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 \textsc{Init} in Figure 1; subsequent execution of processes is modelled by the loop labelled \textsc{Byz}. Note that two types of processors execute. Those that are faulty are modelled by program \textsc{Faulty}, which can do anything; those that are non-faulty are modelled by program \textsc{Normal}, which correctly executes the agreement protocol as defined in Figure 2. \textsc{Gen} can be a member of either \textsc{F} or \textsc{T}.

The behavior of the communications network is modelled by variable \textsc{Broad}, defined as follows:

\[ \textsc{Broad}_{i}^{r}[j] = \text{"The set of messages broadcast by processor } i \text{ to processor } j \text{ during round } r." \]

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

\[ (\forall j, k: j, k \in \textsc{Tuf}: i \in \textsc{T} \Rightarrow \textsc{Broad}_{i}^{r}[j] = \textsc{Broad}_{i}^{r}[k]) \]

By abuse of notation, \textsc{Broad}_{i}^{r} will represent the message broadcast by processor \textsc{i}, when all messages \textsc{i} broadcast in that round were the same.

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

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

-2-
\( r := 1; \quad i := 0; \)

\textbf{INIT:} \quad \textbf{do} \ i \neq n \ 	ext{+ \ \textbf{i := i+1;}\ mitochondria
\begin{align*}
& \text{receive}_{i}^{T}[1... n] := \emptyset; \\
& \text{commit}^{T}_{i} := 0; \ mitochondria
& \text{if} \ (i = \text{GEN} \wedge \text{GEN} \in T) \ 	ext{+ \ if true + \ broad}^{T}_{i} := \{\ast\} \ mitochondria
& \quad \text{if true + \ broad}^{T}_{i} := \emptyset \ mitochondria
\end{align*}
\text{fi}
\begin{align*}
& \text{if} \ (i = \text{GEN} \wedge \text{GEN} \in F) \ 	ext{+ j := 0;} \ mitochondria
& \text{do} \ j \neq n \ 	ext{+ j := j+1;} \ mitochondria
& \quad \text{if true + \ broad}^{T}_{j} := \{\ast\} \ mitochondria
& \quad \text{if true + \ broad}^{T}_{j} := \emptyset \ mitochondria
\end{align*}
\text{fi}
\text{od}
\text{if} \ i \neq \text{GEN} \ 	ext{+ broad}^{T}_{i} [1... n] := \emptyset \ mitochondria
\text{od;}

\{(\forall i \in P : \text{receive}^{T}_{i} = \emptyset \wedge \text{commit}^{T}_{i} = 0 \wedge (i \neq \text{GEN} \Rightarrow \text{broad}^{T}_{i} [1... n] = \emptyset) \wedge (i = \text{GEN} \Rightarrow (\forall j \in P : j \neq \text{broad}^{T}_{i} [1... n])))\}

\{I\}

\textbf{BYZ:} \quad \textbf{do} \ r \neq R \ 	ext{+ } \{r < 2t + 4 \wedge I\}
\begin{align*}
& \quad \text{r := r+1;} \ mitochondria
& \quad \{\text{IR}^{r}_{i} \wedge r \geq 2\} \ mitochondria
\end{align*}
\textbf{cobegin}
\begin{align*}
& \quad // \quad \text{NORMAL}_{i} \ mitochondria
& \quad \text{i} \in T \ mitochondria
& \quad // \quad \text{FAULTY}_{i} \ mitochondria
& \quad \text{i} \in F \ mitochondria
\end{align*}
\textbf{coend}
\text{od}
\{r = R \wedge I\}

