# An Assertional Proof of a Byzantine Agreement Protocol

Jiahua Qian*

TR 83-566

August 1983

Department of Computer Science
Cornell University
Ithaca, New York 14853

*On leave from
Department of Computer Science,
Fudan University, People's Republic of China

# An Assertional Proof of a Byzantine Agreement Protocol

Jiahua Qian[+]

Department of Computer Science
Cornell University
Ithaca, New York 14853

August 1, 1983

ABSTRACT

An assertional proof of a Byzantine Agreement protocol is given. This provides a formal argument for the correctness of the protocol.

[+]On leave from Department of Computer Science, Fudan University, People's Republic of China.

## 1. Introduction

One of the fundamental problems in the design of fault-tolerant distributed programs is to ensure that a collection of processes can reach agreement, despite the fact that some processes may be faulty. The problem can be described abstractly, as follows:

> Given is a collection of N processes, where one -- the transmitter -- desires the others to agree on its value. Processors may fail and upon failing may behave in an arbitrary manner. Desired is a protocol that establishes:
>
> BYZ1: All functioning processors agree on the same value.
>
> BYZ2: If the transmitter is non-faulty then all functioning processors agree on the transmitters value.

A number of protocols have appeared in the literature to solve this problem [DS82]. In this paper, we prove that the Byzantine Agreement Protocol of [LFF82] is correct using assertional reasoning.

We proceed as follows. In section 2 we define the protocol, modelling failures as malevolent processes. Section 3 contains a correctness proof.

## 2. Byzantine Agreement Program

The program for modelling Byzantine Agreement appears below. There, T is the set of reliable processes, F is the set of faulty processes, and GEN is the transmitter. Assertions in the text of the program are defined in the next section. However, we are given that $|T| \geq 2|F|+1$.

Execution of the agreement protocol involves a number of rounds. In the first round, if GEN is non-faulty, it sends either '*' or $\emptyset$ to all other processes. In subsequent rounds, processes exchange the values they have received in previous rounds until they agree on the value sent by GEN. If GEN is faulty then it may not send the same value to the other processes. We model this by a loop INIT in Figure 1; subsequent execution of processes is modelled by the loop labelled BYZ. Note that two types of processors execute. Those that are faulty are modelled by program FAULTY, which can do anything; those that are non-faulty are modelled by program NORMAL, which correctly executes the agreement protocol as defined in Figure 2. GEN can be a member of either F or T.

The behavior of the communications network is modelled by variable BROAD, defined as follows:

$\mathrm{BROAD}_i^r[j] \equiv$ "The set of messages broadcast by processor i to processor j during round r."

According to the protocol, non-faulty processors will broadcast the same message to all processes at each round. Thus, we have

$$(\forall j,k\colon j,k \in T \cup F\colon i \in T \Rightarrow \mathrm{BROAD}_i^r[j]=\mathrm{BROAD}_i^r[k])$$

By abuse of notation, $\mathrm{BROAD}_i^r$ will represent the message broadcast by processor i, when all messages i broadcast in that round were the same.

In the agreement protocol (see Figure 2), the message broadcast by a process i may be * or some process name j. A message with value * is broadcast by i if i supports the fact that the value sent by GEN during round 1 is *; a message with value j is broadcast if process i knows that j supports the fact that the value sent by GEN at the first round is *.

The meanings of the other variables in the program are as follows. Variable $\mathrm{RECEIVE}_i^r[j]$ contains the set of messages received by process i from process j by round r-1. Variable $\mathrm{COMMIT}_i^r$ has value 0 at the first round; its value becomes 1 (and remains 1) as soon as process i agrees that the value sent by GEN at first round is *.

```
r:= 1;  i:= 0;
INIT:  do i≠n → i:= i+1;
                 RECEIVE_i^r[ 1...n ] := ∅;
                 COMMIT_i^r:= 0;
                 if (i=GEN ∧ GEN ∈ T) → if true → BROAD_i^r := {*}
                                         [] true → BROAD_i^r := ∅
                                        fi
                  [] (i=GEN ∧ GEN ∈ F) → j:= 0;   do j≠n → j:= j+1;
                                                   if true → BROAD_i^r[j]:= {*}
                                                    [] true → BROAD_i^r[j]:= ∅
                                                   fi
                                         od
                  [] i≠GEN → BROAD_i^r[ 1...n ]:= ∅
                 fi
       od;
{(∀i: i ∈ P: RECEIVE_i^1=∅ ∧ COMMIT_i^1=0 ∧ (i≠GEN ⇒ BROAD_i^1[ 1...n ]=∅) ∧
          (i=GEN ⇒ (∀j: j ∈ P: j ∉ BROAD_i^1[ 1...n ])))}
{I}
BYZ:  do r≠R → {r<2t+4  ∧  I}
               r:= r+1;
               {I_{r-1}^r  ∧  r≥2}
               cobegin

                    //    NORMAL_i
                  i ∈ T

                    //    FAULTY_i
                  i ∈ F

               coend
      od
{r=R  ∧  I}
```

