \text{QED}$

2806 BY $\langle 7 \rangle 2$
 2807 $\langle 6 \rangle 3. \wedge \max Bal[a] \in Ballot \cup \{-1\}$
 2808 $\wedge \max Bal'[a] \in Ballot \cup \{-1\}$
 2809 BY $\langle 4 \rangle 2$ DEF *Inv*, *TypeOK*
 2810 $\langle 6 \rangle 4$. QED
 2811 BY $\langle 6 \rangle 1, \langle 6 \rangle 2, \langle 6 \rangle 3, \langle 5 \rangle 1, \langle 5 \rangle 3$
 2812 $\langle 5 \rangle 5$. QED
 2813 BY $\langle 5 \rangle 2, \langle 5 \rangle 4$
 2814 $\langle 4 \rangle 11$. *knowsSentInv'*
 2815 $\langle 5 \rangle 1. msgsOfType("1b") \subseteq msgsOfType("1b")'$
 2816 BY $\langle 4 \rangle 1$ DEF *Phase2b*, *msgsOfType*
 2817 $\langle 5 \rangle 2$. QED
 2818 BY $\langle 5 \rangle 1$ DEF *Inv*, *knowsSentInv*, *Phase2b*
 2819 $\langle 4 \rangle 12$. QED
 2820 BY $\langle 4 \rangle 2, \langle 4 \rangle 3, \langle 4 \rangle 4, \langle 4 \rangle 5, \langle 4 \rangle 6, \langle 4 \rangle 7, \langle 4 \rangle 8, \langle 4 \rangle 9,$
 2821 $\langle 4 \rangle 10, \langle 4 \rangle 11$ DEF *Inv*
 2822 $\langle 3 \rangle 4$. CASE *LearnsSent*(*self*, *b*)
 2823 $\langle 4 \rangle$ USE *LearnsSent*(*self*, *b*)
 2824 $\langle 4 \rangle 1$. PICK *MS* : $\wedge MS \subseteq \{m \in msgsOfType("1c") : m.bal = b\}$
 2825 $\wedge msgs' = msgs \cup MS$
 2826 BY *MsgsLemma* DEF *Inv*
 2827 $\langle 4 \rangle 2$. PICK *S* :
 2828 $\wedge S \subseteq sentMsgs("1b", b)$
 2829 $\wedge knowsSent' =$
 2830 $[knowsSent \text{ EXCEPT } ![self] = knowsSent[self] \cup S]$
 2831 BY DEF *LearnsSent*
 2832 $\langle 4 \rangle 3$. *TypeOK'*
 2833 $\langle 5 \rangle 1. knowsSent' \in [Acceptor \rightarrow \text{SUBSET } 1bMessage]$
 2834 $\langle 6 \rangle$ DEFINE $ks(a) \triangleq \text{IF } a = self \text{ THEN } knowsSent[self] \cup S$
 2835 $\text{ELSE } knowsSent[a]$
 2836 $\langle 6 \rangle$ SUFFICES ASSUME NEW $a \in Acceptor$
 2837 PROVE $ks(a) \in \text{SUBSET } 1bMessage$
 2838 BY $\langle 4 \rangle 2$ DEF *Inv*, *TypeOK*
 2839 $\langle 6 \rangle 1$. CASE $a \neq self$
 2840 BY $\langle 6 \rangle 1$ DEF *Inv*, *TypeOK*
 2841 $\langle 6 \rangle 2$. CASE $a = self$
 2842 $\langle 7 \rangle$ SUFFICES ASSUME NEW $m \in S$
 2843 PROVE $m \in 1bMessage$
 2844 BY $\langle 6 \rangle 2$ DEF *Inv*, *TypeOK*
 2845 $\langle 7 \rangle$ QED
 2846 BY $\langle 4 \rangle 2, BMessageLemma$ DEF *sentMsgs*, *Inv*, *TypeOK*
 2847 $\langle 6 \rangle 3$. QED
 2848 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
 2849 $\langle 5 \rangle 2$. QED
 2850 BY $\langle 5 \rangle 1$ DEF *Inv*, *TypeOK*, *LearnsSent*

```

2851   <4>4. bmsgsFinite'
2852       BY DEF LearnsSent, Inv, bmsgsFinite, 1bOr2bMsgs
2853   <4>5. 1bInv1'
2854       BY <4>1 DEF LearnsSent, Inv, 1bInv1
2855   <4>6. 1bInv2'
2856       BY DEF LearnsSent, Inv, 1bInv2
2857   <4>7. maxBalInv'
2858       BY DEF LearnsSent, Inv, maxBalInv
2859   <4>8. 2avInv1'
2860       BY DEF LearnsSent, Inv, 2avInv1
2861   <4>9. 2avInv2'
2862       BY DEF LearnsSent, Inv, 2avInv2
2863   <4>10. 2avInv3'
2864       BY <4>1 DEF LearnsSent, Inv, 2avInv3
2865   <4>11. accInv'
2866       BY <4>1 DEF LearnsSent, Inv, accInv
2867   <4>12. knowsSentInv'
2868       <5> SUFFICES ASSUME NEW a ∈ Acceptor
2869           PROVE knowsSent'[a] ⊆ msgsOfType("1b")
2870       BY DEF LearnsSent, knowsSentInv, msgsOfType
2871   <5>1.CASE a ≠ self
2872       BY <4>2 DEF Inv, TypeOK, knowsSentInv, sentMsgs, msgsOfType
2873   <5>2.CASE a = self
2874       BY <4>2 DEF Inv, TypeOK, knowsSentInv, sentMsgs, msgsOfType
2875   <5>3. QED
2876       BY <5>1, <5>2
2877   <4>13. QED
2878       BY <4>3, <4>4, <4>5, <4>6, <4>7, <4>8, <4>9, <4>10,
2879       <4>11, <4>12 DEF Inv
2880   <3>5. QED
2881       BY <2>1, <3>1, <3>2, <3>3, <3>4
2882   <2>2. ASSUME NEW self ∈ Ballot,
2883       ∨ Phase1a(self)
2884       ∨ Phase1c(self)
2885       PROVE Inv'
2886   <3>1.CASE Phase1a(self)
2887   <4> USE Phase1a(self)
2888   <4> DEFINE ma ≜ [type ↦ "1a", bal ↦ self]
2889   <4>1. msgs' = msgs ∪ {ma}
2890       BY MsgsLemma DEF Inv
2891   <4>2. TypeOK'
2892       <5>1. bmsgs' ⊆ BMessage
2893       BY DEF Phase1a, Inv, TypeOK, BMessage, 1aMessage
2894   <5>2. QED
2895       BY <5>1 DEF Inv, TypeOK, Phase1a

```

2896 $\langle 4 \rangle 3. \text{bmsgsFinite}'$
 2897 BY *FiniteMsgsLemma* DEF *Inv*, *bmsgsFinite*, *Phase1a*
 2898 $\langle 4 \rangle 4. \text{1bInv1}'$
 2899 BY $\langle 4 \rangle 1$ DEF *Phase1a*, *Inv*, *1bInv1*
 2900 $\langle 4 \rangle 5. \text{1bInv2}'$
 2901 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m1 \in \text{bmsgs}'$, NEW $m2 \in \text{bmsgs}'$,
 2902 $\text{1bInv2}!(m1, m2)!1$
 2903 PROVE $\text{1bInv2}!(m1, m2)!2'$
 2904 BY DEF *1bInv2*
 2905 $\langle 5 \rangle 2. m1 \neq ma \wedge m2 \neq ma$
 2906 BY $\langle 5 \rangle 1$, $ma.type = "1a"$
 2907 $\langle 5 \rangle 3. m1 \in \text{bmsgs} \wedge m2 \in \text{bmsgs}$
 2908 BY $\langle 5 \rangle 2$ DEF *Phase1a*
 2909 $\langle 5 \rangle 4.$ QED
 2910 BY $\langle 5 \rangle 1$, $\langle 5 \rangle 3$ DEF *Inv*, *1bInv2*
 2911 $\langle 4 \rangle 6. \text{maxBalInv}'$
 2912 BY DEF *Phase1a*, *Inv*, *maxBalInv*
 2913 $\langle 4 \rangle 7. \text{2avInv1}'$
 2914 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $m1 \in \text{bmsgs}'$, NEW $m2 \in \text{bmsgs}'$,
 2915 $\text{2avInv1}!(m1, m2)!1$
 2916 PROVE $\text{2avInv1}!(m1, m2)!2'$
 2917 BY DEF *2avInv1*
 2918 $\langle 5 \rangle 2. m1 \neq ma \wedge m2 \neq ma$
 2919 BY $\langle 5 \rangle 1$, $ma.type = "1a"$
 2920 $\langle 5 \rangle 3. m1 \in \text{bmsgs} \wedge m2 \in \text{bmsgs}$
 2921 BY $\langle 5 \rangle 2$ DEF *Phase1a*
 2922 $\langle 5 \rangle 4.$ QED
 2923 BY $\langle 5 \rangle 1$, $\langle 5 \rangle 3$ DEF *Inv*, *2avInv1*
 2924 $\langle 4 \rangle 8. \text{2avInv2}'$
 2925 BY DEF *Phase1a*, *Inv*, *2avInv2*
 2926 $\langle 4 \rangle 9. \text{2avInv3}'$
 2927 BY $\langle 4 \rangle 1$ DEF *Phase1a*, *Inv*, *2avInv3*
 2928 $\langle 4 \rangle 10. \text{accInv}'$
 2929 BY $\langle 4 \rangle 1$ DEF *Phase1a*, *Inv*, *accInv*
 2930 $\langle 4 \rangle 11. \text{knowsSentInv}'$
 2931 BY DEF *Inv*, *knowsSentInv*, *msgsOfType*, *Phase1a*
 2932 $\langle 4 \rangle 12.$ QED
 2933 BY $\langle 4 \rangle 2$, $\langle 4 \rangle 3$, $\langle 4 \rangle 4$, $\langle 4 \rangle 5$, $\langle 4 \rangle 6$, $\langle 4 \rangle 7$, $\langle 4 \rangle 8$, $\langle 4 \rangle 9$,
 2934 $\langle 4 \rangle 10$, $\langle 4 \rangle 11$ DEF *Inv*
 2935 $\langle 3 \rangle 2.$ CASE *Phase1c*(*self*)
 2936 $\langle 4 \rangle$ USE *Phase1c*(*self*)
 2937 $\langle 4 \rangle 1.$ PICK $S : \wedge S \in \text{SUBSET} [\text{type} : \{ "1c" \}, \text{bal} : \{ \text{self} \}, \text{val} : \text{Value}]$
 2938 $\wedge \text{bmsgs}' = \text{bmsgs} \cup S$
 2939 BY DEF *Phase1c*
 2940 $\langle 4 \rangle 2.$ PICK *MS* :

2941 $\wedge MS \in \text{SUBSET } [type : \{ "1c" \}, bal : \{ self \}, val : Value]$
 2942 $\wedge \forall m \in MS :$
 2943 $\quad \exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)$
 2944 $\wedge msgs' = msgs \cup MS$
 2945 BY *MsgsLemma* DEF *Inv*
 2946 $\langle 4 \rangle 3. \text{TypeOK}'$
 2947 $\langle 5 \rangle 1. bmsgs' \subseteq BMessage$
 2948 BY $\langle 4 \rangle 1$ DEF *Inv*, *TypeOK*, *BMessage*, *1cMessage*
 2949 $\langle 5 \rangle 2. \text{QED}$
 2950 BY $\langle 5 \rangle 1$ DEF *Inv*, *TypeOK*, *Phase1c*
 2951 $\langle 4 \rangle 4. bmsgsFinite'$
 2952 $\langle 5 \rangle 1. 1bOr2bMsgs' = 1bOr2bMsgs$
 2953 BY $\langle 4 \rangle 1$ DEF *1bOr2bMsgs*
 2954 $\langle 5 \rangle 2. \text{QED}$
 2955 BY $\langle 5 \rangle 1$ DEF *bmsgsFinite*, *Inv*
 2956 $\langle 4 \rangle 5. 1bInv1'$
 2957 BY $\langle 4 \rangle 2$ DEF *Phase1c*, *Inv*, *1bInv1*
 2958 $\langle 4 \rangle 6. 1bInv2'$
 2959 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m1 \in bmsgs', \text{ NEW } m2 \in bmsgs',$
 2960 $\quad 1bInv2!(m1, m2)!1$
 2961 $\quad \text{PROVE } 1bInv2!(m1, m2)!2'$
 2962 BY DEF *1bInv2*
 2963 $\langle 5 \rangle 2. m1 \notin S \wedge m2 \notin S$
 2964 $\langle 6 \rangle 1. \forall m \in S : m.type = "1c"$
 2965 BY $\langle 4 \rangle 1$
 2966 $\langle 6 \rangle 2. \text{QED}$
 2967 BY $\langle 6 \rangle 1, \langle 5 \rangle 1$
 2968 $\langle 5 \rangle 3. m1 \in bmsgs \wedge m2 \in bmsgs$
 2969 BY $\langle 5 \rangle 2, \langle 4 \rangle 1$
 2970 $\langle 5 \rangle 4. \text{QED}$
 2971 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$ DEF *Inv*, *1bInv2*
 2972 $\langle 4 \rangle 7. maxBalInv'$
 2973 BY DEF *Phase1c*, *Inv*, *maxBalInv*
 2974 $\langle 4 \rangle 8. 2avInv1'$
 2975 $\langle 5 \rangle 1. \text{SUFFICES ASSUME NEW } m1 \in bmsgs', \text{ NEW } m2 \in bmsgs',$
 2976 $\quad 2avInv1!(m1, m2)!1$
 2977 $\quad \text{PROVE } 2avInv1!(m1, m2)!2'$
 2978 BY DEF *2avInv1*
 2979 $\langle 5 \rangle 2. m1 \notin S \wedge m2 \notin S$
 2980 $\langle 6 \rangle 1. \forall m \in S : m.type = "1c"$
 2981 BY $\langle 4 \rangle 1$
 2982 $\langle 6 \rangle 2. \text{QED}$
 2983 BY $\langle 6 \rangle 1, \langle 5 \rangle 1$
 2984 $\langle 5 \rangle 3. m1 \in bmsgs \wedge m2 \in bmsgs$
 2985 BY $\langle 5 \rangle 2, \langle 4 \rangle 1$