\textbf{Figure 1} -- Byzantine Agreement Program
Finally, we define

$$0 \leq |F| \leq t$$

$$P \equiv T \cup F$$

$$\text{LOW} \equiv t+1$$

$$\text{HIGH} \equiv 2t+1$$

$$R \equiv 2t+4$$

3. Correctness of the Program

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

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

and

$$I_0 \equiv (\forall i \in P: ((i \not\in \text{GEN}) \Rightarrow \text{BROAD}^1_{i}[1...n] = \emptyset) \land$$

$$(i \in \text{GEN} \Rightarrow (\forall j: j \in P: j \not\in \text{BROAD}^1_{i}[1...n])))$$

$$I_1 \equiv (\forall j, s: j \in T \land s \geq 2: \text{RECEIVE}^g_{i}[j] = \cup_{s' = 1}^{s-1} j$$

$$I_2 \equiv (\forall j, k: j \in P: \text{BROAD}^g_{i}[j] = \text{BROAD}^g_{i}[k] = \text{BROAD}^g_{i})$$

$$I_3 \equiv (\text{BROAD}^1_{\text{GEN}[i]} = \{\star\} \Rightarrow \ast \in \text{BROAD}^2_{i} \land (\text{BROAD}^1_{\text{GEN}[i]} = \emptyset \Rightarrow \text{BROAD}^2_{i} = \emptyset)) \land$$

$$((s > 2 \land \ast \in \text{BROAD}^g_{i}) \Rightarrow (\ast \not\in \text{RECEIVE}^g_{i}[i] \land$$

$$([k]: j \in \text{RECEIVE}^g_{i}[k] \Rightarrow \text{HIGH} \land j \not\in \text{GEN}) \Rightarrow (\text{LOW} \land \text{HIGH} - 2)) \land$$

$$((s > 2 \land \exists j: ([k]: j \in \text{RECEIVE}^g_{i}[k] \Rightarrow \text{HIGH} \land j \not\in \text{GEN}) \Rightarrow (\text{LOW} \land \text{HIGH} - 2)) \Rightarrow$$

$$([s': s' \leq s: \ast \in \text{BROAD}^g_{i}[s'])$$
j := 0;

\textbf{do} j \neq n \rightarrow j := j + 1;

\textbf{if} BROAD^r_{i-1}[i] \neq \emptyset \rightarrow RECEIVE^r_i[j] := RECEIVE^r_{i-1}[j] \cup BROAD^r_{j-1}[i]

\textbf{if} BROAD^r_{j-1}[i] = \emptyset \rightarrow \text{skip}

\textbf{fi}

\textbf{od};

OK_i := \text{true};

\textbf{wait} OK_1 \land OK_2 \land \ldots \land OK_n;

BROAD^r_i := \emptyset; \quad OK_i := \text{false};

\textbf{if} r = 2 \rightarrow \textbf{if} RECEIVE^r_i[GEN] = \{\ast\} \land i \neq GEN \rightarrow BROAD^r_i := BROAD^r_i \cup \{\ast\}

\textbf{if} RECEIVE^r_i[GEN] = \emptyset \lor i = GEN \rightarrow \text{skip}

\textbf{fi}

\textbf{else} \ r > 2 \rightarrow \textbf{if} (\ast \notin RECEIVE^r_i[i] \land

(\exists j : j \neq GEN \land (\exists k : j \in RECEIVE^r_i[k]) \geq \text{HIGH}) \geq \text{LOW} + \lceil \frac{r}{2} \rceil - 2

\rightarrow BROAD^r_i := BROAD^r_i \cup \{\ast\}

\textbf{else} \ \text{otherwise} \rightarrow \text{skip}

\textbf{fi}

\textbf{fi};

j := 0;

\textbf{do} j \neq n \rightarrow j := j + 1;

\textbf{if} ((j \notin RECEIVE^r_i[i]) \land

(\ast \in RECEIVE^r_i[j] \lor (\exists k : j \in RECEIVE^r_i[k]) \geq \text{LOW}))

\rightarrow BROAD^r_i := BROAD^r_i \cup \{j\}

\textbf{else} \ \text{otherwise} \rightarrow \text{skip}

\textbf{fi}

\textbf{od};