Figure 1 -- Byzantine Agreement Program

Finally, we define

$0 \leq |F| \leq t$

$P \equiv T \cup F$

$LOW \equiv t+1$

$HIGH \equiv 2t+1$

$R \equiv 2t+4$

## 3. Correctness of the Program

We now argue the correctness of the programs given above. In Figure 1,

$$I \equiv I_0 \;\wedge\; (\forall i,s\colon i \in T \wedge s \leq r\colon I_1 \wedge I_2 \wedge I_3 \wedge I_4 \wedge I_5)$$

and

$$I_0 \equiv (\forall i\colon i \in P\colon ((i \neq GEN \Rightarrow BROAD_i^1[\,1\ldots n\,]=\emptyset) \;\wedge$$
$$(i=GEN \Rightarrow (\forall j\colon j \in P\colon j \notin BROAD_i^1[\,1\ldots n\,]))))$$

$$I_1 \equiv (\forall j,s\colon j \in T \wedge s \geq 2\colon RECEIVE_i^s[j] = \bigcup_{s'=1}^{s-1} BROAD_j^{s'})$$

$$I_2 \equiv (\forall j,k\colon j,k \in P\colon BROAD_i^s[j] = BROAD_i^s[k] = BROAD_i^s)$$

$$\begin{aligned}I_3 \equiv\; & (BROAD_{GEN}^1[i]=\{*\} \;\Rightarrow\; * \in BROAD_i^2) \wedge (BROAD_{GEN}^1[i]=\emptyset \;\Rightarrow\; BROAD_i^2=\emptyset) \;\wedge \\ & ((s>2 \wedge * \in BROAD_i^s) \;\Rightarrow\; (* \notin RECEIVE_i^s[i] \;\wedge \\ & \;(\blacksquare j\colon (\blacksquare k\colon j \in RECEIVE_i^s[k]) \geq HIGH \wedge j \neq GEN) \geq (LOW+\lceil \tfrac{s}{2} \rceil -2))) \;\wedge \\ & ((s>2 \wedge (\blacksquare j\colon (\blacksquare k\colon j \in RECEIVE_i^s[k]) \geq HIGH \wedge j \neq GEN) \geq (LOW+\lceil \tfrac{s}{2} \rceil - 2)) \;\Rightarrow \\ & \;(\exists\, s'\colon s' \leq s\colon * \in BROAD_i^{s'}))\end{aligned}$$

```
j:= 0;
do j≠n → j := j+1;
        if BROAD_j^{r-1}[i]≠∅ → RECEIVE_i^r[j]:= RECEIVE_i^{r-1}[j] ∪ BROAD_j^{r-1}[i]
         [] BROAD_j^{r-1}[i]=∅ → skip
        fi
od;
OK_i:= true;
wait OK_1 ∧ OK_2 ∧ ... ∧ OK_n;
BROAD_i^r:= ∅;   OK_i:= false;
if r=2 → if RECEIVE_i^r[GEN]={*} ∧ i≠GEN → BROAD_i^r:= BROAD_i^r ∪ {*}
          [] RECEIVE_i^r[GEN]=∅ ∨ i=GEN → skip
         fi
 [] r>2 → if (* ∉ RECEIVE_i^r[i] ∧
              (■j: j≠GEN ∧ (■k:j ∈ RECEIVE_i^r[k])≥HIGH)≥LOW+⌈r/2⌉-2
                   → BROAD_i^r:= BROAD_i^r∪{*}
          [] otherwise → skip
         fi
fi ;
j:= 0;
do j≠n → j:= j+1;
        if ((j ∉ RECEIVE_i^r[i]) ∧
            (* ∈ RECEIVE_i^r[j] ∨ (■k: j ∈ RECEIVE_i^r[k])≥LOW))
                → BROAD_i^r:= BROAD_i^r ∪ {j}
         [] otherwise → skip
        fi
od;
COMMIT_i^r:= COMMIT_i^{r-1}
if (COMMIT_i^r=0 ∧ (■j: (■k: j ∈ RECEIVE_i^r[k])≥HIGH) ≥ HIGH) → COMMIT_i^r:= 1
 [] otherwise → skip
fi
```

