# FEDERATED BYZANTINE AGREEMENT SYSTEM AND STELLAR CONSENSUS PROTOCOL

HIDENORI SHINOHARA

## Contents

## 1. Federated Byzantine Agreement System

### 1.1. **Quorums.**

**Definition 1.1.1 (Federated Byzantine Agreement System).** Let $V$ be a set and $Q : V \to 2^{2^V} \setminus \{\emptyset\}$ be a function such that $\forall v \in V, \forall q \in Q(v), v \in q$. Then we call the pair $\langle V, Q \rangle$ a federated Byzantine agreement system, or FBAS for short. Each $q$ in $Q(v)$ is called a quorum slice for each $v \in V$.

*Remark* 1.1.2.

- For each node $v$, $Q(v)$ is a set of subsets of $V$. For instance, node $v_1$ may trust $v_2, v_3, v_4$ and may have $\{v_1, v_2, v_3, v_4\} \in Q(v_1) \subset 2^V$.
- Note that we explicitly exclude $\emptyset$ from the co-domain. In other words, we want $Q(v) \neq \emptyset$ for all $v \in V$. If $Q(v) = \emptyset$ for some $v \in V$, it satisfies $\forall q \in Q(v), v \in q$. As we will see, each $q \in Q(v)$ is the list of nodes that $v$ trusts. If $v$ has no list of nodes that it trusts, $v$ cannot really do anything. Thus we want $Q(v) \neq \emptyset$ for all $v \in V$.
- Consider the case when $V = \emptyset$. Note that $2^{\emptyset} = \{\emptyset\}$ and thus $2^{2^{\emptyset}} = \{\emptyset, \{\emptyset\}\}$. Thus $V$ forms an FBAS where $Q$ is the map $\emptyset \mapsto \{\{\emptyset\}\}$.

**Definition 1.1.3 (Quorum).** Let $\langle V, Q \rangle$ be an FBAS. $U \subset V$ is called a quorum if and only if $U \neq \emptyset$ and $\forall v \in U, \exists q \in Q(v), q \subset U$.

**Theorem 1.1.4.** *In an FBAS $\langle V, Q \rangle$, the union of two quorums is a quorum.*

*Proof.* Let $U_1, U_2$ be two quorums. Let $v \in U_1 \cup U_2$. Then $v \in U_i$ for $i = 1$ or $i = 2$. Then $q \subset U_i$ for some $q \in Q(v)$. Therefore, $q \subset U_1 \cup U_2$, so $U_1 \cup U_2$ is indeed a quorum. □

**Corollary 1.1.5.** *The set of quorums of a given FBAS is closed under union.*

**Theorem 1.1.6.** *In an FBAS $\langle V, Q \rangle$, $V$ is a quorum.*

*Proof.* For any $v \in V$, for any $q \in Q(v)$, $q \subset V$. Therefore, $V$ is indeed a quorum. □

**Example 1.1.7.** One might wonder if the intersection of quorums is always a quorum. However, this is not true in general.

Let $V = \{v_1, \ldots, v_4\}$ and

- $Q(v_1) = \{\{v_1, v_2, v_3\}, \{v_1, v_2, v_4\}, \{v_1, v_3, v_4\}\}$,
- $\vdots$
- $Q(v_4) = \{\{v_1, v_2, v_4\}, \{v_1, v_3, v_4\}, \{v_2, v_3, v_4\}\}$.

In other words, $Q(v_i) = \{U \subset V \mid |U| = 3, v_i \in U\}$.

Then $U_1 = \{v_1, v_2, v_3\}$ is a quorum, and $U_2 = \{v_2, v_3, v_4\}$ is a quorum. However, $U_1 \cap U_2 = \{v_2, v_3\}$ is not a quorum because the size of any quorum slice is 3.

**Definition 1.1.8 (Quorum Intersection).** Let $\langle V, Q \rangle$ be an FBAS. We say $\langle V, Q \rangle$ enjoys quorum intersection if and only if $U_1 \cap U_2 \neq \emptyset$ for any pair of quorums $U_1, U_2$.