\text{COMM}_i^r := \text{COMM}_{i-1}^r

\textbf{if} \ (\text{COMM}_i^r = 0 \land (\exists j : (\exists k : j \in RECEIVE^r_i[k]) \geq \text{HIGH}) \geq \text{HIGH}) \rightarrow \text{COMM}_i^r := 1

\textbf{else} \ \text{otherwise} \rightarrow \text{skip}

\textbf{fi}

\textbf{end}

\textbf{end}

\textbf{end} -- \text{NORMAL}_i
\[ I_4 \equiv (\forall j, s: j \in T \land s \geq 2: \ast \in \text{BROAD}^{s-1}_j \iff j \in \text{BROAD}^s_i \land \\
(\forall j: j \in P: ((\exists k: j \in \text{RECEIVE}^s_i[k]) \geq \text{LOW}) \implies \\
(\exists s': s' \leq s: j \in \text{BROAD}^{s'}_i)) \]

\[ I_5 \equiv (\exists j: (\exists k: j \in \text{RECEIVE}^s_i[k]) \geq \text{HIGH}) \iff \text{HIGH} \iff \text{COMMIT}^s_i = 1 \]

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:** \( (\forall i, j: i, j \in T \land r \geq 2: j \in \text{BROAD}^r_i \implies \ast \in \text{BROAD}^{r-1}_j) \)

This is proved as follows:

**Suppose:** \( r = 2 \land i, j \in T \land j \in \text{BROAD}^r_i \)

\[ (I_4) \implies \ast \in \text{RECEIVE}^2_i[j] \lor (\exists k: j \in \text{RECEIVE}^2_i[k]) \geq \text{LOW} \]

\[ (I'_1) \implies \ast \in \text{RECEIVE}^2_i[j] \]

\[ (I'_0) \implies \ast \in \text{BROAD}^1_j \]

**Suppose:** \( r \geq 2 \land i, j \in T \land j \in \text{BROAD}^r_i \)

\[ (I_4) \implies (j \notin \text{RECEIVE}^r_i[i]) \land \\
(\ast \in \text{RECEIVE}^r_i[j] \lor (\exists k: j \in \text{RECEIVE}^r_i[k]) \geq \text{LOW}) \]

\[ (I'_1) \implies j \notin \text{RECEIVE}^r_i[i] \land (\ast \in \text{BROAD}^{r-1}_j \lor (\exists s: s \leq r-1: \ast \in \text{BROAD}^{s-1}_j) \lor \\
(\exists k: j \in \text{RECEIVE}^r_i[k]) \geq \text{LOW}) \]

Since \( j \in T \land (\exists s: s \leq r-1: \ast \in \text{BROAD}^{s-1}_j) \)

\[ (I_4) \land s \leq r-1 \implies (\forall i: i \in T: (\exists s: s \leq r-1: j \in \text{BROAD}^s_i) \]