2986 $\langle 5 \rangle 4$. QED
 2987 BY $\langle 5 \rangle 1, \langle 5 \rangle 3$ DEF $Inv, 2avInv1$
 2988 $\langle 4 \rangle 9$. $2avInv2'$
 2989 BY DEF $Phase1c, Inv, 2avInv2$
 2990 $\langle 4 \rangle 10$. $2avInv3'$
 2991 BY $\langle 4 \rangle 2$ DEF $Phase1c, Inv, 2avInv3$
 2992 $\langle 4 \rangle 11$. $accInv'$
 2993 BY $\langle 4 \rangle 2$ DEF $Phase1c, Inv, accInv$
 2994 $\langle 4 \rangle 12$. $knowsSentInv'$
 2995 BY DEF $Inv, knowsSentInv, msgsOfType, Phase1c$
 2996 $\langle 4 \rangle 13$. QED
 2997 BY $\langle 4 \rangle 3, \langle 4 \rangle 4, \langle 4 \rangle 5, \langle 4 \rangle 6, \langle 4 \rangle 7, \langle 4 \rangle 8, \langle 4 \rangle 9, \langle 4 \rangle 10,$
 2998 $\langle 4 \rangle 11, \langle 4 \rangle 12$ DEF Inv
 2999 $\langle 3 \rangle 3$. QED
 3000 BY $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 2 \rangle 2$
 3001 $\langle 2 \rangle 3$. ASSUME NEW $self \in FakeAcceptor,$
 3002 $FakingAcceptor(self)$
 3003 PROVE
 3004 Inv'
 3005 $\langle 3 \rangle$ USE $FakingAcceptor(self)$
 3006 $\langle 3 \rangle 1$. PICK $m \in 1bMessage \cup 2avMessage \cup 2bMessage :$
 3007 $\wedge m.acc \notin Acceptor$
 3008 $\wedge bmsgs' = bmsgs \cup \{m\}$
 3009 BY BQA DEF $FakingAcceptor$
 3010 $\langle 3 \rangle 2$. $msgs' = msgs$
 3011 BY $MsgsLemma$ DEF Inv
 3012 $\langle 3 \rangle 3$. $TypeOK'$
 3013 BY $\langle 3 \rangle 1$ DEF $Inv, TypeOK, BMessage, FakingAcceptor$
 3014 $\langle 3 \rangle 4$. $bmsgsFinite'$
 3015 BY $\langle 3 \rangle 1, FiniteMsgsLemma$ DEF $Inv, TypeOK$
 3016 $\langle 3 \rangle 5$. $1bInv1'$
 3017 $\langle 4 \rangle 1$. SUFFICES ASSUME NEW $mm \in bmsgs',$
 3018 $1bInv1!(mm)!1$
 3019 PROVE $1bInv1!(mm)!2'$
 3020 BY DEF $1bInv1$
 3021 $\langle 4 \rangle 2$. $mm \in bmsgs$
 3022 BY $\langle 4 \rangle 1, \langle 3 \rangle 1$
 3023 $\langle 4 \rangle 3$. QED
 3024 BY $\langle 4 \rangle 1, \langle 4 \rangle 2, \langle 3 \rangle 2$ DEF $Inv, 1bInv1$
 3025 $\langle 3 \rangle 6$. $1bInv2'$
 3026 $\langle 4 \rangle 1$. SUFFICES ASSUME NEW $m1 \in bmsgs',$ NEW $m2 \in bmsgs',$
 3027 $1bInv2!(m1, m2)!1$
 3028 PROVE $m1 = m2$
 3029 BY DEF $1bInv2$
 3030 $\langle 4 \rangle 2$. $m1 \in bmsgs \wedge m2 \in bmsgs$

3031 BY $\langle 4 \rangle 1, \langle 3 \rangle 1$
 3032 $\langle 4 \rangle 3$. QED
 3033 BY $\langle 4 \rangle 1, \langle 4 \rangle 2$ DEF *Inv*, *1bInv2*
 3034 $\langle 3 \rangle 7$. *maxBalInv'*
 3035 $\langle 4 \rangle 1$. SUFFICES ASSUME NEW $mm \in bmsgs'$,
 3036 $maxBalInv!(mm)!1$
 3037 PROVE $maxBalInv!(mm)!2'$
 3038 BY DEF *maxBalInv*
 3039 $\langle 4 \rangle 2$. $mm \in bmsgs$
 3040 BY $\langle 4 \rangle 1, \langle 3 \rangle 1$
 3041 $\langle 4 \rangle 3$. QED
 3042 BY $\langle 4 \rangle 1, \langle 4 \rangle 2$ DEF *Inv*, *maxBalInv*, *FakingAcceptor*
 3043 $\langle 3 \rangle 8$. *2avInv1'*
 3044 $\langle 4 \rangle 1$. SUFFICES ASSUME NEW $m1 \in bmsgs'$, NEW $m2 \in bmsgs'$,
 3045 $2avInv1!(m1, m2)!1$
 3046 PROVE $m1 = m2$
 3047 BY DEF *2avInv1*
 3048 $\langle 4 \rangle 2$. $m1 \in bmsgs \wedge m2 \in bmsgs$
 3049 BY $\langle 4 \rangle 1, \langle 3 \rangle 1$
 3050 $\langle 4 \rangle 3$. QED
 3051 BY $\langle 4 \rangle 1, \langle 4 \rangle 2$ DEF *Inv*, *2avInv1*
 3052 $\langle 3 \rangle 9$. *2avInv2'*
 3053 $\langle 4 \rangle 1$. SUFFICES ASSUME NEW $mm \in bmsgs'$,
 3054 $2avInv2!(mm)!1$
 3055 PROVE $2avInv2!(mm)!2'$
 3056 BY DEF *2avInv2*
 3057 $\langle 4 \rangle 2$. $mm \in bmsgs$
 3058 BY $\langle 4 \rangle 1, \langle 3 \rangle 1$
 3059 $\langle 4 \rangle 3$. QED
 3060 BY $\langle 4 \rangle 1, \langle 4 \rangle 2$ DEF *Inv*, *2avInv2*, *FakingAcceptor*
 3061 $\langle 3 \rangle 10$. *2avInv3'*
 3062 $\langle 4 \rangle 1$. SUFFICES ASSUME NEW $mm \in bmsgs'$,
 3063 $2avInv3!(mm)!1$
 3064 PROVE $2avInv3!(mm)!2'$
 3065 BY DEF *2avInv3*
 3066 $\langle 4 \rangle 2$. $mm \in bmsgs$
 3067 BY $\langle 4 \rangle 1, \langle 3 \rangle 1$
 3068 $\langle 4 \rangle 3$. QED
 3069 BY $\langle 4 \rangle 1, \langle 4 \rangle 2, \langle 3 \rangle 2$ DEF *Inv*, *2avInv3*
 3070 $\langle 3 \rangle 11$. *accInv'*
 3071 BY $\langle 3 \rangle 2$ DEF *Inv*, *accInv*, *FakingAcceptor*
 3072 $\langle 3 \rangle 12$. *knowsSentInv'*
 3073 $\langle 4 \rangle$ SUFFICES ASSUME NEW $a \in Acceptor$
 3074 PROVE $knowsSent'[a] \subseteq msgsOfType("1b")'$
 3075 BY DEF *knowsSentInv*

```

3076      <4>1.  $msgsOfType("1b") \subseteq msgsOfType("1b")'$ 
3077      BY <3>1 DEF  $msgsOfType$ 
3078      <4>2. QED
3079      BY <4>1 DEF  $FakingAcceptor, Inv, knowsSentInv$ 
3080      <3>13. QED
3081      BY <3>3, <3>4, <3>5, <3>6, <3>7, <3>8, <3>9, <3>10,
3082      <3>11, <3>12 DEF  $Inv$ 
3083      <2>4. ASSUME UNCHANGED  $vars$ 
3084      PROVE  $Inv'$ 
3085      <3> USE UNCHANGED  $vars$  DEF  $Inv, vars$ 
3086      <3>  $msgs = msgs'$ 
3087      BY DEF  $msgs, msgsOfType, 1bmsgs, 1bRestrict, acceptorMsgsOfType, 1cmsgs,$ 
3088       $KnowsSafeAt, 2amsgs$ 
3089      <3> QED
3090      BY DEF  $TypeOK, bmsgsFinite, 1bOr2bMsgs, 1bInv1, 1bInv2,$ 
3091       $maxBallInv, 2avInv1, 2avInv2, 2avInv3, accInv, knowsSentInv, msgsOfType$ 
3092      <2>5. QED
3093      BY <2>1, <2>2, <2>3, <2>4,  $NextDef$ 

3095      <1>3. QED
      BY <1>1, <1>2,  $RuleInv1$  DEF  $Spec$ 

3099      PROOF OMITTED
3100 |-----|
      We next use the invariance of  $Inv$  to prove that algorithm  $BPCon$  implements algorithm
       $PaxosConsensus$  under the refinement mapping defined by the INSTANCE statement above. Again,
      we must omit the trivial temporal logic proofs until temporal logic reasoning is implemented in
       $TLAPS$ .

3108      THEOREM  $Spec \Rightarrow P!Spec$ 
3109      <1>1.  $Init \Rightarrow P!Init$ 
3110      <2> SUFFICES ASSUME  $Init$ 
3111      PROVE  $P!Init$ 
3112      OBVIOUS
3113      <2>1.  $MaxBallot(\{\}) = -1$ 
3114      BY  $MaxBallotProp, EmptySetFinite$ 
3115      <2>2.  $P!Init!1$ 
3116      BY <2>1 DEF  $Init, PmaxBal, 1bOr2bMsgs$ 
3117      <2>3.  $P!Init!2 \wedge P!Init!3$ 
3118      BY DEF  $Init, None, P!None$ 
3119      <2>4.  $msgs = \{\}$ 
3120      <3>1.  $msgsOfType("1a") = \{\} \wedge acceptorMsgsOfType("2b") = \{\}$ 
3121      BY DEF  $Init, msgsOfType, acceptorMsgsOfType$ 
3122      <3>2.  $1bmsgs = \{\} \wedge 1cmsgs = \{\}$ 
3123      BY DEF  $Init, msgsOfType, acceptorMsgsOfType, 1bmsgs, 1cmsgs$ 
3124      <3>3.  $2amsgs = \{\}$ 
3125      <4>1.  $\{\} \notin Quorum$ 

```


3126 BY *BQA* DEF *Quorum*
 3127 $\langle 4 \rangle 2.$ *acceptorMsgsOfType*("2av") = {}
 3128 BY DEF *Init*, *msgsOfType*, *acceptorMsgsOfType*
 3129 $\langle 4 \rangle$ QED
 3130 BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$ DEF *2amsgs*
 3131 $\langle 3 \rangle 4.$ QED
 3132 BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$ DEF *msgs*
 3133 $\langle 2 \rangle 5.$ QED
 3134 BY $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$ DEF *P!Init*