**Definition 1.1.9 (Delete).** Let $\langle V, Q \rangle$ be an FBAS and $B \subset V$. Then the FBAS $\langle V, Q \rangle^B$ is defined to be $\left\langle V \setminus B, Q^B \right\rangle$ where $\forall v \in V \setminus B, Q^B(v) = \{q \setminus B \mid q \in Q(v)\}$.

*Remark* 1.1.10. One may think that this is related to fail-stop behaviors where $B$ is the set of nodes that stopped responding. In general, however, this is not true as we also remove nodes from quorum slices. One can think of this as the *alternate* universe where nodes from $B$ simply did not even exist from the beginning.

**Theorem 1.1.11.** *Definition 1.1.9 is well-defined. In other words, if $\langle V, Q\rangle$ is an FBAS and $B \subset V$, then $\langle V, Q\rangle^B$ is an FBAS.*

*Proof.* If $V = B$, then we are done because of Remark 1.1.2.

Suppose otherwise. Let $v \in V \setminus B$ be given. By the definition of an FBAS, $Q(v) \neq \emptyset$. Therefore, $Q^B(v) = \{q \setminus B \mid q \in Q(v)\}$ is nonempty.

Let $q' \in Q^B(v)$ be given arbitrarily. Then $q' = q \setminus B$ for some $q \in Q(v)$. Then $v \in q$ by the definition of an FBAS, so $v \in q'$.

Thus $Q^B$ is indeed a quorum function. Therefore, $\langle V, Q\rangle^B$ is an FBAS. □

**Theorem 1.1.12.** *Let $U$ be a quorum in FBAS $\langle V, Q\rangle$, let $B \subset V$ be a set of nodes, and let $U' = U \setminus B$. If $U' \neq \emptyset$, then $U'$ is a quorum in $\langle V, Q\rangle^B$.*

*Proof.* Since $U' \neq \emptyset$, it suffices to show that $\forall v \in U', \exists q \in Q^B(v), q \subset U'$. Let $v \in U'$. Then $v \in U$. Since $U$ is a quorum in $\langle V, Q\rangle$, we can find $q \in Q(v)$ such that $q \subset U$. Then $q' = q \setminus B \in Q^B(v)$, and $q' = q \setminus B \subset U \setminus B = U'$. Therefore, $U'$ is a quorum in $\langle V, Q\rangle^B$. □

*Remark* 1.1.13. One can think of this theorem as "*A quorum in the 'original' universe is a quorum in the 'alternate' universe.*"

**Definition 1.1.14 (Quorum Intersection Despite $B$).** Let $\langle V, Q\rangle$ be an FBAS and $B \subset V$ be a set of nodes. We say $\langle V, Q\rangle$ enjoys quorum intersection despite $B$ if and only if $\langle V, Q\rangle^B$ enjoys quorum intersection.

*Remark* 1.1.15. Quorum intersection despite $B$ is related to the system-level safety when nodes in $B$ act arbitrarily. For instance, suppose $\langle V, Q\rangle$ is an FBAS, $B$ is the set of all ill-behaved nodes, and $\langle V, Q\rangle$ enjoys quorum intersection despite $B$. Suppose two well-behaved nodes $v_1, v_2$ agree with contradictory statements $a_1, a_2$ in quorums $q_1, q_2$, respectively.

Rewrite this!

Then $q_1 \cap q_2 \neq \emptyset$ have well-behaved nodes who agreed with both $a_1$ and $a_2$. This is a contradiction because a well-behaved node cannot contradict itself. This example illustrates how the concept of quorum intersection despite $B$ is related to system-level safety when nodes in $B$ experience Byzantine failures.

**Definition 1.1.16 (Quorum Availability Despite $B$).** Let $\langle V, Q\rangle$ be an FBAS and $B \subset V$ be a set of nodes. We say $\langle V, Q\rangle$ enjoys quorum availability despite $B$ if and only if $V \setminus B$ is a quorum in $\langle V, Q\rangle$ or $B = V$.