-6-
\{ r^f_{r-1} \}
\quad j := 0;
\quad \textbf{do} \quad j := \text{n} \rightarrow j := j + 1;
\quad \begin{array}{l}
\quad \textbf{if} \ BROAD^r_{r-1}[i] \neq \emptyset \rightarrow RECEIVE^r_1[j] := RECEIVE^r_{r-1}[j] \cup BROAD^r_{r-1}[i] \\
\quad \quad \text{\} BROAD^r_{j-1}[i] = \emptyset \rightarrow \text{skip} \\
\quad \textbf{fi}
\quad \{(\forall k: 1 \leq k \leq r \wedge k \in T: RECEIVE^r_1[k] = \cup BROAD^s_{s=1} \}
\textbf{od};
\quad \{ I'_1 : (\forall j \in T: RECEIVE^r_1[j] = \cup BROAD^s_{s=1} \}
\quad \textbf{OK}^r_1 := \text{true};
\quad \textbf{wait} \text{OK}^r_1 \wedge \text{OK}^r_2 \wedge \ldots \wedge \text{OK}^r_n;
\quad BROAD^r_1 := \emptyset;
\quad \textbf{OK}^r_1 := \text{false};
\quad \{BROAD^r_1 = \emptyset \wedge \}
\quad I'_2 : (\forall j, k: j, k \in P: BROAD^r_1[j] = BROAD^r_1[k] = BROAD^r_1) \\
\quad \textbf{if} \ r = 2 \rightarrow \textbf{if} \ i \in \text{GEN} \wedge RECEIVE^r_1[\text{GEN}] = \{\ast\} \rightarrow BROAD^r_1 := BROAD^r_1 \cup \{\ast\} \\
\quad \quad \text{\} i \in \text{GEN} \vee RECEIVE^r_1[\text{GEN}] = \emptyset \rightarrow \text{skip} \\
\quad \textbf{fi}
\quad \quad \textbf{fi}
\quad \quad \textbf{fi}
\quad \{ I'_2 \wedge (\forall j: j \in P: j \notin BROAD^r_1) \wedge \}
\quad \quad I'_3 : (\text{BROAD}^1_{\text{GEN}}[i] = \{\ast\} \Rightarrow * \in \text{BROAD}^2_{\text{GEN}} \wedge (\text{BROAD}^1_{\text{GEN}}[i] = \emptyset \Rightarrow \text{BROAD}^2_{\text{GEN}} = \emptyset) \wedge \)
\quad \quad \quad ((r > 2 \wedge * \in \text{BROAD}^r_{\text{GEN}}) \Rightarrow
\quad \quad \quad \quad (\nexists j: (j \in \text{RECEIVE}^r_1[k]) \geq \text{HIGH} \wedge j \notin \text{GEN}) \geq (\text{LOW} + [r/2] - 2)) \wedge
\quad \quad \quad (((r > 2 \wedge \exists j: (j \in \text{RECEIVE}^r_1[k]) \geq \text{HIGH} \wedge j \notin \text{GEN}) \geq (\text{LOW} + [r/2] - 2)) \Rightarrow
\quad \quad \quad \quad (\exists s: s \leq r: * \in \text{BROAD}^s_{i}))
\quad j := 0;
\quad \textbf{do} \quad j := \text{n} \rightarrow j := j + 1;
if \((j \notin \text{RECEIVE}_{1}^{_i}[i]) \land \)
\((* \in \text{RECEIVE}_{1}^{_i}[j] \lor (\exists k: j \in \text{RECEIVE}_{1}^{_i}[k] \geq \text{LOW}))) \land \\
+ \text{BROAD}_{1}^{_i} := \text{BROAD}_{1}^{_i} \cup \{j\}
\)
\(\) otherwise \(\rightarrow\) skip
\fi

ed;

\{L_4: (\forall j: j \in T: j \in \text{BROAD}_{1}^{_i} \Rightarrow \\
(j \notin \text{RECEIVE}_{1}^{_i}[i] \land (* \in \text{RECEIVE}_{1}^{_i}[j] \lor (\exists k: j \in \text{RECEIVE}_{1}^{_i}[k] \geq \text{LOW}))) \land \\
(* \in \text{RECEIVE}_{1}^{_i}[j] \lor (\exists k: j \in \text{RECEIVE}_{1}^{_i}[k] \geq \text{LOW}) \Rightarrow \\
(\exists s: s \leq r: j \in \text{BROAD}_1^s) \land I_2'
\}