Figure 2 -- $\mathrm{NORMAL}_i$

$$I_4 \equiv (\forall j, s:\ j \in T \wedge s \ge 2:\ \star \in BROAD_j^{s-1} \Leftrightarrow j \in BROAD_i^{s} \wedge$$
$$(\forall j:\ j \in P:\ ((\blacksquare k:\ j \in RECEIVE_i^{s}[k]) \ge LOW) \Rightarrow$$
$$(\exists\, s':\ s' \le s:\ j \in BROAD_i^{s'})))$$

$$I_5 \equiv (\blacksquare j:\ (\blacksquare k:\ j \in RECEIVE_i^{s}[k]) \ge HIGH) \ge HIGH \Leftrightarrow COMMIT_i^{s} = 1$$

It is easy to see that I is true at the start of the loop labelled BYZ. It therefore suffices to establish that if I is true at the beginning of an iteration, it will be true at the end of an iteration. To do this, we consider the proof outline for $NORMAL_i$ in Figure 3 below.

It is obvious that this proof outline is valid except for $I'_4$. The proof of this is as follows. First we establish:

**Assertion:** $(\forall i, j:\ i, j \in T \wedge r \ge 2:\ j \in BROAD_i^{r} \Rightarrow \star \in BROAD_j^{r-1})$

This is proved as follows:

| | |
|---|---|
| Suppose: | $r=2 \ \wedge\ i, j \in T \ \wedge\ j \in BROAD_i^{r}$ |
| $(L_4)$ | $\Rightarrow \star \in RECEIVE_i^{2}[j] \vee (\blacksquare k:\ j \in RECEIVE_i^{2}[k]) \ge LOW$ |
| $(I'_1, I_0)$ | $\Rightarrow \star \in RECEIVE_i^{2}[j]$ |
| $(I'_1)$ | $\Rightarrow \star \in BROAD_j^{1}$ |

| | |
|---|---|
| Suppose: | $r>2 \ \wedge\ i, j \in T \ \wedge\ j \in BROAD_i^{r}$ |
| $(L_4)$ | $\Rightarrow (j \notin RECEIVE_i^{r}[i]) \wedge$ $(\star \in RECEIVE_i^{r}[j] \vee (\blacksquare k:\ j \in RECEIVE_i^{r}[k]) \ge LOW)$ |
| $(I'_1)$ | $\Rightarrow j \notin RECEIVE_i^{r}[i] \wedge (\star \in BROAD_j^{r-1} \vee (\exists s:\ s \le r-1:\ \star \in BROAD_j^{s-1}) \vee$ $(\blacksquare k:\ j \in RECEIVE_i^{r}[k]) \ge LOW))$ |