 3136 $\langle 1 \rangle 2.$ $Inv \wedge Inv' \wedge [Next]_{vars} \Rightarrow [P!Next]_P!vars$
 3137 $\langle 2 \rangle$ $InvP \triangleq Inv'$ We probably don't need to assume *Inv'*
 3138 $\langle 2 \rangle 1.$ UNCHANGED *vars* \Rightarrow UNCHANGED *P!vars*
 3139 $\langle 3 \rangle$ SUFFICES ASSUME UNCHANGED *vars*
 3140 PROVE UNCHANGED *P!vars*
 3141 OBVIOUS
 3142 $\langle 3 \rangle 1.$ UNCHANGED $\langle maxVBal, maxVVal \rangle$
 3143 BY DEF *vars*
 3144 $\langle 3 \rangle 2.$ UNCHANGED *PmaxBal*
 3145 BY DEF *vars*, *PmaxBal*, *1bOr2bMsgs*
 3146 $\langle 3 \rangle 3.$ UNCHANGED *msgs*
 3147 $\langle 4 \rangle$ USE DEF *vars*
 3148 $\langle 4 \rangle 1.$ UNCHANGED $\langle msgsOfType("1a"), acceptorMsgsOfType("2b"), 1bmsgs \rangle$
 3149 BY DEF *msgsOfType*, *acceptorMsgsOfType*, *1bmsgs*, *2amsgs*
 3150 $\langle 4 \rangle 2.$ UNCHANGED *1cmsgs*
 3151 BY DEF *1cmsgs*, *msgsOfType*, *KnowsSafeAt*
 3152 $\langle 4 \rangle 3.$ UNCHANGED *2amsgs*
 3153 BY DEF *2amsgs*, *msgsOfType*, *acceptorMsgsOfType*
 3154 $\langle 4 \rangle 4.$ QED
 3155 BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEF *msgs*
 3156 $\langle 3 \rangle 4.$ QED
 3157 BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$ DEF *P!vars*
 3158 $\langle 2 \rangle$ SUFFICES ASSUME *Inv*, *InvP*, *Next*
 3159 PROVE $P!TLANext \vee P!vars' = P!vars$
 3160 $\langle 3 \rangle 1.$ $Inv \wedge [Next]_{vars} \Rightarrow Inv \wedge [Next]_{vars}$
 3161 BY DEF *Inv*
 3162 $\langle 3 \rangle 2.$ UNCHANGED *vars* \Rightarrow UNCHANGED *P!vars*
 3163 $\langle 4 \rangle$ HAVE UNCHANGED *vars*
 3164 $\langle 4 \rangle$ USE DEF *vars*
 3165 $\langle 4 \rangle 1.$ UNCHANGED *PmaxBal*
 3166 BY DEF *PmaxBal*, *1bOr2bMsgs*
 3167 $\langle 4 \rangle 2.$ UNCHANGED *msgs*
 3168 $\langle 5 \rangle 1.$ \wedge UNCHANGED *msgsOfType*("1a")
 3169 \wedge UNCHANGED *acceptorMsgsOfType*("2b")
 3170 BY DEF *msgsOfType*, *acceptorMsgsOfType*

```

3171      ⟨5⟩2. UNCHANGED 1bmsgs
3172      BY DEF 1bmsgs, msgsOfType, acceptorMsgsOfType
3173      ⟨5⟩3. UNCHANGED 1cmsgs
3174      BY DEF 1cmsgs, msgsOfType, KnowsSafeAt
3175      ⟨5⟩4. UNCHANGED 2amsgs
3176      BY DEF 2amsgs, msgsOfType, acceptorMsgsOfType
3177      ⟨5⟩5. QED
3178      BY ⟨5⟩1, ⟨5⟩2, ⟨5⟩3, ⟨5⟩4 DEF msgs
3179      ⟨4⟩3. QED
3180      BY ⟨4⟩1, ⟨4⟩2 DEF P!vars, PmaxBal, 1bOr2bMsgs
3181      ⟨3⟩3. Inv ∧ P!TLANext ⇒ P!Next
3182      BY ⟨3⟩1, ⟨3⟩2, PNextDef
3183      DEF Inv, P!ProcSet, P!Init, Ballot, P!Ballot
3184      ⟨3⟩ QED
3185      BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, P!NextDef, NextDef DEF Inv
3186      ⟨2⟩ HIDE DEF InvP
3187      ⟨2⟩2. ∀ a ∈ Acceptor : PmaxBal[a] ∈ Ballot ∪ {−1}
3188      ⟨3⟩ SUFFICES ASSUME NEW a ∈ Acceptor
3189      PROVE PmaxBal[a] ∈ Ballot ∪ {−1}
3190      OBVIOUS
3191      ⟨3⟩ DEFINE S ≜ {m.bal : m ∈ {ma ∈ bmsgs :
3192      ∧ ma.type ∈ {"1b", "2b"}
3193      ∧ ma.acc = a}}
3194      ⟨3⟩1. PmaxBal[a] = MaxBallot(S)
3195      BY DEF PmaxBal, 1bOr2bMsgs
3196      ⟨3⟩2. ∧ IsFiniteSet(S)
3197      ∧ S ∈ SUBSET Ballot
3198      BY PMaxBalLemma3 DEF Inv
3199      ⟨3⟩3.CASE S = {}
3200      BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, MaxBallotProp
3201      ⟨3⟩4.CASE S ≠ {}
3202      BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩4, MaxBallotProp
3203      ⟨3⟩5. QED
3204      BY ⟨3⟩3, ⟨3⟩4
3205      ⟨2⟩3. ASSUME NEW self ∈ Acceptor, NEW b ∈ Ballot,
3206      Phase1b(self, b)
3207      PROVE P!TLANext ∨ P!vars' = P!vars
3208      ⟨3⟩1. ∧ P!sentMsgs("1a", b) ≠ {}
3209      ∧ msgs' = msgs ∪ {[type ↦ "1b", acc ↦ self, bal ↦ b,
3210      mbal ↦ maxVBal[self], mval ↦ maxVVal[self]]}
3211      ⟨4⟩1.⟨3⟩1!2
3212      BY ⟨2⟩3, MsgsLemma DEF Inv
3213      ⟨4⟩2. PICK m ∈ sentMsgs("1a", b) : m.type = "1a" ∧ m.bal = b
3214      BY ⟨2⟩3 DEF Phase1b, sentMsgs
3215      ⟨4⟩3. m ∈ msgsOfType("1a")

```

3216 BY $\langle 4 \rangle 2$ DEF *sentMsgs*, *msgsOfType*
 3217 $\langle 4 \rangle 4$. $m \in \text{msgs}$
 3218 BY $\langle 4 \rangle 3$ DEF *msgs*
 3219 $\langle 4 \rangle 5$. $m \in P!\text{sentMsgs}(\text{"1a"}, b)$
 3220 BY $\langle 4 \rangle 4$, $\langle 4 \rangle 2$ DEF $P!\text{sentMsgs}$
 3221 $\langle 4 \rangle 6$. QED
 3222 BY $\langle 4 \rangle 1$, $\langle 4 \rangle 5$
 3223 $\langle 3 \rangle 2$. UNCHANGED $\langle \text{maxVVal}, \text{maxVVal} \rangle$
 3224 BY $\langle 2 \rangle 3$ DEF *Phase1b*
 3225 $\langle 3 \rangle 3$. $\wedge b > P\text{maxBal}[\text{self}]$
 3226 $\wedge P\text{maxBal}' = [P\text{maxBal} \text{ EXCEPT } ![\text{self}] = b]$
 3227 $\langle 4 \rangle 1$. $b > P\text{maxBal}[\text{self}]$
 3228 $\langle 5 \rangle 1$. $b > \text{maxBal}[\text{self}]$
 3229 BY $\langle 2 \rangle 3$ DEF *Phase1b*
 3230 $\langle 5 \rangle 2$. $\text{maxBal}[\text{self}] \in \text{Ballot} \cup \{-1\}$
 3231 BY DEF *Inv*, *TypeOK*
 3232 $\langle 5 \rangle 3$. $\forall \text{pmb}, \text{mb} \in \text{Ballot} \cup \{-1\}$:
 3233 $b > \text{mb} \wedge \text{pmb} \leq \text{mb} \Rightarrow b > \text{pmb}$
 3234 BY *SimpleArithmetic* DEF *Ballot*
 3235 $\langle 5 \rangle 4$. QED
 3236 BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$, *PmaxBalLemma4*, $\langle 2 \rangle 2$ DEF *Inv*
 3237 $\langle 4 \rangle$ DEFINE $m \triangleq [\text{type} \mapsto \text{"1b"}, \text{bal} \mapsto b, \text{acc} \mapsto \text{self},$
 3238 $\text{m2av} \mapsto 2\text{avSent}[\text{self}],$
 3239 $\text{mbal} \mapsto \text{maxVVal}[\text{self}], \text{mval} \mapsto \text{maxVVal}[\text{self}]]$
 3240 $\text{mA}(a) \triangleq \{\text{ma} \in \text{bmsgs} : \wedge \text{ma.type} \in \{\text{"1b"}, \text{"2b"}\}$
 3241 $\wedge \text{ma.acc} = a\}$
 3242 $S(a) \triangleq \{\text{ma.bal} : \text{ma} \in \text{mA}(a)\}$
 3243 $\langle 4 \rangle 2$. $\text{bmsgs}' = \text{bmsgs} \cup \{m\}$
 3244 BY $\langle 2 \rangle 3$ DEF *Phase1b*
 3245 $\langle 4 \rangle 3$. $\text{mA}(\text{self})' = \text{mA}(\text{self}) \cup \{m\}$
 3246 $\langle 5 \rangle 1$. $\text{mA}(\text{self})' = \text{mA}(\text{self}) \cup \{\text{ma} \in \{m\} : \wedge \text{ma.type} \in \{\text{"1b"}, \text{"2b"}\}$
 3247 $\wedge \text{ma.acc} = \text{self}\}$
 3248 BY $\langle 4 \rangle 2$
 3249 $\langle 5 \rangle 2$. $\text{m.type} = \text{"1b"} \wedge \text{m.acc} = \text{self}$
 3250 OBVIOUS
 3251 $\langle 5 \rangle 3$. $\forall \text{ma} \in \{m\} : \text{ma.type} = \text{"1b"} \wedge \text{ma.acc} = \text{self}$
 3252 BY $\langle 5 \rangle 2$
 3253 $\langle 5 \rangle 4$. QED
 3254 BY $\langle 5 \rangle 1$, $\langle 5 \rangle 3$
 3255 $\langle 4 \rangle 4$. $\wedge P\text{maxBal} = [a \in \text{Acceptor} \mapsto \text{MaxBallot}(S(a))]$
 3256 $\wedge P\text{maxBal}' = [a \in \text{Acceptor} \mapsto \text{MaxBallot}(S(a))']$
 3257 BY DEF *PmaxBal*, *1bOr2bMsgs*
 3258 $\langle 4 \rangle$ HIDE DEF *mA*
 3259 $\langle 4 \rangle 5$. $S(\text{self})' = S(\text{self}) \cup \{b\}$
 3260 BY $\langle 4 \rangle 3$, $\text{m.bal} = b$

3261 $\langle 4 \rangle 6. \text{MaxBallot}(S(\text{self}) \cup \{b\}) = b$
3262 $\langle 5 \rangle 1. b > \text{MaxBallot}(S(\text{self}))$
3263 BY $\langle 4 \rangle 1, \langle 4 \rangle 4$
3264 $\langle 5 \rangle$ DEFINE $SS \triangleq S(\text{self}) \cup \{b\}$
3265 $\langle 5 \rangle 2. b \in SS$
3266 OBVIOUS
3267 $\langle 5 \rangle 3. \text{IsFiniteSet}(S(\text{self}))$
3268 $\langle 6 \rangle 1. \text{IsFiniteSet}(1b\text{Or}2b\text{Msgs})$
3269 BY DEF $Inv, b\text{msgsFinite}$
3270 $\langle 6 \rangle 2. \text{IsFiniteSet}(mA(\text{self}))$
3271 BY $\langle 6 \rangle 1, \text{SubsetOfFiniteSetFinite}$ DEF $mA, 1b\text{Or}2b\text{Msgs}$
3272 $\langle 6 \rangle$ DEFINE $f[ma \in mA(\text{self})] \triangleq ma.bal$
3273 $\langle 6 \rangle 3. S(\text{self}) = \{f[ma] : ma \in mA(\text{self})\}$
3274 OBVIOUS
3275 $\langle 6 \rangle$ HIDE DEF f
3276 $\langle 6 \rangle 4.$ QED
3277 BY $\langle 6 \rangle 2, \langle 6 \rangle 3, \text{ImageOfFiniteSetFinite}$
3278 $\langle 5 \rangle 4. \text{IsFiniteSet}(SS)$
3279 BY $\langle 5 \rangle 3, \text{SingletonSetFinite}, \text{UnionOfFiniteSetsFinite}$
3280 $\langle 5 \rangle 5. SS \subseteq \text{Ballot} \cup \{-1\}$
3281 $\langle 6 \rangle 1.$ ASSUME NEW $mm \in mA(\text{self})$
3282 PROVE $mm.bal \in \text{Ballot} \cup \{-1\}$
3283 $\langle 7 \rangle 1. mm \in b\text{msgs} \wedge mm.type \in \{“1b”, “2b”\}$
3284 BY DEF mA
3285 $\langle 7 \rangle 2.$ CASE $mm.type = “1b”$
3286 BY $\langle 7 \rangle 1, \langle 7 \rangle 2, \text{BMessageLemma}$ DEF $Inv, \text{TypeOK}, 1b\text{Message}$
3287 $\langle 7 \rangle 3.$ CASE $mm.type = “2b”$
3288 BY $\langle 7 \rangle 1, \langle 7 \rangle 2, \text{BMessageLemma}$ DEF $Inv, \text{TypeOK}, 2b\text{Message}$
3289 $\langle 7 \rangle 4.$ QED
3290 BY $\langle 7 \rangle 1, \langle 7 \rangle 2, \langle 7 \rangle 3$
3291 $\langle 6 \rangle 2.$ QED
3292 BY $\langle 6 \rangle 1$
3293 $\langle 5 \rangle 6. \forall x \in SS : b \geq x$
3294 $\langle 6 \rangle 1. b \geq b$
3295 BY SimpleArithmetic DEF Ballot
3296 $\langle 6 \rangle 2.$ SUFFICES ASSUME NEW $x \in S(\text{self})$
3297 PROVE $b \geq x$
3298 BY $\langle 6 \rangle 1$
3299 $\langle 6 \rangle 3. S(\text{self}) \neq \{\}$
3300 OBVIOUS
3301 $\langle 6 \rangle$ HIDE DEF S
3302 $\langle 6 \rangle 4. \wedge \text{MaxBallot}(S(\text{self})) \in S(\text{self})$
3303 $\wedge \text{MaxBallot}(S(\text{self})) \geq x$
3304 BY $\langle 5 \rangle 3, \langle 5 \rangle 5, \langle 6 \rangle 3, \text{MaxBallotProp}, \text{IsFiniteSet}(S(\text{self}))$
3305 $\langle 6 \rangle 5. b > \text{MaxBallot}(S(\text{self}))$