**Theorem 1.1.17.** *Let $\langle V, Q\rangle$ be an FBAS and $B \subset V$. $\langle V, Q\rangle$ enjoys quorum availability despite $B$ if and only if $\forall v \in V \setminus B$, there exists a quorum $U_v$ such that $v \in U_v \subset (V \setminus B)$.*

*Proof.* If $V = B$, we are done. Suppose otherwise.

$$\begin{aligned}\forall v \in V \setminus B, \exists \text{a quorum } U_v, v \in U_v \subset (V \setminus B) &\implies \bigcup_{v \in V \setminus B} U_v \text{ is a quorum in } \langle V, Q\rangle \\ &\implies V \setminus B \text{ is a quorum in } \langle V, Q\rangle\end{aligned}$$

by Theorem 1.1.4. On the other hand, if $V \setminus B$ is a quorum in $\langle V, Q\rangle$, then $\forall v \in V \setminus B, \exists$a quorum $U_v, v \in U_v \subset (V \setminus B)$ because we can let $U_v = V \setminus B$ for each $v$. □

*Remark* 1.1.18. Theorem 1.1.17 shows that $\langle V, Q\rangle$ enjoys quorum availability despite $B$ if all nodes in $V \setminus B$ can find a quorum without $B$. This is related to the liveness of the system. If $\langle V, Q\rangle$ enjoys quorum availability despite $B$, then regardless of what happens to nodes in $B$, nodes in $V \setminus B$ can keep going.

**Definition 1.1.19 ($v$-blocking).** Let $\langle V, Q\rangle$ be an FBAS. Let $v \in V$. A subset $B \subset V$ is called $v$-blocking if and only if $\forall q \in Q(v), q \cap B \neq \emptyset$.

*Remark* 1.1.20. Intuitively, if a subset $B \subset V$ is $v$-blocking, then one may think of it as "*$v$ can't really get by without $B$.*" The following theorem can be interpreted as "*If $v$ can't get by without $B$, $v$ can't get by without $C$ for any $C \supset B$.*"

**Theorem 1.1.21.** *Let $\langle V, Q\rangle$ be an FBAS. Let $v \in V$. Then*

- *The union of two $v$-blocking sets is $v$-blocking.*
- *Any superset of a $v$-blocking set is $v$-blocking.*

*Proof.* It suffices to only prove the second statement. If $B \subset B'$ and $B$ is $v$-blocking, $q \cap B' \supset q \cap B \neq \emptyset$ for any $q \in Q(v)$. $\square$

**Theorem 1.1.22.** *Let $\langle V, Q\rangle$ be an FBAS. Let $A \subsetneq V$ and $U_1, U_2$ be a partition of $V \setminus A$. Let $v \in U_1$. If $U_2$ is not $v$-blocking in $\langle V, Q\rangle$, then $U_2$ is not $v$-blocking in $\langle V, Q\rangle^A$.*

*Proof.* Since $U_2$ is not $v$-blocking in $\langle V, Q\rangle$, there exists $q_v \in Q(v)$ such that $q_v \cap U_2 = \emptyset$.

$$\begin{aligned}(q_v \setminus A) \cap U_2 &= (q_v \cap U_2) \setminus (A \cap U_2) \\ &= q_v \cap U_2 = \emptyset.\end{aligned}$$

Thus $U_2$ is not $v$-blocking in $\langle V, Q\rangle^A$. $\square$

**Theorem 1.1.23.** *Let $\langle V, Q\rangle$ be an FBAS. Let $B \subset V$. $\langle V, Q\rangle$ enjoys quorum availability despite $B$ if and only if $B$ is not $v$-blocking for any $v \in V \setminus B$.*

*Proof.*

$$\begin{aligned}\forall v \in V \setminus B, \neg(B \text{ is } v\text{-blocking}) &\iff \forall v \in V \setminus B, \neg(\forall q \in Q(v), q \cap B \neq \emptyset) \\ &\iff \forall v \in V \setminus B, \exists q \in Q(v), q \cap B = \emptyset \\ &\iff \forall v \in V \setminus B, \exists q \in Q(v), q \subset V \setminus B \\ &\iff V = B \text{ or } V \setminus B \text{ is a quorum in } \langle V, Q\rangle \\ &\iff \langle V, Q\rangle \text{ enjoys quorum availability despite } B\end{aligned}$$

$\square$

1.2. **Dispensable Sets.**

**Definition 1.2.1 (Dispensable Set).** Let $\langle V, Q\rangle$ be an FBAS and $B \subset V$ be a set of nodes. $B$ is called a dispensable set, or DSet, if and only if $\langle V, Q\rangle$ enjoys both quorum intersection despite $B$ and quorum availability despite $B$.