Since $j \in T \ \wedge\ (\exists s:\ s \le r-1:\ \star \in BROAD_j^{s-1})$

$(I_4)_{s \le r-1}$ $\Rightarrow (\forall i:\ i \in T:\ (\exists s:\ s \le r-1:\ j \in BROAD_i^{s})$

```
{I^r_{r-1}}
j:= 0;
do j≠n → j:= j+1;
        if BROAD^{r-1}_j[i]≠∅ → RECEIVE^r_i[j]:= RECEIVE^{r-1}_i[j] ∪ BROAD^{r-1}_j[i]
         [] BROAD^{r-1}_j[i]=∅ → skip
        fi
        {(∀k: 1≤k≤j ∧ k ∈ T: RECEIVE^r_i[k]= ∪_{s=1}^{r-1} BROAD^s_j}
od;
{I'_1:  (∀j ∈ T: RECEIVE^r_i[j]= ∪_{s=1}^{r-1} BROAD^s_j}
OK_i:= true;
wait OK_1 ∧ OK_2 ∧ ... ∧ OK_n;
BROAD^r_i:= ∅;
OK_i:= false;
{BROAD^r_i=∅  ∧
I'_2:  (∀j,k: j,k ∈ P: BROAD^r_i[j]=BROAD^r_i[k]=BROAD^r_i}
if r=2 → if i≠GEN ∧ RECEIVE^r_i[GEN]={*} → BROAD^r_i:= BROAD^r_i ∪ {*}
          [] i=GEN ∨ RECEIVE^r_i[GEN]=∅ → skip
         fi
 [] r>2 → if (* ∉ RECEIVE^r_i[i] ∧
             (■j: (■k: j ∈ RECEIVE^r_i[k])≥HIGH ∧ j≠GEN)≥(LOW+⌈r/2⌉-2))
            → BROAD^r_i:= BROAD^r_i ∪ {*}
          [] otherwise → skip
         fi
fi;
{I'_2  ∧  (∀j: j ∈ P: j ∉ BROAD^r_i  ∧
  I'_3:  (BROAD^1_GEN[i]={*} ⇒ * ∈ BROAD^2_i) ∧ (BROAD^1_GEN[i]=∅ ⇒ BROAD^2_i=∅) ∧
         ((r>2 ∧ * ∈ BROAD^r_i) ⇒
          (* ∉ RECEIVE^r_i[i] ∧ (■j: (■k: j ∈ RECEIVE^r_i[k])≥HIGH ∧ j≠GEN)≥(LOW+⌈r/2⌉-2))) ∧
         ((r>2 ∧ (■j: (■k: j ∈ RECEIVE^r_i[k])≥HIGH ∧ j≠GEN)≥(LOW+⌈r/2⌉-2)))  ⇒
          (∃s: s≤r: * ∈ BROAD^s_i)}
j:= 0;
do j≠n → j:= j+1;
```

**if** $((j \notin RECEIVE_i^r[i]) \wedge$

$(* \in RECEIVE_i^r[j] \vee (\blacksquare k\text{: } j \in RECEIVE_i^r[k]) \geq LOW))$

$\rightarrow BROAD_i^r := BROAD_i^r \cup \{j\}$

$\square$ **otherwise** $\rightarrow$ skip

**fi**

**od;**

$\{L_4\text{: } (\forall j\text{: } j \in P\text{: } j \in BROAD_i^r \Rightarrow$

$(j \notin RECEIVE_i^r[i] \wedge (* \in RECEIVE_i^r[j] \vee (\blacksquare k\text{: } j \in RECEIVE_i^r[k]) \geq LOW))) \wedge$

$(* \in RECEIVE_i^r[j] \vee (\blacksquare k\text{: } j \in RECEIVE_i^r[k]) \geq LOW) \Rightarrow$

$(\exists s\text{: } s \leq r\text{: } j \in BROAD_i^s) \wedge I'_2\}$

$\{I'_2 \wedge$

$I'_4\text{: } (\forall j\text{: } j \in T\text{: } (j \in BROAD_i^r \Leftrightarrow * \in BROAD_j^{r-1})) \wedge$

$(\forall j\text{: } j \in P\text{: } (\blacksquare k\text{: } j \in RECEIVE_i^r[k]) \geq LOW \Rightarrow (\exists s\text{: } s \leq r\text{: } j \in BROAD_i^s)\}$

$COMMIT_i^r := COMMIT_i^{r-1}$

$\{COMMIT_i^r = COMMIT_i^{r-1}\}$

**if** $(COMMIT_i^r = 0 \wedge (\blacksquare j\text{: } (\blacksquare k\text{: } j \in RECEIVE_i^r[k]) \geq HIGH) \geq HIGH) \rightarrow COMMIT_i^r := 1$

$\square$ **otherwise** $\rightarrow$ skip

**fi**

$\{I'_5\text{: } COMMIT_i^r = 1 \Leftrightarrow (\blacksquare j\text{: } (\blacksquare k\text{: } j \in RECEIVE_i^r[k]) \geq HIGH) \geq HIGH\}$

$\{I_{r-1}^r \wedge I'_1 \wedge I'_2 \wedge I'_3 \wedge I'_4 \wedge I'_5\}$

$\{I\}$

Figure 3 -- Proof outline of $NORMAL_i$

---

$(I'_1)$ $\Rightarrow (\forall i\text{: } i \in T\text{: } j \in RECEIVE_i^r[i])$

However, this contradicts $j \notin RECEIVE_i^r[i]$.