3306 BY $\langle 5 \rangle 1, \langle 4 \rangle 4$
3307 $\langle 6 \rangle 6. \wedge \text{MaxBallot}(S(\text{self})) \in \text{Ballot} \cup \{-1\}$
3308 $\wedge x \in \text{Ballot} \cup \{-1\}$
3309 BY $\langle 5 \rangle 5, \langle 6 \rangle 4$
3310 $\langle 6 \rangle 7. \forall mbs \in \text{Ballot} \cup \{-1\} :$
3311 $b > mbs \wedge mbs \geq x \Rightarrow b \geq x$
3312 BY $\langle 6 \rangle 6, \text{SimpleArithmetic}$ DEF *Ballot*
3313 $\langle 6 \rangle 8.$ QED
3314 BY $\langle 5 \rangle 1, \langle 6 \rangle 4, \langle 6 \rangle 6, \langle 6 \rangle 7$
3315 $\langle 5 \rangle 7.$ QED
3316 $\langle 6 \rangle$ HIDE DEF *SS*
3317 $\langle 6 \rangle 1. b = \text{MaxBallot}(SS)$
3318 BY $\langle 5 \rangle 2, \langle 5 \rangle 4, \langle 5 \rangle 5, \langle 5 \rangle 6, \text{MaxBallotLemma1}$
3319 $\langle 6 \rangle 2.$ QED
3320 BY $\langle 6 \rangle 1$ DEF *SS*
3321 $\langle 4 \rangle 7. \forall a \in \text{Acceptor} : a \neq \text{self} \Rightarrow S(a)' = S(a)$
3322 $\langle 5 \rangle$ USE DEF *mA*
3323 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $a \in \text{Acceptor}, a \neq \text{self}$
3324 PROVE $S(a)' = S(a)$
3325 OBVIOUS
3326 $\langle 5 \rangle 2. m.\text{acc} \neq a$
3327 BY $\langle 5 \rangle 1$
3328 $\langle 5 \rangle 3. mA(a)' = mA(a)$
3329 $\langle 6 \rangle 1.$ ASSUME NEW $mm \in mA(a)'$
3330 PROVE $mm \in mA(a)$
3331 BY $\langle 4 \rangle 2, \langle 5 \rangle 2, mm.\text{acc} = a$ $\langle 7 \rangle 3$
3332 $\langle 6 \rangle 2.$ ASSUME NEW $mm \in mA(a)$
3333 PROVE $mm \in mA(a)'$
3334 BY $\langle 4 \rangle 2$
3335 $\langle 6 \rangle 3.$ QED
3336 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$
3337 $\langle 5 \rangle 4.$ QED
3338 BY $\langle 5 \rangle 3$
3340 $\langle 4 \rangle 8. PmaxBal' = [PmaxBal \text{ EXCEPT } ![self] = b]$
3341 $\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $a \in \text{Acceptor}$
3342 PROVE $PmaxBal'[a] = \text{IF } a = \text{self} \text{ THEN } b$
3343 $\text{ELSE } PmaxBal[a]$
3344 BY DEF *PmaxBal, 1bOr2bMsgs*
3345 $\langle 5 \rangle 2. (a \neq \text{self}) \Rightarrow \text{MaxBallot}(S(a))' = \text{MaxBallot}(S(a))$
3346 BY $\langle 4 \rangle 7$
3347 $\langle 5 \rangle 3. (a \neq \text{self}) \Rightarrow PmaxBal'[a] = PmaxBal[a]$
3348 BY $\langle 4 \rangle 4, \langle 4 \rangle 7, \langle 5 \rangle 2$ DEF *PmaxBal, 1bOr2bMsgs*
3349 $\langle 5 \rangle$ QED
3350 BY $\langle 5 \rangle 2, \langle 4 \rangle 4, \langle 4 \rangle 5, \langle 4 \rangle 6$

3396 $\wedge mav.bal = b$
 3397 $\wedge mav.val = m.val$
 3398 BY $\langle 5 \rangle 2$ DEF $2amsgs$
 3399 $\langle 5 \rangle 4$. PICK $Q2 \in Quorum$:
 3400 $\forall a \in Q2$:
 3401 $\exists m2av \in acceptorMsgsOfType("2av")'$:
 3402 $\wedge m2av.acc = a$
 3403 $\wedge m2av.bal = b$
 3404 $\wedge m2av.val = v$
 3405 $\langle 6 \rangle 1$. $\wedge m2a.type = "2a"$
 3406 $\wedge m2a.bal = b$
 3407 $\wedge m2a.val = v$
 3408 OBVIOUS
 3409 $\langle 6 \rangle 2$. $m2a \in 2amsgs'$
 3410 BY $\langle 4 \rangle 1, \langle 6 \rangle 1, m2a \in msgs', MsgsTypeLemmaPrime$
 3411 $\langle 6 \rangle$ HIDE DEF $m2a$
 3412 $\langle 6 \rangle 3$. QED
 3413 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$ DEF $2amsgs$
 3414 $\langle 5 \rangle 5$. PICK $a \in Q \cap Q2 : a \in Acceptor$
 3415 BY *QuorumTheorem*
 3416 $\langle 5 \rangle 6$. PICK $mav \in acceptorMsgsOfType("2av")$:
 3417 $\wedge mav.acc = a$
 3418 $\wedge mav.bal = b$
 3419 $\wedge mav.val = m.val$
 3420 BY $\langle 5 \rangle 3, \langle 5 \rangle 5$
 3421 $\langle 5 \rangle 7$. PICK $m2av \in acceptorMsgsOfType("2av")'$:
 3422 $\wedge m2av.acc = a$
 3423 $\wedge m2av.bal = b$
 3424 $\wedge m2av.val = v$
 3425 BY $\langle 5 \rangle 4, \langle 5 \rangle 5$
 3426 $\langle 5 \rangle 8$. $mav \in acceptorMsgsOfType("2av")'$
 3427 BY $\langle 2 \rangle 4$ DEF *acceptorMsgsOfType, msgsOfType, Phase2av*
 3428 $\langle 5 \rangle 9$. $m2av = mav$
 3429 BY $\langle 5 \rangle 5, \langle 5 \rangle 6, \langle 5 \rangle 7, \langle 5 \rangle 8$ DEF $2avInv1, InvP, Inv, acceptorMsgsOfType, msgsOfType$
 3430 $\langle 5 \rangle 10$. $m = [type \mapsto "2a", bal \mapsto b, val \mapsto m.val]$
 3431 BY $\langle 5 \rangle 2$ DEF $2amsgs$
 3432 $\langle 5 \rangle 11$. QED
 3433 BY $\langle 5 \rangle 6, \langle 5 \rangle 7, \langle 5 \rangle 9, \langle 5 \rangle 10$
 3434 $\langle 4 \rangle 3$. $P!Phase2a(b, v)$
 3435 BY $\langle 2 \rangle 4, \langle 3 \rangle 1, \langle 4 \rangle 1, \langle 4 \rangle 2$ DEF $P!Phase2a, Phase2av$
 3436 $\langle 4 \rangle 4$. QED
 3437 BY $\langle 4 \rangle 3$ DEF $P!TLANext, Ballot, P!Ballot$
 3438 $\langle 3 \rangle 4$. QED
 3439 BY $\langle 3 \rangle 2, \langle 3 \rangle 3, MsgsLemma, \langle 2 \rangle 4$ DEF *Inv*
 3440 $\langle 2 \rangle 5$. ASSUME NEW $self \in Acceptor$, NEW $b \in Ballot$,

3441 $Phase2b(self, b)$
 3442 PROVE $P!TLANext \vee P!vars' = P!vars$
 3443 $\langle 3 \rangle$ USE $\langle 2 \rangle 5$
 3444 $\langle 3 \rangle 1. b \geq PmaxBal[self]$
 3445 $\langle 4 \rangle 1. PmaxBal[self] \leq maxBal[self]$
 3446 BY $PmaxBalLemma4$ DEF Inv
 3447 $\langle 4 \rangle 2. maxBal[self] \leq b$
 3448 BY DEF $Phase2b$
 3449 $\langle 4 \rangle 3. \forall pmb, mb \in Ballot \cup \{-1\} :$
 3450 $pmb \leq mb \wedge mb \leq b \Rightarrow b \geq pmb$
 3451 BY $SimpleArithmetic$ DEF $Ballot$
 3452 $\langle 4 \rangle 4.$ QED
 3453 BY $\langle 4 \rangle 1, \langle 4 \rangle 2, \langle 4 \rangle 3, PmaxBalLemma5$ DEF $Inv, TypeOK$
 3454 $\langle 3 \rangle 2.$ PICK $v \in Value :$
 3455 $\wedge \exists Q \in ByzQuorum :$
 3456 $\forall a \in Q :$
 3457 $\exists m \in sentMsgs("2av", b) : \wedge m.val = v$
 3458 $\wedge m.acc = a$
 3459 $\wedge msgs' = msgs \cup$
 3460 $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\}$
 3461 $\wedge bmsgs' = bmsgs \cup$
 3462 $\{[type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]\}$
 3463 $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = v]$
 3464 $\langle 4 \rangle 1. MsgsLemma!2!3$
 3465 BY $MsgsLemma$ DEF Inv
 3466 $\langle 4 \rangle 2. MsgsLemma!2!3!(self, b)!2$
 3467 BY $\langle 4 \rangle 1$
 3468 $\langle 4 \rangle 3.$ QED
 3469 BY $\langle 4 \rangle 2$
 3470 $\langle 3 \rangle$ DEFINE $m \triangleq [type \mapsto "2a", bal \mapsto b, val \mapsto v]$
 3471 $m2b \triangleq [type \mapsto "2b", acc \mapsto self, bal \mapsto b, val \mapsto v]$
 3472 $\langle 3 \rangle 3. m \in P!sentMsgs("2a", b)$
 3473 $\langle 4 \rangle 1. m \in 2amsgs$
 3474 $\langle 5 \rangle 1. m \in [type : \{"2a"\}, bal : Ballot, val : Value]$
 3475 OBVIOUS
 3476 $\langle 5 \rangle 2.$ PICK $Q \in Quorum :$
 3477 $\forall a \in Q :$
 3478 $\exists mm \in sentMsgs("2av", b) : \wedge mm.val = v$
 3479 $\wedge mm.acc = a$
 3480 $\langle 6 \rangle 1. \forall BQ \in ByzQuorum : \exists Q \in Quorum : Q \subseteq BQ$
 3481 BY DEF $Quorum$
 3482 $\langle 6 \rangle 2.$ QED
 3483 BY $\langle 3 \rangle 2, \langle 6 \rangle 1$ * need to first pick BQ in $ByzQuorum$
 3484 * and then let $Q \triangleq BQ \cap Acceptor$
 3485 $\langle 5 \rangle 3.$ ASSUME NEW $a \in Q$


```

3486      PROVE  $\exists m2av \in \text{acceptorMsgsOfType}("2av") :$ 
3487           $\wedge m2av.acc = a$ 
3488           $\wedge m2av.bal = m.bal$ 
3489           $\wedge m2av.val = m.val$ 
3490       $\langle 6 \rangle 1.$  PICK  $m2av \in \text{sentMsgs}("2av", b) : \wedge m2av.val = v$ 
3491           $\wedge m2av.acc = a$ 
3492      BY  $\langle 5 \rangle 2$ 
3493       $\langle 6 \rangle 2.$   $m2av \in \text{acceptorMsgsOfType}("2av")$ 
3494      BY  $\langle 6 \rangle 1$  DEF sentMsgs, Quorum, acceptorMsgsOfType, msgsOfType
3495       $\langle 6 \rangle$  WITNESS  $m2av \in \text{acceptorMsgsOfType}("2av")$ 
3496       $\langle 6 \rangle$  QED
3497      BY  $\langle 6 \rangle 1$  DEF sentMsgs
3498       $\langle 5 \rangle$  QED
3499      BY  $\langle 5 \rangle 1, \langle 5 \rangle 3$  DEF 2amsgs
3500       $\langle 4 \rangle 2.$  QED
3501      BY  $\langle 4 \rangle 1$  DEF P!sentMsgs, msgs
3502       $\langle 3 \rangle 4.$   $PmaxBal' = [PmaxBal \text{ EXCEPT } ![self] = b]$ 
3503       $\langle 4 \rangle 1.$  ASSUME NEW  $a \in \text{Acceptor},$ 
3504           $a \neq self$ 
3505      PROVE  $PmaxBal'[a] = PmaxBal[a]$ 
3506       $\langle 5 \rangle 1.$   $bmsgs' = bmsgs \cup \{m2b\} \wedge m2b.acc = self$ 
3507      BY  $\langle 3 \rangle 2$ 
3508       $\langle 5 \rangle 2.$  QED
3509      BY  $\langle 4 \rangle 1, \langle 5 \rangle 1, PmaxBalLemma2$ 
3510       $\langle 4 \rangle 2.$   $PmaxBal'[self] = b$ 
3511       $\langle 5 \rangle$  DEFINE  $S \triangleq \{mm.bal : mm \in \{ma \in bmsgs :$ 
3512           $\wedge ma.type \in \{"1b", "2b"\}$ 
3513           $\wedge ma.acc = self\}\}$ 
3514       $T \triangleq S \cup \{m2b.bal\}$ 
3515       $\langle 5 \rangle 1.$   $IsFiniteSet(S) \wedge (S \in \text{SUBSET } Ballot)$ 
3516      BY PMaxBalLemma3 DEF Inv
3517       $\langle 5 \rangle 2.$   $IsFiniteSet(T) \wedge (T \in \text{SUBSET } Ballot)$ 
3518      BY  $\langle 5 \rangle 1, OnePlusFinite$ 
3519       $\langle 5 \rangle 3.$   $PmaxBal[self] = MaxBallot(S)$ 
3520      BY DEF PmaxBal, 1bOr2bMsgs
3521       $\langle 5 \rangle 4.$   $PmaxBal'[self] = MaxBallot(T)$ 
3522      BY  $\langle 3 \rangle 2$  DEF PmaxBal, 1bOr2bMsgs
3523       $\langle 5 \rangle$  HIDE DEF S, T
3524       $\langle 5 \rangle 5.$  CASE  $S = \{\}$ 
3525           $\langle 6 \rangle 1.$   $T = \{b\} \cup \{\}$ 
3526          BY  $\langle 5 \rangle 5$  DEF T
3527           $\langle 6 \rangle 2.$   $\wedge b \geq b$ 
3528               $\wedge b \geq -1$ 
3529          BY SimpleArithmetic DEF Ballot
3530           $\langle 6 \rangle 3.$   $MaxBallot(\{b\}) = b$ 