We will first show some basic properties of DSets.

**Theorem 1.2.2.** *Let $\langle V, Q\rangle$ be an FBAS. Then*

- *$V$ is a DSet.*
- *If $\forall v \in V, Q(v) = \{V\}$, then $\emptyset$ and $V$ are the only DSets of $\langle V, Q\rangle$.*

*Proof.*

- $\langle V, Q\rangle^V$ enjoys quorum intersection because there is no quorum. $\langle V, Q\rangle$ enjoys quorum availability despite $V$ because $V = V$.
- Suppose $\forall v \in V, Q(v) = \{V\}$. As shown above, $V$ is a DSet of $\langle V, Q\rangle$. The empty set is a DSet because
  - $\langle V, Q\rangle$ enjoys quorum intersection despite $\emptyset$ because the only quorum is $V$.
  - $\langle V, Q\rangle$ enjoys quorum availability despite $B$ because $V \setminus \emptyset = V$ is a quorum.

  Let $\emptyset \subsetneq S \subsetneq V$ be given. Then $V \neq S$ and $V \setminus S$ is not a quorum for it is nonempty and does not contain any quorum slice. Therefore, $\langle V, Q\rangle$ does not enjoy quorum availability despite $B$, so no nonempty, proper subset of $V$ is a DSet.

$\square$

**Definition 1.2.3 (Intact and Befouled).** Let $\langle V, Q\rangle$ be an FBAS and $v \in V$. $v$ is said to be intact if and only if there exists a DSet $B$ containing all ill-behaved nodes and $v \notin B$. $v$ is said to be befouled if and only if $v$ is not intact.

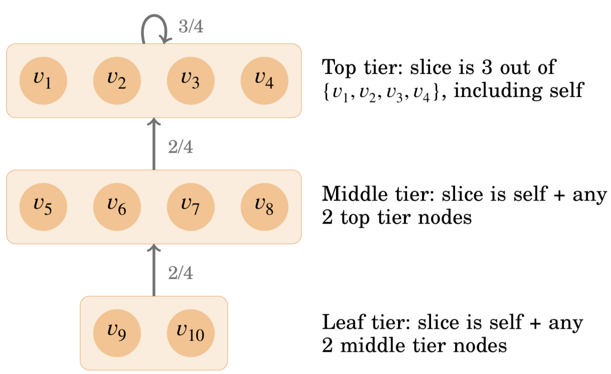


FIGURE 1. Tiered Quroum Example (P.5 of the white paper)

**Example 1.2.4.** We will use Figure 1 as an example.

- The smallest DSet containing $v_5, v_6$ in Figure 1 is $\{v_5, v_6, v_9, v_{10}\}$.
  - First, we will show that $B = \{v_5, v_6\}$ is not a DSet. By definition,

$$Q^B(v_9) = \{\{v_9\}, \{v_9, v_7\}, \{v_9, v_8\}, \{v_9, v_7, v_8\}\}$$
$$Q^B(v_{10}) = \{\{v_{10}\}, \{v_{10}, v_7\}, \{v_{10}, v_8\}, \{v_{10}, v_7, v_8\}\}$$