Now, since $i, j \in T \wedge (\blacksquare k\text{: } j \in RECEIVE_i^r[k]) \geq LOW$

$\Rightarrow i, j \in T \wedge (\exists k\text{: } k \in T\text{: } j \in RECEIVE_i^r[k])$

$(I'_1)$ $\Rightarrow j \in T \wedge (\exists k, s\text{: } k \in T \wedge s \leq r-1\text{: } j \in BROAD_k^s)$

$(I_4)_{s \leq r-1}$ $\Rightarrow j \in T \wedge (\exists s\text{: } s \leq r-1\text{: } * \in BROAD_j^{s-1})$

$(I_4)_{s \leq r-1}$ $\Rightarrow (\exists s\text{: } s \leq r-1\text{: } (\forall i\text{: } i \in T\text{: } j \in BROAD_i^s))$

$(I'_1)$ $\quad \Rightarrow (\forall i:\ i \in T:\ j \in RECEIVE_i^r[i])$

This also contradicts $j \notin RECEIVE_i^r[i]$.

Q.E.D.

**Assertion:** $(\forall i,j:\ i,j \in T \wedge r \geq 2:\ (* \in BROAD_j^{r-1} \Rightarrow j \in BROAD_i^r))$

The proof of this is as follows.

Suppose: $\quad r=2 \wedge i,j \in T \wedge * \in BROAD_j^{r-1}$

$(I'_1)$ $\quad \Rightarrow i,j \in T \wedge * \in RECEIVE_i^2[j]$

$(L_4)$ $\quad \Rightarrow (\exists s:\ s \leq 2:\ j \in BROAD_i^s)$

$(I_0)$ $\quad \Rightarrow j \in BROAD_i^2$

Suppose: $\quad r>2 \wedge i,j \in T \wedge * \in BROAD_j^{r-1}$

$(I'_1, (I_3)_{s \leq r-1})$ $\quad \Rightarrow i,j \in T \wedge * \in RECEIVE_i^r[j] \wedge * \notin RECEIVE_j^{r-1}[j]$

$(L_4, (I_1)_{s \leq r-1})$ $\quad \Rightarrow i,j \in T \wedge (\exists s:\ s \leq r:\ j \in BROAD_i^s) \wedge (\forall s:\ s \leq r-1:\ * \notin BROAD_j^{s-1})$

$(I_4)_{s \leq r-1}$ $\quad \Rightarrow (\exists s:\ s \leq r:\ j \in BROAD_i^s) \wedge (\forall s:\ s \leq r-1:\ j \notin BROAD_i^s)$

$\quad \Rightarrow j \in BROAD_i^r$

We now go on to prove,

**Lemma 1:** $(j \in T \wedge * \in BROAD_j^{s-2}) \Rightarrow (\forall i:\ i \in T:\ (\blacksquare k:\ j \in RECEIVE_i^s[k]) \geq HIGH)$

**Proof:** Suppose $j \in T \wedge * \in BROAD_j^{s-2}$

$(I_4)$ $\quad \Rightarrow (\forall k:\ k \in T:\ j \in BROAD_k^{s-1})$

$(I_1)$ $\quad \Rightarrow (\forall k:\ k \in T:\ (\forall i:\ i \in T:\ j \in RECEIVE_i^s[k]))$

$\quad \Rightarrow (\forall i:\ i \in T:\ (\forall k:\ k \in T:\ j \in RECEIVE_i^s[k]))$

$\quad \Rightarrow (\forall i:\ i \in T:\ (\blacksquare k:\ j \in RECEIVE_i^s[k]) \geq HIGH)$

**Lemma 2:** $(\forall i_1, i_2\colon i_1, i_2 \in T\colon (\blacksquare j\colon (\blacksquare k\colon j \in \mathrm{RECEIVE}_{i_1}^{s}[k]) \geq \mathrm{HIGH}) \geq$

$(\blacksquare j\colon (\blacksquare k\colon j \in \mathrm{RECEIVE}_{i_2}^{s-1}[k]) \geq \mathrm{HIGH})$

**Proof:** For any $j \in P$, we have $i_2 \in T \wedge (\blacksquare k\colon j \in \mathrm{RECEIVE}_{i_2}^{s-1}[k]) \geq \mathrm{HIGH}$

$\Rightarrow i_2 \in T \wedge (\blacksquare k\colon j \in \mathrm{RECEIVE}_{i_2}^{s-1}[k] \wedge k \in T) \geq \mathrm{LOW}$