```

3531 BY $\langle 6 \rangle 2$, *SingletonSetFinite*, *MaxBallotLemma1*
 3532 $\langle 6 \rangle 4$. *MaxBallot*($\{\}$) = -1
 3533 BY *EmptySetFinite*, *MaxBallotProp*
 3534 $\langle 6 \rangle$ QED
 3535 BY *SingletonSetFinite*, *EmptySetFinite*, $\langle 7 \rangle 1$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$, $\langle 6 \rangle 4$, *MaxBallotLemma2*, $\langle 5 \rangle 4$
 3536 $\langle 5 \rangle 6$. CASE $S \neq \{\}$
 3537 $\langle 6 \rangle 1$. $\forall bb \in S : PmaxBal[self] \geq bb$
 3538 BY $\langle 5 \rangle 1$, $\langle 5 \rangle 3$, *MaxBallotProp*
 3539 $\langle 6 \rangle 2$. ASSUME NEW $bb \in S$
 3540 PROVE $b \geq bb$
 3541 $\langle 7 \rangle 1$. $\forall pmb \in Ballot \cup \{-1\} :$
 3542 $b \geq pmb \wedge pmb \geq bb \Rightarrow b \geq bb$
 3543 BY *SimpleArithmetic* DEF *Ballot*
 3544 $\langle 7 \rangle 2$. QED
 3545 BY $\langle 6 \rangle 1$, $\langle 7 \rangle 1$, $\langle 3 \rangle 1$, *PmaxBalLemma5* DEF *Inv*
 3546 $\langle 6 \rangle 3$. $b \geq b$
 3547 BY *SimpleArithmetic* DEF *Ballot*
 3548 $\langle 6 \rangle 4$. $\forall bb \in T : b \geq bb$
 3549 BY $\langle 6 \rangle 2$, $\langle 6 \rangle 3$, $m2b.bal = b$ DEF *T*
 3550 $\langle 6 \rangle 5$. $b = MaxBallot(T)$
 3551 BY $\langle 5 \rangle 2$, $\langle 6 \rangle 4$, *MaxBallotLemma1* DEF *T*
 3552 $\langle 6 \rangle 6$. QED
 3553 BY $\langle 6 \rangle 5$, $\langle 5 \rangle 4$
 3554 $\langle 5 \rangle 7$. QED
 3555 BY $\langle 5 \rangle 5$, $\langle 5 \rangle 6$
 3556 $\langle 4 \rangle 3$. QED
 3557 BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$ DEF *PmaxBal*, *1bOr2bMsgs*
 3558 $\langle 3 \rangle 5$. $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = b]$
 3559 $\wedge maxVVal' = [maxVVal \text{ EXCEPT } ![self] = m.val]$
 3560 BY $\langle 3 \rangle 2$, $m.val = v$ DEF *Phase2b*
 3561 $\langle 3 \rangle 6$. QED
 3562 $\langle 4 \rangle 1$. $P!Phase2b(self, b)$
 3563 $\langle 5 \rangle 1$. $P!Phase2b(self, b)!2$
 3564 $\langle 6 \rangle$ USE $\langle 3 \rangle 3$
 3565 $\langle 6 \rangle 1$. WITNESS $m \in P!sentMsgs("2a", b)$
 3566 $\langle 6 \rangle 2$. QED
 3567 BY $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 2$
 3568 $\langle 5 \rangle 2$. QED
 3569 BY $\langle 5 \rangle 1$, $\langle 3 \rangle 1$ DEF $P!Phase2b$
 3570 $\langle 4 \rangle 2$. QED
 3571 BY $\langle 4 \rangle 1$ DEF $P!TLANext$, *Ballot*, $P!Ballot$
 3572 $\langle 2 \rangle 6$. ASSUME NEW $self \in Acceptor$, NEW $b \in Ballot$,
 3573 *LearnsSent*($self, b$)
 3574 PROVE $P!TLANext \vee P!vars' = P!vars$
 3575 $\langle 3 \rangle$ USE *LearnsSent*($self, b$)

3576 $\langle 3 \rangle 1.$ PICK $SM \in \text{SUBSET } \{m \in \text{msgsOfType}(\text{"1c"}) : m.\text{bal} = b\} :$
 3577 $\text{msgs}' = \text{msgs} \cup SM$
 3578 BY *MsgsLemma* DEF *Inv*
 3579 $\langle 3 \rangle$ DEFINE $S \triangleq \{m.\text{val} : m \in SM\}$
 3580 $\langle 3 \rangle 2.$ $S \in \text{SUBSET } \text{Value}$
 3581 $\langle 4 \rangle$ SUFFICES ASSUME NEW $m \in SM$
 3582 PROVE $m.\text{val} \in \text{Value}$
 3583 OBVIOUS
 3584 $\langle 4 \rangle$ QED
 3585 BY $m \in \text{msgsOfType}(\text{"1c"}), B\text{MessageLemma}$ DEF *Inv*, *TypeOK*, *msgsOfType*, *1cMessage*
 3586 $\langle 3 \rangle 3.$ $\text{msgs}' = \text{msgs} \cup \{[type \mapsto \text{"1c"}, bal \mapsto b, val \mapsto v] : v \in S\}$
 3587 $\langle 4 \rangle$ SUFFICES ASSUME NEW m
 3588 PROVE $m \in SM \equiv \wedge m = [type \mapsto \text{"1c"}, bal \mapsto b, val \mapsto m.\text{val}]$
 3589 $\wedge m.\text{val} \in S$
 3590 BY $\langle 3 \rangle 1$ DEF *msgsOfType*
 3591 $\langle 4 \rangle 1.$ ASSUME NEW $mm \in SM$
 3592 PROVE $\wedge mm = [type \mapsto \text{"1c"}, bal \mapsto b, val \mapsto mm.\text{val}]$
 3593 $\wedge mm.\text{val} \in S$
 3594 $\langle 5 \rangle 1.$ $\wedge mm \in b\text{msgs}$
 3595 $\wedge mm.\text{type} = \text{"1c"}$
 3596 $\wedge mm.\text{bal} = b$
 3597 BY $\langle 4 \rangle 1$ DEF *msgsOfType*
 3598 $\langle 5 \rangle 2.$ $mm \in 1c\text{Message}$
 3599 BY $\langle 5 \rangle 1, B\text{MessageLemma}$ DEF *Inv*, *TypeOK*
 3600 $\langle 5 \rangle 3.$ $mm = [type \mapsto mm.\text{type}, bal \mapsto mm.\text{bal}, val \mapsto mm.\text{val}]$
 3601 BY ONLY $\langle 5 \rangle 2$ DEF *1cMessage*
 3602 $\langle 5 \rangle 4.$ $mm.\text{val} \in S$
 3603 OBVIOUS
 3604 $\langle 5 \rangle 5.$ QED
 3605 BY $\langle 5 \rangle 1, \langle 5 \rangle 3, \langle 4 \rangle 1, \langle 5 \rangle 4$ DEF *1cMessage*
 3606 $\langle 4 \rangle 2.$ ASSUME $\wedge m = [type \mapsto \text{"1c"}, bal \mapsto b, val \mapsto m.\text{val}]$
 3607 $\wedge m.\text{val} \in S$
 3608 PROVE $m \in SM$
 3609 $\langle 5 \rangle 1.$ PICK $mm \in SM : mm.\text{val} = m.\text{val}$
 3610 BY $\langle 4 \rangle 2$
 3611 $\langle 5 \rangle 2.$ $mm = [type \mapsto \text{"1c"}, bal \mapsto b, val \mapsto mm.\text{val}]$
 3612 BY $\langle 4 \rangle 1$
 3613 $\langle 5 \rangle 3.$ QED
 3614 BY $\langle 4 \rangle 2, \langle 5 \rangle 1, \langle 5 \rangle 2$
 3615 $\langle 4 \rangle 3.$ QED
 3616 BY $\langle 4 \rangle 1, \langle 4 \rangle 2$
 3617 $\langle 3 \rangle 4.$ ASSUME NEW $v \in S$
 3618 PROVE $\exists Q \in \text{Quorum} : P!\text{ShowsSafeAt}(Q, b, v)$
 3619 $\langle 4 \rangle 1.$ ASSUME NEW $ac \in \text{Acceptor},$
 3620 $\text{KnowsSafeAt}(ac, b, v)'$

3621 PROVE $\exists Q \in \text{Quorum} : P! \text{ShowsSafeAt}(Q, b, v)$
 3622 $\langle 5 \rangle 1. \text{bmsgs}' = \text{bmsgs}$
 3623 BY DEF *LearnsSent*
 3624 $\langle 5 \rangle$ DEFINE $Q(BQ) \triangleq BQ \cap \text{Acceptor}$
 3625 $SS \triangleq \{m \in \text{knowsSent}'[ac] : m.bal = b\}$
 3626 $SQ(BQ) \triangleq \{1b\text{Restrict}(mm) :$
 3627 $mm \in \{m \in SS : m.acc \in Q(BQ)\}\}$
 3628 $Q1b(BQ) \triangleq \{m \in P! \text{sentMsgs}(\text{"1b"}, b) : m.acc \in Q(BQ)\}$
 3629 $\langle 5 \rangle 2.$ ASSUME NEW $BQ \in \text{ByzQuorum},$
 3630 $\forall a \in BQ : \exists m \in SS : m.acc = a$
 3631 PROVE $SQ(BQ) = Q1b(BQ)$
 3632 $\langle 6 \rangle 1.$ ASSUME NEW $m \in P! \text{sentMsgs}(\text{"1b"}, b),$
 3633 $m.acc \in Q(BQ)$
 3634 PROVE $m \in SQ(BQ)$
 3635 $\langle 7 \rangle 1. \wedge m \in 1\text{bmsgs}$
 3636 $\wedge m.type = \text{"1b"}$
 3637 $\wedge m.bal = b$
 3638 BY *MsgsTypeLemma* DEF $P! \text{sentMsgs}, \text{msgs}$
 3639 $\langle 7 \rangle 2.$ PICK $m1 \in \text{bmsgs} : \wedge m1.type = \text{"1b"}$
 3640 $\wedge m1.acc \in \text{Acceptor}$
 3641 $\wedge m = 1b\text{Restrict}(m1)$
 3642 BY $\langle 7 \rangle 1$ DEF $1\text{bmsgs}, \text{acceptorMsgsOfType}, \text{msgsOfType}$
 3643 $\langle 7 \rangle 3. m1.bal = b$
 3644 BY $\langle 7 \rangle 1, \langle 7 \rangle 2$ DEF $1b\text{Restrict}$
 3645 $\langle 7 \rangle 4.$ PICK $m2 \in \text{knowsSent}[ac]'$:
 3646 $\wedge m2.bal = b$
 3647 $\wedge m2.acc = m.acc$
 3648 BY $\langle 5 \rangle 2, \langle 6 \rangle 1$
 3649 $\langle 7 \rangle 5. m2 \in \text{bmsgs} \wedge m2.type = \text{"1b"}$
 3650 BY $\langle 5 \rangle 1$ DEF $\text{InvP}, \text{Inv}, \text{knowsSentInv}, \text{msgsOfType}$
 3651 $\langle 7 \rangle 6. \wedge m1.acc = m.acc$
 3652 $\wedge m1.bal = b$
 3653 BY $\langle 7 \rangle 1, \langle 7 \rangle 2$ DEF $1b\text{Restrict}$
 3654 $\langle 7 \rangle 7. m1 = m2$
 3655 BY $\langle 7 \rangle 2, \langle 7 \rangle 4, \langle 7 \rangle 5, \langle 7 \rangle 6, \langle 7 \rangle 7$ DEF $\text{Inv}, 1b\text{Inv2}$
 3656 $\langle 7 \rangle 8. m2 \in SS \wedge m2.acc \in Q(BQ)$
 3657 BY $\langle 7 \rangle 7, \langle 6 \rangle 1, \langle 7 \rangle 2, \langle 7 \rangle 4$
 3658 $\langle 7 \rangle 9.$ QED
 3659 BY $\langle 7 \rangle 8, \langle 7 \rangle 7, \langle 7 \rangle 2$
 3660 $\langle 6 \rangle 2.$ ASSUME NEW $m \in SS,$
 3661 $m.acc \in Q(BQ)$
 3662 PROVE $1b\text{Restrict}(m) \in Q1b(BQ)$
 3663 $\langle 7 \rangle 1. \wedge m \in \text{bmsgs}$
 3664 $\wedge m.bal = b$
 3665 $\wedge m.type = \text{"1b"}$

3666 BY $\langle 5 \rangle 1$ DEF $InvP, Inv, knowsSentInv, msgsOfType$
 3667 $\langle 7 \rangle 2. m \in acceptorMsgsOfType("1b")$
 3668 BY $\langle 7 \rangle 1, \langle 6 \rangle 2$ DEF $acceptorMsgsOfType, msgsOfType$
 3669 $\langle 7 \rangle 3. 1bRestrict(m) \in msgs$
 3670 BY $\langle 7 \rangle 2$ DEF $msgs, 1bmsgs$
 3671 $\langle 7 \rangle 4.$ QED
 3672 BY $\langle 6 \rangle 2, \langle 7 \rangle 1, \langle 7 \rangle 3$ DEF $P!sentMsgs, 1bRestrict$
 3673 $\langle 6 \rangle 3.$ QED
 3674 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$ DEF $Q1b, SQ$
 3675 $\langle 5 \rangle 3.$ CASE $KnowsSafeAt(ac, b, v)!1!1'$
 3676 $\langle 6 \rangle 1.$ PICK $BQ \in ByzQuorum : KnowsSafeAt(ac, b, v)!1!1!(BQ)'$
 3677 OBVIOUS
 3678 $\langle 6 \rangle 2. Q(BQ) \in Quorum$
 3679 BY DEF $Quorum$
 3680 $\langle 6 \rangle 3. \forall a \in Q(BQ) : \exists m \in SS : \wedge m.acc = a$
 3681 $\wedge m.mbal = -1$
 3682 BY $\langle 6 \rangle 1$
 3683 $\langle 6 \rangle 4. \forall a \in Q(BQ) : \exists m \in SQ(BQ) : \wedge m.acc = a$
 3684 $\wedge m.mbal = -1$
 3685 $\langle 7 \rangle$ HIDE DEF SS
 3686 $\langle 7 \rangle$ TAKE $a \in Q(BQ)$
 3687 $\langle 7 \rangle 1.$ PICK $m \in SS : m.acc = a \wedge m.mbal = -1$
 3688 BY $\langle 6 \rangle 3$
 3689 $\langle 7 \rangle 2. 1bRestrict(m) \in SQ(BQ)$
 3690 BY $\langle 7 \rangle 1$
 3691 $\langle 7 \rangle$ WITNESS $1bRestrict(m) \in SQ(BQ)$
 3692 $\langle 7 \rangle 3.$ QED
 3693 BY $\langle 7 \rangle 1$ DEF $1bRestrict$
 3694 $\langle 6 \rangle 5. \forall m \in SQ(BQ) : m.mbal = -1$
 3695 $\langle 7 \rangle$ TAKE $mm \in SQ(BQ)$
 3696 $\langle 7 \rangle 1.$ PICK $m \in SS : \wedge m \in knowsSent[ac]'$
 3697 $\wedge m.bal = b$
 3698 $\wedge m.acc \in Q(BQ)$
 3699 $\wedge mm = 1bRestrict(m)$
 3700 OBVIOUS
 3701 $\langle 7 \rangle 2.$ PICK $mm1 \in SQ(BQ) : \wedge mm1.acc = m.acc$
 3702 $\wedge mm1.mbal = -1$
 3703 BY $\langle 7 \rangle 1, \langle 6 \rangle 4$
 3704 $\langle 7 \rangle 3.$ PICK $m1 \in SS : \wedge m1 \in knowsSent[ac]'$
 3705 $\wedge m1.bal = b$
 3706 $\wedge m1.acc \in Q(BQ)$
 3707 $\wedge mm1 = 1bRestrict(m1)$
 3708 OBVIOUS
 3709 $\langle 7 \rangle 4. m.acc \in Acceptor$
 3710 BY $\langle 7 \rangle 1$