This implies that $U_9 = \{v_9\}$ and $U_{10} = \{v_{10}\}$ are both quorums. Then $U_9 \cap U_{10} = \emptyset$, so $\langle V, Q\rangle^B$ does not enjoy quorum intersection. Therefore, $B$ is not a DSet.
Next, we will consider $C = \{v_5, v_6, v_1\}$. Then we can use the same argument as above. $U_9 = \{v_9\} \in Q^C(v_9)$ and $U_{10} = \{v_{10}\} \in Q^C(v_{10})$, and the intersection is empty. Therefore, $C$ is not a DSet. It is easy to see that this argument works for the case of $\{v_5, v_6, v_i\}$ for any $i = 1, 2, 3, 4$.
We will consider $D = \{v_5, v_6, v_9\}$. Similarly, $U = \{v_{10}\} \in Q^D(v_{10})$ is a quorum. Moreover, $U' = \{v_1, v_2, v_3, v_4\}$ is a quorum. Then $U \cap U' = \emptyset$, so $\langle V, Q\rangle^D$ does not enjoy quorum intersection. It is easy to see that a similar argument shows that $\{v_5, v_6, v_{10}\}$ is not a DSet.
Finally, we will show that $E = \{v_5, v_6, v_9, v_{10}\}$ is a DSet. $V \setminus E$ is a quorum in $\langle V, Q\rangle$ because every node in $V \setminus E$ has a quorum slice consisting of nodes in $V \setminus E$. If a quorum in $\langle V, Q\rangle^E$ contains $v_7$ or $v_8$, then it must contain some of $v_1, v_2, v_3, v_4$. If a quorum in $\langle V, Q\rangle^E$ contains at least one of $v_1, v_2, v_3$, or $v_4$, then it must contain at least three of $v_1, v_2, v_3, v_4$. Therefore, any intersection of two quorums in $\langle V, Q\rangle^E$ contains at least two of $v_1, v_2, v_3, v_4$ by the pigeon hole principle.
Therefore, $E$ is indeed a smallest DSet containing $v_5$ and $v_6$.
  - We showed that $B = \{v_5, v_6\}$ is not a DSet because $\langle V, Q\rangle$ does not enjoy quorum intersection despite $B$. What this means is that if both $v_5$ and $v_6$ either stop responding or are malicious, then it is not possible to guarantee safety for $v_9$ and $v_{10}$. For instance, consider the following situation:
    * Both $v_5$ and $v_6$ tell $v_9$ and $v_{10}$ that $Q(v_5) = Q(v_6) = \{\{v_5, v_6\}\}$ convincing that $\{v_5, v_6, v_9\}$ and $\{v_5, v_6, v_{10}\}$ are both quorums.
    * Both $v_5$ and $v_6$ tell $v_9$ that they want to process a certain transaction. This transaction does not contradict what $v_9$ knows about $v_5$. Moreover, everyone in the quorum $\{v_5, v_6, v_9\}$ is in favor of this transaction. Thus there is no reason for $v_9$ to not believe this transaction.
    * Both $v_5$ and $v_6$ tell $v_{10}$ that they want to process a certain transaction that contradicts the transaction they told $v_5$ about. For the same reason, there is no reason for $v_{10}$ to not believe this transaction.
    * Then the network processes contradicting transactions. This can let $v_5$ double-spend some money, for instance.
    * One can verify that this is possible by looking into the definition of accepting, confirming and such that are introduced in later chapters.
- $B = \{v_1\}$ is a DSet.
  - First, we will check if $\langle V, Q\rangle$ enjoys quorum intersection despite $B$.
  Consider $\langle V, Q\rangle^B$. Any quorum containing $v_9$ and/or $v_{10}$ must contain at least two of $v_5, v_6, v_7, v_8$. Any quorum containing at least one of $v_5, \cdots, v_8$ must contain at least one of $v_2, v_3, v_4$. Any quorum containing at least one of $v_2, v_3, v_4$ must contain at least two of $v_2, v_3, v_4$. This is because $Q(v_i)^B = \{\{v_2, v_3, v_4\}, \{v_i, v_j\}, \{v_i, v_k\}\}$ where $\{i, j, k\} = \{2, 3, 4\}$.
  Therefore, the intersection of any two quorums must contain at least one of $v_2, v_3, v_4$ by the pigeon hole principle.

Next, we need to check if $\langle V, Q\rangle$ enjoys quorum availability despite $B$. $V \setminus B$ is indeed a quorum in $\langle V, Q\rangle$ because each node in $V \setminus B$ has a quorum slice that does not contain $v_1$.