\{I_2' \land \\
I_4': (\forall j: j \in T: (j \in \text{BROAD}_{1}^{_i} \iff * \in \text{BROAD}_{1}^{_i-1})) \land \\
(\forall j: j \in T: (\exists k: j \in \text{RECEIVE}_{1}^{_i}[k] \geq \text{LOW}) \Rightarrow (\exists s: s \leq r: j \in \text{BROAD}_1^s)
\}
\begin{align*}
\text{COMMIT}_{1}^{_i} &= \text{COMMIT}_{1}^{_i-1} \\
\{\text{COMMIT}_{1}^{_i} = \text{COMMIT}_{1}^{_i-1}\}
\end{align*}

if \(\text{COMMIT}_{1}^{_i} = 0 \land (\exists j: (\exists k: j \in \text{RECEIVE}_{1}^{_i}[k] \geq \text{HIGH}) \geq \text{HIGH}) \rightarrow \text{COMMIT}_{1}^{_i} = 1
\)
\(\) otherwise \(\rightarrow\) skip
\fi

\{I_5': \text{COMMIT}_{1}^{_i} = 1 \iff (\exists j: (\exists k: j \in \text{RECEIVE}_{1}^{_i}[k] \geq \text{HIGH}) \geq \text{HIGH})
\}
\{I_5' \land I_1' \land I_2' \land I_3' \land I_4' \land I_5'
\}
\{I\}

---

Figure 3 -- Proof outline of \(\text{NORMAL}_{1}\)

\begin{align*}
(I_1') & \Rightarrow (\forall i: i \in T: j \in \text{RECEIVE}_{1}^{_i}[i]) \\
\text{However, this contradicts } j \notin \text{RECEIVE}_{1}^{_i}[i].
\end{align*}

Now, since \(i, j \in T \land (\exists k: j \in \text{RECEIVE}_{1}^{_i}[k] \geq \text{LOW})
\)
\(\Rightarrow i, j \in T \land (\exists k: k \in T: j \in \text{RECEIVE}_{1}^{_i}[k])
\)
\begin{align*}
(I_1') & \Rightarrow j \in T \land (\exists k: k \in T: s \leq r-1: j \in \text{BROAD}_k^s) \\
(I_4') & \Rightarrow j \in T \land (\exists k: s \leq r-1: j \in \text{BROAD}_k^s) \\
\end{align*}
\(\)
\begin{align*}
(I_4') & \Rightarrow (\exists s: s \leq r-1: (\forall i: i \in T: j \in \text{BROAD}_k^s))
\end{align*}
(I'1) \quad \Rightarrow (\forall i: i \in T: j \in \text{RECEIVE}^r_i [i])

This also contradicts \( j \notin \text{RECEIVE}^r_i [i] \).

Q.E.D.

**Assertion:** \((\forall i,j: i,j \in T \land r \geq 2: (\forall \in \text{BROAD}^{r-1}_j \Rightarrow j \in \text{BROAD}^r_i)\)\)

The proof of this is as follows.

Suppose: \(r=2 \land i,j \in T \land * \in \text{BROAD}^{r-1}_j\)

\((I'1)\quad \Rightarrow i,j \in T \land * \in \text{RECEIVE}^r_i [j]\)

\((I_4)\quad \Rightarrow (\exists s: s \leq 2: j \in \text{BROAD}^r_i)\)

\((I_0)\quad \Rightarrow j \in \text{BROAD}^2_i\)

Suppose: \(r>2 \land i,j \in T \land * \in \text{BROAD}^{r-1}_j\)

\((I'1, (I_3)_{s \leq r-1})\quad \Rightarrow i,j \in T \land * \in \text{RECEIVE}^r_i [j] \land * \notin \text{RECEIVE}^{r-1}_j [j]\)

\((I_4, (I_1)_{s \leq r-1})\quad \Rightarrow i,j \in T \land (\exists s: s \leq r: j \in \text{BROAD}^s_i) \land (\forall s: s \leq r-1: * \notin \text{BROAD}^s_j)\)

\((I_4)_{s \leq r-1} \quad \Rightarrow (\exists s: s \leq r: j \in \text{BROAD}^s_i) \land (\forall s: s \leq r-1: j \notin \text{BROAD}^s_i)\)