3711 $\langle 7 \rangle 5. \wedge m \in bmsgs \wedge m1 \in bmsgs$
3712 $\wedge m.type = \text{"1b"} \wedge m1.type = \text{"1b"}$
3713 BY $\langle 5 \rangle 1, \langle 7 \rangle 1, \langle 7 \rangle 3$ DEF $InvP, Inv, knowsSentInv, msgsOfType$
3714 $\langle 7 \rangle 6. m.acc = m1.acc$
3715 BY $\langle 7 \rangle 2, \langle 7 \rangle 3$ DEF $1bRestrict$
3716 $\langle 7 \rangle 7. m = m1$
3717 BY $\langle 7 \rangle 5, \langle 7 \rangle 4, \langle 7 \rangle 1, \langle 7 \rangle 3, \langle 7 \rangle 6$ DEF $Inv, 1bInv2$
3718 $\langle 7 \rangle 8. m.mbal = -1$
3719 BY $\langle 7 \rangle 7, \langle 7 \rangle 2, \langle 7 \rangle 3$ DEF $1bRestrict$
3720 $\langle 7 \rangle 9.$ QED
3721 BY $\langle 7 \rangle 8, \langle 7 \rangle 1$ DEF $1bRestrict$
3722 $\langle 6 \rangle 6. SQ(BQ) = Q1b(BQ)$
3723 BY $\langle 5 \rangle 2, \langle 6 \rangle 1$
3724 $\langle 6 \rangle$ HIDE DEF SS, Q, SQ
3725 $\langle 6 \rangle$ WITNESS $Q(BQ) \in Quorum$
3726 $\langle 6 \rangle 7.$ QED
3727 BY $\langle 6 \rangle 4, \langle 6 \rangle 5, \langle 6 \rangle 6$ DEF $P!ShowsSafeAt$
3728 $\langle 5 \rangle 4.$ CASE $KnowsSafeAt(ac, b, v)!1!2'$
3729 $\langle 6 \rangle 1.$ PICK $c \in 0 \dots (b-1) : KnowsSafeAt(ac, b, v)!1!2!(c)'$
3730 BY $\langle 5 \rangle 4$
3731 $\langle 6 \rangle 2.$ PICK $BQ \in ByzQuorum :$
3732 $\forall a \in BQ : \exists m \in SS : \wedge m.acc = a$
3733 $\wedge m.mbal \leq c$
3734 $\wedge (m.mbal = c) \Rightarrow (m.mval = v)$
3735 BY $\langle 6 \rangle 1$
3736 $\langle 6 \rangle 3. SQ(BQ) = Q1b(BQ)$
3737 BY $\langle 6 \rangle 2, \langle 5 \rangle 2$
3738 $\langle 6 \rangle 4. P!ShowsSafeAt(Q(BQ), b, v)!1!1$
3739 $\langle 7 \rangle 1.$ SUFFICES ASSUME NEW $a \in Q(BQ)$
3740 PROVE $\exists m \in Q1b(BQ) : m.acc = a$
3741 OBVIOUS
3742 $\langle 7 \rangle 2.$ PICK $m \in SS : m.acc = a$
3743 BY $\langle 6 \rangle 2$
3744 $\langle 7 \rangle 3. 1bRestrict(m) \in SQ(BQ)$
3745 BY $\langle 7 \rangle 2$
3746 $\langle 7 \rangle 4. 1bRestrict(m).acc = a$
3747 BY $\langle 7 \rangle 2$ DEF $1bRestrict$
3748 $\langle 7 \rangle 5.$ QED
3749 BY $\langle 6 \rangle 3, \langle 7 \rangle 3, \langle 7 \rangle 4$
3750 $\langle 6 \rangle 5.$ PICK $m1c \in msgs :$
3751 $\wedge m1c = [type \mapsto \text{"1c"}, bal \mapsto m1c.bal, val \mapsto v]$
3752 $\wedge m1c.bal \geq c$
3753 $\wedge m1c.bal \in Ballot$
3754 $\langle 7 \rangle 1.$ PICK $WQ \in WeakQuorum :$
3755 $\forall a \in WQ : \exists m \in SS : \wedge m.acc = a$

3756 $\wedge \exists r \in m.m2av :$
 3757 $\wedge r.bal \geq c$
 3758 $\wedge r.val = v$
 3759 BY $\langle 6 \rangle 1$
 3760 $\langle 7 \rangle 2$. PICK $a \in WQ, m \in SS :$
 3761 $\wedge a \in Acceptor$
 3762 $\wedge m.acc = a$
 3763 $\wedge \exists r \in m.m2av : \wedge r.bal \geq c$
 3764 $\wedge r.val = v$
 3765 $\langle 8 \rangle 1$. PICK $a \in WQ : a \in Acceptor$
 3766 BY BQA
 3767 $\langle 8 \rangle 2$. $\wedge a \in Acceptor$
 3768 $\wedge \langle 7 \rangle 1!(WQ)!(a)$
 3769 BY $\langle 7 \rangle 1, \langle 8 \rangle 1$
 3770 $\langle 8 \rangle 3$. QED
 3771 BY $\langle 8 \rangle 2$
 3772 $\langle 7 \rangle 3$. $\wedge m.bal = b$
 3773 $\wedge m \in bmsgs$
 3774 $\wedge m.type = "1b"$
 3775 BY $\langle 5 \rangle 1$ DEF $InvP, Inv, knowsSentInv, msgsOfType$
 3776 $\langle 7 \rangle 4$. PICK $r \in m.m2av : \wedge r.bal \geq c$
 3777 $\wedge r.val = v$
 3778 BY $\langle 7 \rangle 2$
 3779 $\langle 7 \rangle 5$. $r.bal \in Ballot$
 3780 BY $\langle 7 \rangle 2, \langle 7 \rangle 3, BMessageLemma$ DEF $Inv, TypeOK, 1bMessage$ $\langle 8 \rangle 2$
 3781 $\langle 7 \rangle 6$. $[type \mapsto "1c", bal \mapsto r.bal, val \mapsto r.val] \in msgs$
 3782 BY $\langle 7 \rangle 2, \langle 7 \rangle 3, \langle 7 \rangle 4$ DEF $Inv, 1bInv1$
 3783 $\langle 7 \rangle 7$. QED
 3784 BY $\langle 7 \rangle 2, \langle 7 \rangle 4, \langle 7 \rangle 5, \langle 7 \rangle 6$
 3785 $\langle 6 \rangle 6$. ASSUME NEW $m \in Q1b(BQ)$
 3786 PROVE $\wedge m1c.bal \geq m.mbal$
 3787 $\wedge (m1c.bal = m.mbal) \Rightarrow (m.mval = v)$
 3788 $\langle 7 \rangle 1$. $m.acc \in Q(BQ)$
 3789 OBVIOUS
 3790 $\langle 7 \rangle 2$. PICK $mm \in SS : \wedge mm.acc = m.acc$
 3791 $\wedge mm.mbal \leq c$
 3792 $\wedge (mm.mbal = c) \Rightarrow (mm.mval = v)$
 3793 BY $\langle 6 \rangle 2$
 3794 $\langle 7 \rangle 3$. PICK $mm2 \in SS : \wedge mm2.acc = m.acc$
 3795 $\wedge m = 1bRestrict(mm2)$
 3796 $\langle 8 \rangle 1$. PICK $mm2 \in SS : m = 1bRestrict(mm2)$
 3797 BY $\langle 6 \rangle 3$
 3798 $\langle 8 \rangle 2$ QED
 3799 BY $\langle 8 \rangle 1$ DEF $1bRestrict$
 3800 $\langle 7 \rangle 4$. $\wedge mm = mm2$

3801 $\wedge mm2.mbal \in \text{Ballot} \cup \{-1\}$
 3802 $\langle 8 \rangle 1. \wedge mm \in \text{knowsSent}'[ac]$
 3803 $\wedge mm.bal = b$
 3804 $\wedge mm2 \in \text{knowsSent}'[ac]$
 3805 $\wedge mm2.bal = b$
 3806 OBVIOUS
 3807 $\langle 8 \rangle 2. \wedge mm \in bmsgs$
 3808 $\wedge mm2 \in bmsgs$
 3809 $\wedge mm.type = \text{"1b"}$
 3810 $\wedge mm2.type = \text{"1b"}$
 3811 BY $\langle 5 \rangle 1, \langle 8 \rangle 1$ DEF $InvP, Inv, \text{knowsSentInv}, \text{msgsOfType}$
 3812 $\langle 8 \rangle 3. mm.acc = mm2.acc$
 3813 BY $\langle 7 \rangle 2, \langle 7 \rangle 3$
 3814 $\langle 8 \rangle 4. mm.acc \in \text{Acceptor}$
 3815 BY $\langle 7 \rangle 1, \langle 7 \rangle 2$
 3816 $\langle 8 \rangle 5. mm2.mbal \in \text{Ballot} \cup \{-1\}$
 3817 BY $\langle 8 \rangle 2, BMessageLemma$ DEF $Inv, TypeOK, 1bMessage$
 3818 $\langle 8 \rangle 6.$ QED
 3819 BY $\langle 8 \rangle 1, \langle 8 \rangle 2, \langle 8 \rangle 3, \langle 8 \rangle 4, \langle 8 \rangle 5$ DEF $Inv, 1bInv2$
 3820 $\langle 7 \rangle 5. \wedge m.mbal \leq c$
 3821 $\wedge (m.mbal = c) \Rightarrow (m.mval = v)$
 3822 $\wedge m.mbal \in \text{Ballot} \cup \{-1\}$
 3823 BY $\langle 7 \rangle 2, \langle 7 \rangle 3, \langle 7 \rangle 4$ DEF $1bRestrict$
 3824 $\langle 7 \rangle 6. m1c.bal \geq m.mbal$
 3825 $\langle 8 \rangle \forall m1c.bal, mmbal \in \text{Ballot} \cup \{-1\} :$
 3826 $mmbal \leq c \wedge m1c.bal \geq c \Rightarrow m1c.bal \geq mmbal$
 3827 BY $SimpleArithmetic$ DEF $Ballot$
 3828 $\langle 8 \rangle$ QED
 3829 BY $\langle 6 \rangle 5, \langle 7 \rangle 5$
 3830 $\langle 7 \rangle 7.$ ASSUME $m1c.bal = m.mbal$
 3831 PROVE $m.mval = v$
 3832 $\langle 8 \rangle \forall m1c.bal, mmbal \in \text{Ballot} \cup \{-1\} :$
 3833 $mmbal \leq c \wedge m1c.bal \geq c \wedge mmbal = m1c.bal \Rightarrow mmbal = c$
 3834 BY $SimpleArithmetic$ DEF $Ballot$
 3835 $\langle 8 \rangle$ QED
 3836 BY $\langle 7 \rangle 5, \langle 6 \rangle 5, \langle 7 \rangle 7$
 3837 $\langle 7 \rangle 8.$ QED
 3838 BY $\langle 7 \rangle 6, \langle 7 \rangle 7$
 3839 $\langle 6 \rangle 7.$ QED
 3840 $\langle 7 \rangle 1. Q(BQ) \in \text{Quorum}$
 3841 BY DEF $Quorum$
 3842 $\langle 7 \rangle 2. P!ShowsSafeAt(Q(BQ), b, v)!1!2!2!(m1c)$
 3843 BY $\langle 6 \rangle 5, \langle 6 \rangle 6$
 3844 $\langle 7 \rangle$ QED
 3845 BY $\langle 7 \rangle 1, \langle 6 \rangle 4, \langle 7 \rangle 2$ DEF $P!ShowsSafeAt$