$(I_1)$ $\Rightarrow (\forall m\colon m \in T\colon (\blacksquare k\colon j \in \mathrm{RECEIVE}_{m}^{s-1}[k] \wedge k \in T) \geq \mathrm{LOW})$

$(I_4)$ $\Rightarrow (\forall m\colon m \in T\colon (\exists s'\colon s' \leq s-1\colon j \in \mathrm{BROAD}_{m}^{s'}))$

$(I_1)$ $\Rightarrow (\forall m\colon m \in T\colon (\forall i\colon i \in T\colon j \in \mathrm{RECEIVE}_{i}^{s}[m]))$

$\Rightarrow (\forall i\colon i \in T\colon (\forall m\colon m \in T\colon j \in \mathrm{RECEIVE}_{i}^{s}[m]))$

$\Rightarrow (\forall i\colon i \in T\colon (\blacksquare m\colon j \in \mathrm{RECEIVE}_{i}^{s}[m]) \geq \mathrm{HIGH})$

$\Rightarrow i_1 \in T \wedge (\blacksquare k\colon j \in \mathrm{RECEIVE}_{i_1}^{s}[k]) \geq \mathrm{HIGH}$

Q.E.D.

**Lemma 3:** $(\forall j\colon j \in T\colon s' \leq s \wedge * \in \mathrm{BROAD}_{j}^{s'-2}) \Rightarrow (\forall i\colon i \in T\colon \mathrm{COMMIT}_{i}^{s}=1)$

**Proof:** Suppose $(\forall j\colon j \in T\colon s' \leq s \wedge * \in \mathrm{BROAD}_{j}^{s'-2})$

(lemma 1,2) $\Rightarrow (\forall j\colon j \in T\colon (\forall i\colon i \in T\colon (\blacksquare k\colon j \in \mathrm{RECEIVE}_{i}^{s}[k]) \geq \mathrm{HIGH}))$

$\Rightarrow (\forall i\colon i \in T\colon (\blacksquare j\colon (\blacksquare k\colon j \in \mathrm{RECEIVE}_{i}^{s}[k]) \geq \mathrm{HIGH}) \geq \mathrm{HIGH})$

$\Rightarrow (\forall i\colon i \in T\colon \mathrm{COMMIT}_{i}^{s}=1)$

We now prove that the protocol does indeed establish agreement among the functioning processors. In particular, we prove

$(r=R \wedge I) \Rightarrow (\mathrm{VALIDITY} \wedge \mathrm{AGREEMENT})$

where:

$\mathrm{AGREEMENT} \equiv (\forall i,m\colon i,m \in T\colon \mathrm{COMMIT}_{i}^{R}=\mathrm{COMMIT}_{m}^{R})$

$$\text{VALIDITY} \equiv (\text{GEN} \in T \wedge \text{BROAD}^{1}_{\text{GEN}}=\{*\}) \Rightarrow (\forall i\text{: } i \in T\text{: COMMIT}^{R}_{i}=1) \wedge$$

$$(\text{GEN} \in T \wedge \text{BROAD}^{1}_{\text{GEN}}=\{\phi\}) \Rightarrow (\forall i\text{: } i \in T\text{: COMMIT}^{R}_{i}=0)$$

Notice that AGREEMENT corresponds to BYZ1 and VALIDITY corresponds to BYZ2.

First, we establish VALIDITY.

Assume $\quad \text{GEN} \in T \wedge \text{BROAD}^{1}_{\text{GEN}}=\{*\}$

$(I_3) \quad \Rightarrow (\forall j\text{: } j \in T\text{: } * \in \text{BROAD}^{2}_{j})$

(lemma 3) $\quad \Rightarrow (\forall i\text{: } i \in T\text{: COMMIT}^{R}_{i}=1)$

Now, assume $\text{GEN} \in T \wedge \text{BROAD}^{1}_{\text{GEN}}=\phi$.

Suppose there exists $i \in T$ such that $\text{COMMIT}^{R}_{i}=1$.