\(\Rightarrow j \in \text{BROAD}^r_i\)

We now go on to prove,

**Lemma 1:** \((j \in T \land * \in \text{BROAD}^{s-2}_j) \Rightarrow (\forall i: i \in T: (\forall k: j \in \text{RECEIVE}^s_i [k]) \geq \text{HIGH})\)

**Proof:** Suppose \(j \in T \land * \in \text{BROAD}^{s-2}_j\)

\((I_4)\quad \Rightarrow (\forall k: k \in T: j \in \text{BROAD}^{s-1}_k)\)

\((I_1)\quad \Rightarrow (\forall k: k \in T: (\forall i: i \in T: j \in \text{RECEIVE}^s_i [k]))\)

\(\Rightarrow (\forall i: i \in T: (\forall k: k \in T: j \in \text{RECEIVE}^s_i [k]))\)

\(\Rightarrow (\forall i: i \in T: (\forall k: j \in \text{RECEIVE}^s_i [k]) \geq \text{HIGH})\)

-9-
Lemma 2: \((\forall i_1, i_2: i_1, i_2 \in T: (\forall j: (\forall k: j \in \text{RECEIVE}^{s-1}_{i_1}[k]) \geq \text{HIGH}) \land (\forall j: (\forall k: j \in \text{RECEIVE}^{s-1}_{i_2}[k]) \geq \text{HIGH}))\)

Proof: For any \(j \in P\), we have \(i_2 \in T \land (\forall k: j \in \text{RECEIVE}^{s-1}_{i_2}[k]) \geq \text{HIGH}\)

\[\Rightarrow i_2 \in T \land (\forall k: j \in \text{RECEIVE}^{s-1}_{i_2}[k]) \geq \text{LOW}\]

\((I_1)\)

\[\Rightarrow (\forall m: m \in T: (\forall k: j \in \text{RECEIVE}^{s-1}_{m}[k]) \land k \in T) \geq \text{LOW}\]

\((I_4)\)

\[\Rightarrow (\forall m: m \in T: (\exists s': s' \leq s-1: j \in \text{BROAD}^{s'}_{m}))\]

\((I_1)\)

\[\Rightarrow (\forall m: m \in T: (\forall i: i \in T: j \in \text{RECEIVE}^{s}_{i}[m]))\]

\[\Rightarrow (\forall i: i \in T: (\forall m: m \in T: j \in \text{RECEIVE}^{s}_{i}[m]))\]

\[\Rightarrow (\forall i: i \in T: (\forall m: m \in T: j \in \text{RECEIVE}^{s}_{i}[m]) \geq \text{HIGH})\]

\[\Rightarrow i_1 \in T \land (\forall k: j \in \text{RECEIVE}^{s}_{i_1}[k]) \geq \text{HIGH}\]

Q.E.D.

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

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

\([\text{lemma 1,2}]\)

\[\Rightarrow (\forall j: j \in T: (\forall i: i \in T: (\forall k: j \in \text{RECEIVE}^{s}_{i}[k]) \geq \text{HIGH}))\]

\[\Rightarrow (\forall i: i \in T: (\forall j: (\forall k: j \in \text{RECEIVE}^{s}_{i}[k]) \geq \text{HIGH}) \geq \text{HIGH})\]

\[\Rightarrow (\forall i: i \in T: \text{COMMIT}^{s-1}_{i}=1)\]

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

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

where:

\[\text{AGREEMENT} \equiv (\forall i, m: i, m \in T: \text{COMMIT}^{R}_{i} = \text{COMMIT}^{R}_{m})\]
VALIDITY \equiv (\text{GEN} \in T \land \text{BROAD}_{\text{GEN}}^1 = \{\ast\}) \Rightarrow (\forall i: i \in T: \text{COMMIT}_{i}^R = 1) \land
\quad (\text{GEN} \in T \land \text{BROAD}_{\text{GEN}}^1 = \varnothing) \Rightarrow (\forall i: i \in T: \text{COMMIT}_{i}^R = 0)

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

First, we establish VALIDITY.