3846 $\langle 5 \rangle 5$. QED
 3847 BY $\langle 4 \rangle 1, \langle 5 \rangle 3, \langle 5 \rangle 4$ DEF *KnowsSafeAt*
 3848 $\langle 4 \rangle 2$. $\exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, b, v)'$
 3849 $\langle 5 \rangle 1$. PICK $m \in SM : m.val = v$
 3850 OBVIOUS
 3851 $\langle 5 \rangle 2$. $\wedge m \in \text{msgs}'$
 3852 $\wedge m.type = \text{"1c"}$
 3853 $\wedge m.bal = b$
 3854 BY $\langle 3 \rangle 1$ DEF *msgsOfType*
 3855 $\langle 5 \rangle 3$. $m \in 1\text{cmgs}'$
 3856 BY $\langle 5 \rangle 2, \text{MsgsTypeLemmaPrime}$
 3857 $\langle 5 \rangle$ QED
 3858 BY $\langle 5 \rangle 1, \langle 5 \rangle 2, \langle 5 \rangle 3$ DEF *1cmgs*
 3859 $\langle 4 \rangle 3$. QED
 3860 BY $\langle 4 \rangle 1, \langle 4 \rangle 2$
 3861 $\langle 3 \rangle 5$. $PmaxBal' = PmaxBal$
 3862 BY DEF *LearnsSent, PmaxBal, 1bOr2bMsgs*
 3863 $\langle 3 \rangle 6$. QED
 3864 BY $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3, \langle 3 \rangle 4, \langle 3 \rangle 5$
 3865 DEF *LearnsSent, P!Phase1c, P!TLANext, Ballot, P!Ballot*
 3866 $\langle 2 \rangle 7$. ASSUME NEW $self \in \text{Ballot}$,
 3867 $Phase1a(self)$

 3869 PROVE $P!TLANext \vee P!vars' = P!vars$
 3870 $\langle 3 \rangle$ USE *Phase1a(self)*
 3871 $\langle 3 \rangle 1$. $\text{msgs}' = \text{msgs} \cup \{[type \mapsto \text{"1a"}, bal \mapsto self]\}$
 3872 BY *MsgsLemma* DEF *Inv*
 3873 $\langle 3 \rangle 2$. UNCHANGED $\langle PmaxBal, maxVBal, maxVVal \rangle$
 3874 BY DEF *Phase1a, PmaxBal, 1bOr2bMsgs*
 3875 $\langle 3 \rangle 3$. $P!Phase1a(self)$
 3876 BY $\langle 3 \rangle 1, \langle 3 \rangle 2$ DEF $P!Phase1a$
 3877 $\langle 3 \rangle 4$. QED
 3878 BY $\langle 3 \rangle 3$ DEF $P!TLANext, Ballot, P!Ballot$
 3879 $\langle 2 \rangle 8$. ASSUME NEW $self \in \text{Ballot}$,
 3880 $Phase1c(self)$
 3881 PROVE $P!TLANext \vee P!vars' = P!vars$
 3882 $\langle 3 \rangle$ USE *Phase1c(self)*
 3883 $\langle 3 \rangle 1$. PICK $SS \in \text{SUBSET } [type : \{\text{"1c"}\}, bal : \{self\},$
 3884 $val : \text{Value}] :$
 3885 $\wedge \forall m \in SS :$
 3886 $\exists a \in \text{Acceptor} : \text{KnowsSafeAt}(a, m.bal, m.val)$
 3887 $\wedge \text{msgs}' = \text{msgs} \cup SS$
 3888 BY *MsgsLemma* DEF *Inv*
 3889 $\langle 3 \rangle$ DEFINE $S \triangleq \{m.val : m \in SS\}$
 3890 $\langle 3 \rangle 2$. $SS = \{[type \mapsto \text{"1c"}, bal \mapsto self,$

3891 $val \mapsto v] : v \in S\}$
 3892 $\langle 4 \rangle 1.$ ASSUME NEW $m \in SS$
 3893 PROVE $m \in \{[type \mapsto "1c", bal \mapsto self,$
 3894 $val \mapsto v] : v \in S\}$
 3895 $\langle 5 \rangle 1.$ $m = [type \mapsto "1c", bal \mapsto self, val \mapsto m.val]$
 3896 $\langle 6 \rangle 1.$ $\exists a \in \{ "1c" \}, b \in \{ self \}, v \in Value :$
 3897 $m = [type \mapsto a, bal \mapsto b, val \mapsto v]$
 3898 OBVIOUS
 3899 $\langle 6 \rangle 2.$ PICK $v \in Value :$
 3900 $m = [type \mapsto "1c", bal \mapsto self, val \mapsto v]$
 3901 BY $\langle 6 \rangle 1$
 3902 $\langle 6 \rangle 3.$ $[type \mapsto "1c", bal \mapsto self, val \mapsto v].val = v$
 3903 OBVIOUS
 3904 $\langle 6 \rangle 4.$ QED
 3905 BY $\langle 6 \rangle 2, \langle 6 \rangle 3$
 3906 $\langle 5 \rangle 2.$ $m.val \in S$
 3907 BY DEF S
 3908 $\langle 5 \rangle 3.$ QED
 3909 BY $\langle 5 \rangle 1, \langle 5 \rangle 2$
 3910 $\langle 4 \rangle 2.$ ASSUME NEW $m \in \{[type \mapsto "1c", bal \mapsto self,$
 3911 $val \mapsto v] : v \in S\}$
 3912 PROVE $m \in SS$
 3913 $\langle 5 \rangle 1.$ PICK $v \in S :$
 3914 $m = [type \mapsto "1c", bal \mapsto self, val \mapsto v]$
 3915 OBVIOUS
 3916 $\langle 5 \rangle 2.$ PICK $mm \in SS : mm.val = v$
 3917 OBVIOUS
 3918 $\langle 5 \rangle 3.$ $mm \in [type : \{ "1c" \}, bal : \{ self \}, val : Value]$
 3919 OBVIOUS
 3920 $\langle 5 \rangle 4.$ $mm = [type \mapsto "1c", bal \mapsto self, val \mapsto v]$
 3921 BY $\langle 5 \rangle 2, \langle 5 \rangle 3$
 3922 $\langle 5 \rangle 5.$ QED
 3923 BY $\langle 5 \rangle 1, \langle 5 \rangle 4$
 3924 $\langle 4 \rangle 3.$ QED
 3925 BY $\langle 4 \rangle 1, \langle 4 \rangle 2$
 3926 $\langle 3 \rangle 3.$ ASSUME NEW $v \in S$
 3927 PROVE $\exists Q \in Quorum : P!ShowsSafeAt(Q, self, v)$
 3928 $\langle 4 \rangle$ DEFINE $m \triangleq [type \mapsto "1c", bal \mapsto self, val \mapsto v]$
 3929 $\langle 4 \rangle 1.$ $m \in SS$
 3930 BY $\langle 3 \rangle 2$
 3931 $\langle 4 \rangle 2.$ PICK $a \in Acceptor : KnowsSafeAt(a, self, v)$
 3932 BY $\langle 4 \rangle 1, \langle 3 \rangle 1$
 3933 $\langle 4 \rangle$ DEFINE $SK \triangleq \{mm \in knowsSent[a] : mm.bal = self\}$
 3934 $\langle 4 \rangle 3.$ ASSUME NEW $BQ \in ByzQuorum,$
 3935 $\forall ac \in BQ : \exists mm \in SK : mm.acc = ac$

3936 PROVE $P!ShowsSafeAt(BQ \cap Acceptor, self, v)!1!1$
 3937 $\langle 5 \rangle$ DEFINE $Q \triangleq BQ \cap Acceptor$
 3938 $Q1b \triangleq \{mm \in P!sentMsgs("1b", self) : mm.acc \in Q\}$
 3939 $\langle 5 \rangle$ SUFFICES ASSUME NEW $ac \in BQ \cap Acceptor$
 3940 PROVE $\exists mm \in Q1b : mm.acc = ac$
 3941 OBVIOUS
 3942 $\langle 5 \rangle 1.$ $\forall mm \in acceptorMsgsOfType("1b") :$
 3943 $(mm.bal = self) \Rightarrow$
 3944 $(1bRestrict(mm) \in P!sentMsgs("1b", self))$
 3945 $\langle 6 \rangle$ SUFFICES ASSUME NEW $mm \in acceptorMsgsOfType("1b"),$
 3946 $mm.bal = self$
 3947 PROVE $1bRestrict(mm) \in P!sentMsgs("1b", self)$
 3948 OBVIOUS
 3949 $\langle 6 \rangle 1.$ $\wedge 1bRestrict(mm).type = "1b"$
 3950 $\wedge 1bRestrict(mm).bal = self$
 3951 BY DEF $1bRestrict, acceptorMsgsOfType, msgsOfType$
 3952 $\langle 6 \rangle 2.$ $1bRestrict(mm) \in msgs$
 3953 BY DEF $1bmsgs, msgs$
 3954 $\langle 6 \rangle 3.$ QED
 3955 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$ DEF $P!sentMsgs$
 3956 $\langle 5 \rangle 2.$ PICK $mm \in SK : mm.acc = ac$
 3957 BY $\langle 4 \rangle 3$
 3958 $\langle 5 \rangle 3.$ $mm \in msgsOfType("1b") \wedge mm.bal = self$
 3959 BY DEF $Inv, knowsSentInv$
 3960 $\langle 5 \rangle 4.$ $1bRestrict(mm) \in P!sentMsgs("1b", self)$
 3961 BY $\langle 5 \rangle 1, \langle 5 \rangle 2, \langle 5 \rangle 3$ DEF $acceptorMsgsOfType$
 3962 $\langle 5 \rangle 5.$ $1bRestrict(mm).acc = ac$
 3963 BY $\langle 5 \rangle 2$ DEF $1bRestrict$
 3964 $\langle 5 \rangle 6.$ QED
 3965 BY $\langle 5 \rangle 4, \langle 5 \rangle 5$
 3966 $\langle 4 \rangle 4.$ CASE $KnowsSafeAt(a, self, v)!1!1$
 3967 $\langle 5 \rangle 1.$ PICK $BQ \in ByzQuorum :$
 3968 $\forall ac \in BQ : \exists mm \in SK : \wedge mm.acc = ac$
 3969 $\wedge mm.mbal = -1$
 3970 BY $\langle 4 \rangle 4$
 3971 $\langle 5 \rangle$ DEFINE $Q \triangleq BQ \cap Acceptor$
 3972 $Q1b \triangleq \{mm \in P!sentMsgs("1b", self) : mm.acc \in Q\}$
 3973 $\langle 5 \rangle 2.$ $P!ShowsSafeAt(Q, self, v)!1!1$
 3974 $\langle 6 \rangle 1.$ $\forall ac \in BQ : \exists mm \in SK : mm.acc = ac$
 3975 BY $\langle 5 \rangle 1$
 3976 $\langle 6 \rangle 2.$ QED
 3977 BY $\langle 6 \rangle 1, \langle 4 \rangle 3$
 3978 $\langle 5 \rangle 3.$ ASSUME NEW $mm \in Q1b$
 3979 PROVE $mm.mbal = -1$
 3980 $\langle 6 \rangle 1.$ $\wedge mm \in 1bmsgs$

3981 $\wedge mm.bal = self$
 3982 $\wedge mm.acc \in Q$
 3983 BY *MsgsTypeLemma* DEF $P!sentMsgs$
 3984 $\langle 6 \rangle 2$. PICK $mb \in bmsgs : \wedge mb.type = \text{"1b"}$
 3985 $\wedge mm = 1bRestrict(mb)$
 3986 BY $\langle 6 \rangle 1$ DEF $1bmsgs, acceptorMsgsOfType, msgsOfType$
 3987 $\langle 6 \rangle 3$. $\wedge mb.bal = self$
 3988 $\wedge mb.acc \in Q$
 3989 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$ DEF $1bRestrict$
 3990 $\langle 6 \rangle 4$. PICK $mk \in SK : (mk.acc = mb.acc) \wedge (mk.mbal = -1)$
 3991 BY $\langle 6 \rangle 3, \langle 5 \rangle 1$
 3992 $\langle 6 \rangle 5$. $(mk \in bmsgs) \wedge (mk.bal = self) \wedge (mk.type = \text{"1b"})$
 3993 BY DEF $Inv, knowsSentInv, msgsOfType$
 3994 $\langle 6 \rangle 6$. $mk = mb$
 3995 BY $\langle 6 \rangle 2, \langle 6 \rangle 3, \langle 6 \rangle 4, \langle 6 \rangle 5$ DEF $Inv, 1bInv2$
 3996 $\langle 6 \rangle 7$. QED
 3997 BY $\langle 6 \rangle 6, \langle 6 \rangle 4, \langle 6 \rangle 2$ DEF $1bRestrict$
 3998 $\langle 5 \rangle 4$. QED
 3999 $\langle 6 \rangle$ USE DEF *Quorum*
 4000 $\langle 6 \rangle$ WITNESS $Q \in Quorum$
 4001 $\langle 6 \rangle$ QED
 4002 BY $\langle 5 \rangle 2, \langle 5 \rangle 3$ DEF $P!ShowsSafeAt, Quorum$
 4003 $\langle 4 \rangle 5$. CASE $KnowsSafeAt(a, self, v)!1!2$
 4004 $\langle 5 \rangle 1$. PICK $c \in 0 \dots (self - 1) : KnowsSafeAt(a, self, v)!1!2!(c)$
 4005 BY $\langle 4 \rangle 5$
 4006 $\langle 5 \rangle 2$. PICK $BQ \in ByzQuorum : KnowsSafeAt(a, self, v)!1!2!(c)!1!(BQ)$
 4007 BY $\langle 5 \rangle 1$
 4008 $\langle 5 \rangle$ DEFINE $Q \triangleq BQ \cap Acceptor$
 4009 $Q1b \triangleq \{mm \in P!sentMsgs(\text{"1b"}, self) : mm.acc \in Q\}$
 4010 $\langle 5 \rangle 3$. $P!ShowsSafeAt(Q, self, v)!1!1$
 4011 $\langle 6 \rangle 1$. $\forall ac \in BQ : \exists mm \in SK : mm.acc = ac$
 4012 BY $\langle 5 \rangle 2$
 4013 $\langle 6 \rangle 2$. QED
 4014 BY $\langle 6 \rangle 1, \langle 4 \rangle 3$
 4015 $\langle 5 \rangle 4$. PICK $WQ \in WeakQuorum : KnowsSafeAt(a, self, v)!1!2!(c)!2!(WQ)$
 4016 BY $\langle 5 \rangle 1$
 4017 $\langle 5 \rangle 5$. PICK $ac \in WQ \cap Acceptor :$
 4018 $KnowsSafeAt(a, self, v)!1!2!(c)!2!(WQ)!(ac)$
 4019 $\langle 6 \rangle 1$. $\exists ac \in WQ \cap Acceptor : \text{TRUE}$
 4020 BY BQA
 4021 $\langle 6 \rangle 2$. QED
 4022 BY $\langle 6 \rangle 1, \langle 5 \rangle 4$
 4023 $\langle 5 \rangle 6$. PICK $mk \in SK : \wedge mk.acc = ac$
 4024 $\wedge \exists r \in mk.m2av : \wedge r.bal \geq c$
 4025 $\wedge r.val = v$