Then, $i \in T \wedge \text{COMMIT}^{R}_{i}=1$

$(I_5) \quad \Rightarrow (i \in T) \wedge (\exists j\text{: } j \in T\text{: } (\blacksquare k\text{: } j \in \text{RECEIVE}^{R}_{i}[k]) \geq \text{HIGH})$

$(I_4) \quad \Rightarrow (i \in T) \wedge (\exists j,s\text{: } j \in T \wedge s \leq R\text{: } j \in \text{BROAD}^{s}_{i})$

$(I_4) \quad \Rightarrow (\exists j,s\text{: } j \in T \wedge s \leq R-1\text{: } * \in \text{BROAD}^{s}_{j})$

Let $s$ be the least integer such that $(\exists m\text{: } m \in T \wedge * \in \text{BROAD}^{s}_{m}\text{: true})$.

Since $\text{BROAD}^{1}_{\text{GEN}}=\phi$, by $(I_0, I_3)$, $s>2$.

Hence, $\quad s>2 \wedge m \in T \wedge * \in \text{BROAD}^{s}_{m}$

$(I_3) \quad \Rightarrow (\blacksquare j\text{: } (\blacksquare k\text{: } j \in \text{RECEIVE}^{s}_{m}[k]) \geq \text{HIGH} \wedge j \neq \text{GEN}) \geq \text{LOW}+\lceil \frac{s}{2} \rceil -2$

$\quad \Rightarrow (\exists m'\text{: } m' \in T\text{: } (\blacksquare k\text{: } m' \in \text{RECEIVE}^{s}_{m}[k]) \geq \text{HIGH})$

$(I_4) \quad \Rightarrow (\exists m',s'\text{: } m' \in T \wedge s' \leq s\text{: } m' \in \text{BROAD}^{s'}_{m})$

$(I_4) \quad \Rightarrow (\exists m',s'\text{:} m' \in T \wedge s' \leq s\text{: } * \in \text{BROAD}^{s'-1}_{m'})$

This, however, contradicts our assumption about s.

We now establish AGREEMENT.

We only need to prove:

$$GEN \in F \Rightarrow (\forall i,j: i,j \in T: COMMIT_i^R = COMMIT_j^R)$$

Assume $GEN \in F \wedge i \in T \wedge COMMIT_i^R = 1$.

$(I_5) \quad \Rightarrow (\blacksquare j: (\blacksquare k: j \in RECEIVE_i^R[k]) \geq HIGH) \geq HIGH$

$\quad \Rightarrow (\exists A: A \subset T \wedge |A| = LOW: (\forall j: j \in A: (\blacksquare k: j \in RECEIVE_i^R[k]) \geq HIGH))$

$(I_4) \quad \Rightarrow (\exists A: A \subset T \wedge |A| = LOW: (\forall j: j \in A: (\exists s: s \leq R-1: * \in BROAD_j^s))) \qquad (1)$

We now select $A_1$ and $s_1, s_2, \ldots, s_{LOW}$ that satisfy (1) such that for any other A and $s'_1, s'_2, \ldots s'_{LOW}$ that satisfy (1) we have:

$$s = \max(s_1, s_2, \ldots, s_{LOW}) \leq \max(s'_1, s'_2, \ldots, s'_{LOW}) \qquad (2)$$

Then $(\exists j_1: j_1 \in A_1 \subset T: * \in BROAD_{j_1}^s)$ and $R-1 \geq s \geq 2$. Suppose $R-1 \geq s \geq R-3 = 2t+1$. Then,

$R-1 \geq s \geq 2t+1 \wedge * \in BROAD_{j_1}^s$.

$(I_3) \quad \Rightarrow (\blacksquare j: (\blacksquare k: j \in RECEIVE_{j_1}^s[k]) \geq HIGH \wedge j \neq GEN) \geq LOW + \lceil \frac{s}{2} \rceil - 2$

$\quad \Rightarrow (\blacksquare j: (\blacksquare k: j \in RECEIVE_{j_1}^s[k]) \geq HIGH \wedge j \neq GEN) \geq HIGH-1 \qquad (3)$

Since $GEN \in F$ and GEN is not among those j satisfying (3),

$\quad \Rightarrow (\exists A_2: A_2 \subset T \wedge |A_2| = LOW: (\forall j: j \in A_2: (\blacksquare k: j \in RECEIVE_{j_1}^s[k]) \geq HIGH))$

$(I_4, j_1 \in T) \quad \Rightarrow (\exists A_2: A_2 \subset T \wedge |A_2| = LOW: (\forall j: j \in A_2: (\exists s': s' \leq s: j \in BROAD_{j_1}^{s'})))$

$(I_4) \quad \Rightarrow (\exists A_2: (A_2 \subset T \wedge |A_2| = LOW): (\forall j: j \in A_2: (\exists s': s' \leq s-1: * \in BROAD_j^{s'})))$