– We showed that $B$ is indeed a DSet. What this means is that even if $v_1$ stops responding or becomes malicious, the rest of the network can make progress safely. For instance, suppose that $v_1$ becomes malicious and tries to double-spend money. $v_1$ might tell $v_5$ that it wants to process a certain transaction. Similarly, $v_1$ might tell $v_6$ that it wants to process a contradicting transaction. However, every quorum slice of $v_5$ and $v_6$ contains at least one tier-1 node that is not $v_1$. Suppose that $v_5$ asks $v_2$ what it thinks, and $v_6$ asks $v_3$ what it thinks. Then every quorum slice of $v_2$ and $v_3$ contains 3 tier-1 nodes. By the pigeon hole principle, at least one tier-1 node that is not $v_1$ gets asked what it thinks about the contradicting transactions from $v_5$. The tier-1 node does not agree with them and $v_1$'s attempt to double-spend money fails.

**Theorem 1.2.5.** *If $B_1$ and $B_2$ are DSets in an FBAS $\langle V, Q\rangle$ enjoying quorum intersection, then $B = B_1 \cap B_2$ is a DSet, too.*

*Proof.* If $B_1 = V$ or $B_2 = V$, then we are done. Suppose otherwise.

First, we will show that $\langle V, Q\rangle$ enjoys quorum availability despite $B$. By Definition 1.1.16, it suffices to show that $V = B$ or $V \setminus B$ is a quorum in $\langle V, Q\rangle$. Since we assumed that $B_1 \neq V$ and $B_2 \neq V$, $B \neq V$. Therefore, we will show that $V \setminus B$ is a quorum in $\langle V, Q\rangle$. By basic set theory, $V \setminus B = V \setminus (B_1 \cap B_2) = (V \setminus B_1) \cup (V \setminus B_2)$. Since $B_1$ is a DSet, $V = B_1$ or $V \setminus B_1$ is a quorum in $\langle V, Q\rangle$. Since we assumed that $V \neq B_1$ earlier, $V \setminus B_1$ is a quorum in $\langle V, Q\rangle$. Similarly, $V \setminus B_2$ is a quorum in $\langle V, Q\rangle$. By Theorem 1.1.4, the union $(V \setminus B_1) \cup (V \setminus B_2) = V \setminus B$ is a quorum in $\langle V, Q\rangle$.

Next, we will show that $\langle V, Q\rangle$ enjoys quorum intersection despite $B$. Let $U_a, U_b$ be quorums in $\langle V, Q\rangle^B$. We want to show that $U_a \cap U_b \neq \emptyset$. We will do so by proving a stronger statement, which is $(U_a \cap U_b) \setminus B_1 \neq \emptyset$. In other words, we will show that $(U_a \setminus B_1) \cap (U_b \setminus B_1) \neq \emptyset$.

Since $B_1$ is a DSet, $\langle V, Q\rangle$ enjoys quorum intersection despite $B_1$. In other words, $\langle V, Q\rangle^{B_1}$ enjoys quorum intersection. Therefore, it suffices to show that $U_a \setminus B_1$ and $U_b \setminus B_1$ are both quorums in $\langle V, Q\rangle^{B_1}$. By Theorem 1.1.12, $U_a \setminus B_1$ and $U_b \setminus B_1$ are quorums in $(\langle V, Q\rangle^B)^{B_1}$ if $U_a \setminus B_1 \neq \emptyset$ and $U_b \setminus B_1 \neq \emptyset$. Since $(\langle V, Q\rangle^B)^{B_1} = \langle V, Q\rangle^{B_1}$, it suffices to show that $U_a \setminus B_1 \neq \emptyset$ and $U_b \setminus B_1 \neq \emptyset$.

We will first show that $U_a \setminus B_1 \neq \emptyset$. By basic set theory,

$$\begin{aligned} U_a &= U_a \setminus B \\ &= U_a \setminus (B_1 \cap B_2) \\ &= (U_a \setminus B_1) \cup (U_a \setminus B_2) \end{aligned}$$

because $U_a \cap B = \emptyset$.

This implies that $(U_a \setminus B_1) \cup (U_a \setminus B_2) \neq \emptyset$. If $U_a \setminus B_1$ is nonempty, we are done. Suppose $U_a \setminus B_2$ is nonempty. We will show that this implies that $U_a \setminus B_1 \neq \emptyset$. We will do so by first finding two quorums in $\langle V, Q\rangle^{B_2}$ whose intersection is a subset of $U_a \setminus B_1$. Since $\langle V, Q\rangle^{B_2}$ enjoys quorum intersection, the intersection of such two quorums must be nonempty, which in turn shows that $U_a \setminus B_1$ is nonempty.