4026 BY $\langle 5 \rangle 5$
 4027 $\langle 5 \rangle 7$. PICK $r \in mk.m2av : \wedge r.bal \geq c$
 4028 $\wedge r.val = v$
 4029 BY $\langle 5 \rangle 6$
 4030 $\langle 5 \rangle 8$. $(mk \in bmsgs) \wedge (mk.type = \text{"1b"}) \wedge (mk.bal = self)$
 4031 BY DEF $Inv, knowsSentInv, msgsOfType$
 4032 $\langle 5 \rangle$ DEFINE $mc \triangleq [type \mapsto \text{"1c"}, bal \mapsto r.bal, val \mapsto v]$
 4033 $\langle 5 \rangle 9$. $mc \in msgs$
 4034 $\langle 6 \rangle 1$. $[type \mapsto \text{"1c"}, bal \mapsto r.bal, val \mapsto r.val] \in msgs$
 4035 BY $\langle 5 \rangle 6, \langle 5 \rangle 8$ DEF $Inv, 1bInv1$
 4036 $\langle 6 \rangle 2$. QED
 4037 BY $\langle 6 \rangle 1, \langle 5 \rangle 7$
 4038 $\langle 5 \rangle 10$. ASSUME NEW $mq \in Q1b$
 4039 PROVE $\wedge mc.bal \geq mq.mbal$
 4040 $\wedge (mc.bal = mq.mbal) \Rightarrow (mq.mval = v)$
 4041 $\langle 6 \rangle 1$. $\wedge mq \in msgs$
 4042 $\wedge mq.type = \text{"1b"}$
 4043 $\wedge mq.bal = self$
 4044 $\wedge mq.acc \in Q$
 4045 BY DEF $P!sentMsgs$
 4046 $\langle 6 \rangle 2$. PICK $mbq \in acceptorMsgsOfType(\text{"1b"}) :$
 4047 $mq = 1bRestrict(mbq)$
 4048 BY $\langle 6 \rangle 1, MsgsTypeLemma$ DEF $1bmsgs$
 4049 $\langle 6 \rangle 3$. $\wedge mbq \in bmsgs$
 4050 $\wedge mbq.type = \text{"1b"}$
 4051 $\wedge mbq.bal = self$
 4052 $\wedge mbq.mbal = mq.mbal$
 4053 $\wedge mbq.mval = mq.mval$
 4054 $\wedge mbq.acc \in Q$
 4055 BY $\langle 6 \rangle 1, \langle 6 \rangle 2$ DEF $acceptorMsgsOfType, msgsOfType, 1bRestrict$
 4056 $\langle 6 \rangle 4$. PICK $ab \in BQ :$
 4057 $\exists mcq \in SK : \wedge mcq.acc = mbq.acc$
 4058 $\wedge mcq.mbal \leq c$
 4059 $\wedge (mcq.mbal = c) \Rightarrow (mcq.mval = v)$
 4060 BY $\langle 5 \rangle 2, \langle 6 \rangle 3$
 4061 $\langle 6 \rangle 5$. PICK $mcq : \wedge mcq \in knowsSent[a]$
 4062 $\wedge mcq.bal = self$
 4063 $\wedge mcq.acc = mbq.acc$
 4064 $\wedge mcq.mbal \leq c$
 4065 $\wedge (mcq.mbal = c) \Rightarrow (mcq.mval = v)$
 4066 BY $\langle 6 \rangle 4$
 4067 $\langle 6 \rangle 6$. $(mcq \in bmsgs) \wedge (mcq.type = \text{"1b"})$
 4068 BY $\langle 6 \rangle 5$ DEF $Inv, knowsSentInv, msgsOfType$
 4069 $\langle 6 \rangle 7$. $mcq = mbq$
 4070 BY $\langle 6 \rangle 3, \langle 6 \rangle 5, \langle 6 \rangle 6$ DEF $Inv, 1bInv2$

4071 $\langle 6 \rangle 8. \wedge mc.bal \geq mcq.mbal$
 4072 $\wedge (mc.bal = mcq.mbal) \Rightarrow (mcq.mval = v)$
 4073 $\langle 7 \rangle 1. mc.bal \in Ballot \cup \{-1\} \wedge mc.bal \geq c$
 4074 $\langle 8 \rangle 1. mc.bal = r.bal$
 4075 OBVIOUS
 4076 $\langle 8 \rangle 2. mk \in bmsgs \wedge mk.type = \text{"1b"}$
 4077 BY DEF *Inv*, *knowsSentInv*, *msgsOfType*
 4078 $\langle 8 \rangle 3. r.bal \in Ballot$
 4079 $\langle 9 \rangle 1. mk \in 1bMessage$
 4080 BY $\langle 8 \rangle 2$, *BMessageLemma* DEF *Inv*, *TypeOK*, *1bMessage*
 4081 $\langle 9 \rangle 2. QED$
 4082 BY $\langle 9 \rangle 1$ DEF *1bMessage*
 4083 $\langle 8 \rangle 4. QED$
 4084 BY $\langle 8 \rangle 1$, $\langle 8 \rangle 3$, $\langle 5 \rangle 7$
 4085 $\langle 7 \rangle 2. mcq.mbal \in Ballot \cup \{-1\}$
 4086 $\langle 8 \rangle mcq \in bmsgs \wedge mcq.type = \text{"1b"}$
 4087 BY $\langle 6 \rangle 5$ DEF *Inv*, *knowsSentInv*, *msgsOfType*
 4088 $\langle 8 \rangle QED$
 4089 BY *BMessageLemma* DEF *Inv*, *TypeOK*, *1bMessage*
 4090 $\langle 7 \rangle 3. \forall mcbal, mcqmbal \in Ballot \cup \{-1\} :$
 4091 $\wedge mcbal \geq c$
 4092 $\wedge mcqmbal \leq c$
 4093 $\Rightarrow \wedge mcbal \geq mcqmbal$
 4094 $\wedge (mcbal = mcqmbal) \Rightarrow (mcqmbal = c)$
 4095 BY *SimpleArithmetic* DEF *Ballot*
 4096 $\langle 7 \rangle 4. \wedge mc.bal \geq mcq.mbal$
 4097 $\wedge (mc.bal = mcq.mbal) \Rightarrow (mcq.mbal = c)$
 4098 BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, $\langle 7 \rangle 3$, $\langle 6 \rangle 5$
 4099 $\langle 7 \rangle 5. QED$
 4100 BY $\langle 7 \rangle 4$, $\langle 6 \rangle 5$
 4101 $\langle 6 \rangle 9. QED$
 4102 BY $\langle 6 \rangle 3$, $\langle 6 \rangle 7$, $\langle 6 \rangle 8$
 4103 $\langle 5 \rangle 11. QED$
 4104 $\langle 6 \rangle Q \in Quorum$
 4105 BY DEF *Quorum*
 4106 $\langle 6 \rangle WITNESS Q \in Quorum$
 4107 $\langle 6 \rangle QED$
 4108 BY $\langle 5 \rangle 3$, $\langle 5 \rangle 9$, $\langle 5 \rangle 10$ DEF *P!ShowsSafeAt*
 4109 $\langle 4 \rangle 6. QED$
 4110 BY $\langle 4 \rangle 2$, $\langle 4 \rangle 4$, $\langle 4 \rangle 5$ DEF *KnowsSafeAt*
 4111 $\langle 3 \rangle 4. P!Phase1c(self, S)$
 4112 BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$ DEF *P!Phase1c*, *Phase1c*, *PmaxBal*, *1bOr2bMsgs*
 4113 $\langle 3 \rangle 5. QED$
 4114 BY $\langle 3 \rangle 4$ DEF *P!TLANext*, *Ballot*, *P!Ballot*
 4115 $\langle 2 \rangle 9. ASSUME NEW self \in FakeAcceptor,$

```

4116      FakingAcceptor(self)
4117      PROVE  $P!TLANext \vee P!vars' = P!vars$ 
4118       $\langle 3 \rangle$  USE FakingAcceptor(self)
4119       $\langle 3 \rangle 1.$   $msgs' = msgs$ 
4120      BY MsgsLemma DEF Inv
4121       $\langle 3 \rangle 2.$   $PmaxBal' = PmaxBal$ 
4122       $\langle 4 \rangle 1.$  PICK  $mm : \wedge bmsgs' = bmsgs \cup \{mm\}$ 
4123       $\wedge mm.acc = self$ 
4124      BY DEF FakingAcceptor
4125       $\langle 4 \rangle$  DEFINE  $S(b, a) \triangleq \{ma \in b : \wedge ma.type \in \{"1b", "2b"\}$ 
4126       $\wedge ma.acc = a\}$ 
4127       $\langle 4 \rangle 2.$  ASSUME NEW  $a \in Acceptor$ 
4128      PROVE  $S(bmsgs, a) = S(bmsgs', a)$ 
4129       $\langle 5 \rangle 1.$   $\forall m : (m.acc = a) \Rightarrow (m \in bmsgs' \equiv m \in bmsgs)$ 
4130      BY  $\langle 4 \rangle 1, BQA$ 
4131       $\langle 5 \rangle 2.$  QED
4132      BY  $\langle 5 \rangle 1$ 
4133       $\langle 4 \rangle$  QED
4134      BY  $\langle 4 \rangle 2$  DEF PmaxBal, 1bOr2bMsgs
4135       $\langle 3 \rangle 3.$   $P!vars' = P!vars$ 
4136      BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$  DEF P!vars, FakingAcceptor
4137       $\langle 3 \rangle 4.$  QED
4138      BY  $\langle 3 \rangle 3$ 
4139       $\langle 2 \rangle 10.$  QED
4140      BY  $\langle 2 \rangle 3, \langle 2 \rangle 4, \langle 2 \rangle 5, \langle 2 \rangle 6, \langle 2 \rangle 7, \langle 2 \rangle 8, \langle 2 \rangle 9, NextDef$ 

4142  $\langle 1 \rangle 3.$  QED
4143 PROOF OMITTED

```

```

4145 |
    To see how learning is implemented, we must describe how to determine that a value has been
    chosen. This is done by the following definition of chosen to be the set of chosen values.
4151 chosen  $\triangleq \{v \in Value : \exists BQ \in ByzQuorum, b \in Ballot :$ 
4152       $\forall a \in BQ : \exists m \in msgs : \wedge m.type = "2b"$ 
4153       $\wedge m.acc = a$ 
4154       $\wedge m.bal = b$ 
4155       $\wedge m.val = v\}$ 

```

The correctness of our definition of *chosen* is expressed by the following theorem, which asserts that if a value is in *chosen*, then it is also in the set *chosen* of the emulated execution of the *PaxosConsensus* algorithm.

The state function *chosen* does not necessarily equal the corresponding state function of the *PaxosConsensus* algorithm. It requires every (real or fake) acceptor in a *ByzQuorum* to vote for (send 2b messages) for a value *v* in the same ballot for *v* to be in *chosen* for the *BPCon* algorithm, but it requires only that every (real) acceptor in a *Quorum* vote for *v* in the same ballot for *v* to be in the set *chosen* of the emulated execution of *PaxosConsensus*.

Liveness for *BPCon* requires that, under suitable assumptions, some value is eventually in *chosen*. Since we can't assume that a fake acceptor does anything useful, liveness requires the assumption that there is a *ByzQuorum* composed entirely of real acceptors (the second conjunct of assumption *BQLA*).

```

4176 THEOREM  $chosen \subseteq P!chosen$ 
4177   Note: I had to define ch and Pch instead of using subexpression
4178   names because of a bug in tlapm that has since been fixed.
4179   <1> DEFINE  $ch(v) \triangleq \exists BQ \in ByzQuorum, b \in Ballot :$ 
4180            $\forall a \in BQ : \exists m \in msgs : \wedge m.type = "2b"$ 
4181            $\wedge m.acc = a$ 
4182            $\wedge m.bal = b$ 
4183            $\wedge m.val = v$ 
4184    $Pch(v) \triangleq \exists Q \in Quorum, b \in P!Ballot :$ 
4185            $\forall a \in Q : \exists m \in msgs : \wedge m.type = "2b"$ 
4186            $\wedge m.acc = a$ 
4187            $\wedge m.bal = b$ 
4188            $\wedge m.val = v$ 
4189   <1> SUFFICES ASSUME NEW  $v \in Value, ch(v)$ 
4190           PROVE  $Pch(v)$ 
4191   BY DEF  $chosen, P!chosen$ 

4193   <1>1. PICK  $BQ \in ByzQuorum, b \in Ballot : ch(v)!(BQ, b)$ 
4194   OBVIOUS
4195   <1> DEFINE  $Q \triangleq BQ \cap Acceptor$ 
4196   <1>2.  $Q \in Quorum$ 
4197   BY DEF  $Quorum$ 
4198   <1> WITNESS  $Q \in Quorum$ 
4199   <1> USE DEF  $P!Ballot, Ballot$ 
4200   <1> WITNESS  $b \in P!Ballot$ 
4201   <1>3. QED
4202   BY <1>1

4204 |
  \ * Modification History
  \ * Last modified Sat Nov 16 22:20:34 CST 2019 by hengxin
  \ * Last modified Tue Feb 08 11:53:20 PST 2011 by lamport

```