Assume \text{GEN} \in T \land \text{BROAD}_{\text{GEN}}^1 = \{\ast\}

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

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

Now, assume \text{GEN} \in T \land \text{BROAD}_{\text{GEN}}^1 = \varnothing.

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

Then, \( i \in T \land \text{COMMIT}_{i}^R = 1 \)

(I_5) \Rightarrow (i \in T) \land (\exists j: j \in T: (\exists k: j \in \text{RECEIVE}_{i}^R[k] \supseteq \text{HIGH}))

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

(I_4) \Rightarrow (\exists j, s: j \in T \land s \leq R - 1: \ast \in \text{BROAD}_{j}^s)

Let \( s \) be the least integer such that (\exists m: m \in T \land \ast \in \text{BROAD}_m^s: \text{true}).

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

Hence, \( s > 2 \land m \in T \land \ast \in \text{BROAD}_m^s \)

(I_3) \Rightarrow (\exists j: (\exists k: j \in \text{RECEIVE}_m^s[k] \supseteq \text{HIGH} \land j \neq \text{GEN}) \supseteq \text{LOW} + \lceil \frac{s}{2} \rceil - 2

\Rightarrow (\exists m': m' \in T: (\exists k: m' \in \text{RECEIVE}_m^s[k] \supseteq \text{HIGH}))

(I_4) \Rightarrow (\exists m', s': m' \in T \land s' \leq s: m' \in \text{BROAD}_m^{s'})

(I_4) \Rightarrow (\exists m', s': m' \in T \land s' \leq s: \ast \in \text{BROAD}_m^{s' - 1})

This, however, contradicts our assumption about \( s \).
We now establish AGREEMENT.

We only need to prove:

\[
\text{GEN } \in F \implies (\forall i, j : i, j \in T : \text{COMMIT}_i^R = \text{COMMIT}_j^R)
\]

Assume \(\text{GEN } \in F \land i \in T \land \text{COMMIT}_i^R = 1\).

\((I_5) \implies (\exists j : (\forall k : j \in \text{RECEIVE}_i^R(k) \geq \text{HIGH}) \implies \text{HIGH})
\]

\(\implies (\exists A : A \subseteq T \land |A| = \text{LOW} : (\forall j : j \in A : (\exists k : j \in \text{RECEIVE}_i^R(k) \geq \text{HIGH})))
\]

\((I_4) \implies (\exists A : A \subseteq T \land |A| = \text{LOW} : (\forall j : j \in A : (\exists s : s \leq R - 1 : * \in \text{BROAD}_j^s))) \quad (1)
\]

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

\[
s = \max(s_1, s_2, \ldots, s_{\text{LOW}}) \leq \max(s'_1, s'_2, \ldots, s'_{\text{LOW}})
\]

(2)

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

\[
R - 1 \geq s \geq 2t + 1 \land * \in \text{BROAD}_{j_1}^s
\]

\((I_3) \implies (\exists j : (\exists k : j \in \text{RECEIVE}_{j_1}^s(k) \geq \text{HIGH} \land j \neq \text{GEN}) \geq \text{LOW} + [\frac{s}{2}] - 2
\]

\(\implies (\exists j : (\exists k : j \in \text{RECEIVE}_{j_1}^s(k) \geq \text{HIGH} \land j \neq \text{GEN}) \geq \text{HIGH} - 1 \quad (3)
\]

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

\[
(\exists A_2 : A_2 \subseteq T \land |A_2| = \text{LOW} : (\forall j : j \in A_2 : (\exists k : j \in \text{RECEIVE}_{j_1}^s(k) \geq \text{HIGH})))
\]