- We claim that $U_a \setminus B_2$ is a quorum in $\langle V, Q\rangle^{B_2}$. $U_a$ is a quorum in $\langle V, Q\rangle^{B}$. Since $U_a \setminus B_2$ is assumed to be nonempty, $U_a \setminus B_2$ is a quorum in $(\langle V, Q\rangle^{B})^{B_2}$ by Theorem 1.1.12. Since $(\langle V, Q\rangle^{B})^{B_2} = \langle V, Q\rangle^{B_2}$, $U_a \setminus B_2$ is a quorum in $\langle V, Q\rangle^{B_2}$.
- $V \setminus B_2 \neq \emptyset$ is a quorum in $\langle V, Q\rangle$ because $\langle V, Q\rangle$ must enjoy quorum availability despite $B_2$ and $B_2 \neq V$. Similarly, $V \setminus B_1 \neq \emptyset$ is a quorum in $\langle V, Q\rangle$. Because $\langle V, Q\rangle$ enjoys quorum intersection, $(V \setminus B_1) \cap (V \setminus B_2) \neq \emptyset$. In other words, $(V \setminus B_1) \setminus B_2 \neq \emptyset$. By applying Theorem 1.1.12 to the fact that $V \setminus B_1$ is a quorum in $\langle V, Q\rangle$ and $(V \setminus B_1) \setminus B_2 \neq \emptyset$, we can conclude that $(V \setminus B_1) \setminus B_2$ is a quorum in $\langle V, Q\rangle^{B_2}$.

Since $\langle V, Q\rangle^{B_2}$ enjoys quorum intersection, $(U_a \setminus B_2) \cap ((V \setminus B_1) \setminus B_2) \neq \emptyset$.

$$\begin{aligned}
\emptyset &\neq (U_a \setminus B_2) \cap ((V \setminus B_1) \setminus B_2) \\
&= (U_a \cap (V \setminus B_1)) \setminus B_2 \\
&\subset U_a \cap (V \setminus B_1) \\
&= U_a \setminus B_1.
\end{aligned}$$

Thus, $U_a \setminus B_1 \neq \emptyset$.

The same argument will show that $U_b \setminus B_1 \neq \emptyset$. □

*Remark* 1.2.6. Theorem 1.2.5 states that the intersection of two DSets is a DSet if the FBAS enjoys quorum intersection. One might wonder if the union of two DSets is a DSet when the FBAS enjoys quorum intersection. However, this is not true in general. Consider the FBAS $\langle V, Q\rangle$ where $V = \{v_1, v_2, v_3, v_4\}$ and $Q(v_i) = \{U \subset V \mid v_i \in U, |U| = 3\}$. This FBAS enjoys quorum intersection by the pigeon-hole principle because each quorum contains at least 3 elements. Then $B = \{v_1\}$ is a DSet because

- Quorum intersection despite $B$
  - Every quorum slice in $\langle V, Q\rangle^{B}$ contains at least 2 nodes because every quorum slice in $\langle V, Q\rangle$ contains exactly 3 nodes. This implies that any quorum in $\langle V, Q\rangle^{B}$ must contain at least 2 nodes. By the pigeon-hole principle, every pair of quorums in $\langle V, Q\rangle^{B}$ must intersect.
- Quorum availability despite $B$
  - $V \setminus B = \{v_2, v_3, v_4\}$ is a quorum in $\langle V, Q\rangle$ because $\{v_2, v_3, v_4\} \in Q(v_i)$ for each $i = 2, 3, 4$.

Similarly, $C = \{v_2\}$ is a DSet. However, $B \cup C = \{v_1, v_2\}$ is not a DSet because $B \cup C \neq V$ and $V \setminus (B \cup C) = \{v_3, v_4\}$ is not a quorum in $\langle V, Q\rangle$.