This contradicts the definition of $A_1$ and s. Therefore, $2 \leq s \leq R-4$. If $s=2$, then we have $\bigwedge_{j \in A_1} * \in BROAD_j^2$. Thus,

$(\text{lemma } 1) \quad \Rightarrow \bigwedge_{j \in A_1} (\forall m: m \in T: (\blacksquare k: j \in RECEIVE_m^4[k]) \geq HIGH)$

$$\Rightarrow (\forall m\colon m \in T\colon (\blacksquare j\colon (\blacksquare k\colon j \in RECEIVE_m^4[k]) \geq HIGH \wedge j \in T) \geq LOW = LOW + \lceil \tfrac{4}{2} \rceil - 2$$

$(I_3)$ $$\Rightarrow (\forall m\colon m \in T\colon (\exists s\colon s \leq 4 \leq R\colon * \in BROAD_m^s))$$

(lemma 3) $$\Rightarrow (\forall m\colon m \in T\colon COMMIT_m^R = 1)$$

If $2 < s \leq R-4$ then since $s > 2 \wedge j_1 \in T \wedge * \in BROAD_{j_1}^s$ we have:

$(I_3)$ $$\Rightarrow (\blacksquare j\colon (\blacksquare k\colon j \in RECEIVE_{j_1}^s[k]) \geq HIGH \wedge j \neq GEN) \geq LOW + \lceil \tfrac{s}{2} \rceil - 2 \qquad (4)$$

From $j_1 \in T \wedge * \in BROAD_{j_1}^s$ we can also get:

(lemma 1) $$\Rightarrow (\forall m\colon m \in T\colon (\blacksquare k\colon j_1 \in RECEIVE_m^{s+2}[k]) \geq HIGH)$$

$(j_1 \in T)$ $$\Rightarrow (\blacksquare k\colon j_1 \in RECEIVE_{j_1}^{s+2}[k]) \geq HIGH$$

But $s > 2 \wedge j_1 \in T \wedge * \in BROAD_{j_1}^s \Rightarrow (\blacksquare k\colon j_1 \in RECEIVE_{j_1}^s[k]) < HIGH$. Otherwise by $I_4$ we can deduce $(\exists s'\colon s' \leq s\colon * \in BROAD_{j_1}^{s'-1})$, and therefore $* \in RECEIVE_{j_1}^{s'}[j_1]$. This contradicts $(s > 2 \wedge j_1 \in T \wedge * \in BROAD_{j_1}^s) \Rightarrow * \notin RECEIVE_{j_1}^{s'}[j_1]$. So, by lemma 2 and (4) we have,

$$(\forall m\colon m \in T\colon (\blacksquare j\colon (\blacksquare k\colon j \in RECEIVE_m^{s+2}[k]) \geq HIGH \wedge j \notin GEN) >$$
$$(\blacksquare j\colon (\blacksquare k\colon j \in RECEIVE_{j_1}^s[k]) \geq HIGH \wedge j \notin GEN) \geq LOW + \lceil \tfrac{s}{2} \rceil - 2$$

Hence, we have

$$(\forall m\colon m \in T\colon (\blacksquare j\colon (\blacksquare k\colon j \in RECEIVE_m^{s+2}[k]) \geq HIGH \wedge j \neq GEN) \geq LOW + \lceil \tfrac{s+2}{2} \rceil - 2$$

$(I_3)$ $$\Rightarrow (\forall m\colon m \in T\colon (\exists s'\colon s' \leq s+2 \leq R-2\colon * \in BROAD_m^{s'}))$$

(lemma 3) $$\Rightarrow (\forall m\colon m \in T\colon COMMIT_m^R = 1)$$

Thus we have proved the correctness of the Byzantine Agreement Program.


<u>Acknovedgments</u>

The author would like to thank David Gries and Fred B. Schneider for assistance in preparing this paper.

## References

[DS82] Dolev, D., and H.R. Strong, Polynomial algorithms for multiple processor agreement, Proc. 14th Annual ACM Symposium on Theory of Computing, May 1982, San Fransisco, CA, 401-407.

[LFF82] Lynch, N.A., M.J. Fischer, and R. Fowler. A simple and efficient byzantine generals algorithm, Technical Report GIT-ICS-82/02, Georgia Institute of Technology, February 1982.