\((I_4, j_1 \in T) \implies (\exists A_2 : A_2 \subseteq T \land |A_2| = \text{LOW} : (\forall j : j \in A_2 : (\exists s' : s' \leq s : j \in \text{BROAD}_{j_1}^{s'})))
\]

\((I_4) \implies (\exists A_2 : (A_2 \subseteq T \land |A_2| = \text{LOW}) : (\forall j : j \in A_2 : (\exists s' : s' \leq s - 1 : * \in \text{BROAD}_{j_1}^{s'})))
\]

This contradicts the definition of \(A_1\) and \(s\). Therefore, \(2 \leq s \leq R - 4\). If \(s = 2\), then we have \(\land * \in \text{BROAD}_{j}^2\). Thus,

\[
\text{j} \in A_1
\]

(lemma 1) \implies \land (\forall m : m \in T : (\exists k : j \in \text{RECEIVE}_{m}^4(k) \geq \text{HIGH})
\]

\[
j \in A_1
\]

-12-
\[
(\forall m \in T: (m \in j \in \text{RECEIVE}^s_m[k]) \Rightarrow \text{HIGH} \land j \in T) \Rightarrow \text{LOW} + \frac{s^2}{2} = 2
\]

\[
(\forall m \in T: (\exists s: s \leq 4 \leq R; s \in \text{BROAD}_m^s))
\]

(lemma 3) \[
(\forall m \in T: \text{COMMIT}_m^R = 1)
\]

If \(2 < s \leq R - 4\) then since \(s > 2 \land j_1 \in T \land * \in \text{BROAD}_j_{j_1}^s\) we have:

\[
(\forall m \in T: (m \in j \in \text{RECEIVE}^s_j[k]) \Rightarrow \text{HIGH} \land j \not\in \text{GEN}) \Rightarrow \text{LOW} + \frac{s^2}{2} = 2
\]

From \(j_1 \in T \land * \in \text{BROAD}_j_{j_1}^s\) we can also get:

\[
(\forall m \in T: (m \in j \in \text{RECEIVE}^{s+2}_m[k]) \Rightarrow \text{HIGH})
\]

\[
(j_1 \in T) \Rightarrow (m \in j \in \text{RECEIVE}^{s+2}_j[k]) \Rightarrow \text{HIGH}
\]

But \(s > 2 \land j \in T \land * \in \text{BROAD}_j_{j_1}^s \Rightarrow (m \in j \in \text{RECEIVE}_m^s[k]) \Rightarrow \text{HIGH}\). Otherwise by I_4 we can deduce \((\exists s': s' \leq s; s' \in \text{BROAD}_j_{j_1}^{s'-1})\), and therefore \(* \in \text{RECEIVE}_j_{j_1}^s[k]\). This contradicts

\[
(s > 2 \land j \in T \land * \in \text{BROAD}_j_{j_1}^s) \Rightarrow * \in \text{RECEIVE}_j_{j_1}^{s'}[k].
\]

So, by lemma 2 and (4) we have,

\[
(\forall m \in T: (m \in j \in \text{RECEIVE}^{s+2}_m[k]) \Rightarrow \text{HIGH} \land j \not\in \text{GEN}) >
\]

\[
(m \in j \in \text{RECEIVE}^s_j[k]) \Rightarrow \text{HIGH} \land j \not\in \text{GEN}) \Rightarrow \text{LOW} + \frac{s^2}{2} = 2
\]

Hence, we have

\[
(\forall m \in T: (m \in j \in \text{RECEIVE}^{s+2}_m[k]) \Rightarrow \text{HIGH} \land j \not\in \text{GEN}) \Rightarrow \text{LOW} + \frac{s^2}{2} = 2
\]

\[
(\forall m \in T: (\exists s': s' \leq s + 2 \leq R - 2; s' \in \text{BROAD}_m^{s'})
\]

(lemma 3) \[
(\forall m \in T: \text{COMMIT}_m^R = 1)
\]

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

Acknowledgments

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