**Theorem 1.2.7.** *In an FBAS with quorum intersection, the set of befouled nodes is a DSet.*

*Proof.* Let $\langle V, Q\rangle$ be an FBAS with quorum intersection. Let $B$ be the intersection of all DSets that contain all ill-behaved nodes. We will show that $B$ is the set of befouled nodes by showing that $V \setminus B$ is the set of intact nodes.

$$\begin{aligned}
v \in V \setminus B &\iff v \notin B \\
&\iff \exists \text{ DSet } B_v \text{ that contains all ill-behaved nodes and } v \notin B_v \\
&\iff v \text{ is intact}
\end{aligned}$$

Therefore, $V \setminus B$ is precisely the set of intact nodes, and thus $B$ is the set of befouled nodes.

By applying Theorem 1.2.5 repeatedly, we can conclude that $B$ is a DSet. $\square$

**Theorem 1.2.8.** *Let $\langle V, Q\rangle$ be an FBAS and let $B \subset V$ be the set of befouled nodes. If $B$ is a DSet, $B$ is not $v$-blocking for any intact $v$.*

*Proof.* By Definition 1.2.3, a node $v \in V$ is intact if and only if $v \notin B$. By Theorem 1.1.23, $\langle V, Q\rangle$ enjoys quorum availability despite $B$ if and only if $B$ is not $v$-blocking for any $v \in V \setminus B$. Since $B$ is a DSet, $\langle V, Q\rangle$ enjoys quorum availability despite $B$. Thus $B$ is not $v$-blocking for any intact $v$. $\square$

### 1.3. **Voting, Accepting, and Ratifying.**

**Definition 1.3.1 (Vote).** A node $v$ votes for a statement $a$ if and only if $v$ asserts

- $a$ is valid,
- $a$ is consistent with all statements $v$ has accepted,
- $v$ has never voted against $a$,
- $v$ promises never to vote for a statement that contradicts $a$ in the future.

**Definition 1.3.2 (Vote Against $a$).** When a node $v$ votes for a statement that contradicts $a$, we say $v$ votes against $a$.

**Definition 1.3.3 (Accept).** Let $\langle V, Q\rangle$ be an FBAS, and let $v \in V$. $v$ accepts a statement $a$ if and only if

- It has never accepted a statement contradicting $a$, and
- It determines that either
  - There exists a quorum $U$ such that $v \in U$ and each member of $U$ either voted for $a$ or broadcast that it has accepted $a$, or
  - There exists a $v$-blocking set $B$ such that every member of $B$ broadcast that it has accepted $a$.

When $v$ accepts $a$, it must vote for the statement "an intact node accepted $a$." For simplicity, we will often write "$accept(a)$" to mean "an intact node accepted $a$."

As you can see, the definitions of voting and accepting have a circular dependency. Note that it is possible for a node to accept a statement after voting for a contradictory statement.

**Definition 1.3.4 (Ratify).** A quorum $U_a$ ratifies a statement $a$ if and only if every member of $U_a$ votes for $a$. A node $v$ ratifies $a$ if and only if $v$ is a member of a quorum $U_a$ that ratifies $a$.

**Theorem 1.3.5.** *Let $\langle V, Q\rangle$ be an FBAS. If a node $v \in V$ ratifies a statement $a$, then it must accept $a$.*

*Proof.* If a node $v$ ratifies $a$, then it is a member of a quorum $U \subset V$ that ratifies $a$. Thus every member of $U$ votes for $a$. This implies that $v$ also votes for $a$. By Definition 1.3.1, $v$ has never accepted a statement contradicting $a$. By Definition 1.3.3, $v$ accepts $a$. $\square$

*Remark* 1.3.6. Theorem 1.3.5 shows that ratifying is a stronger condition than accepting.

**Theorem 1.3.7.** *If an FBAS enjoys quorum intersection and contains no ill-behaved node, then two contradictory statements cannot be both ratified.*

*Proof.* Suppose the statement is false and let $a, \bar{a}$ denote two contradictory statements ratified in such an FBAS. Let $U_a, U_{\bar{a}}$ denote quorums ratifying such statements, respectively. By the definition of quorum intersection, $U_a \cap U_{\bar{a}} \neq \emptyset$. Let $v \in U_a \cap U_{\bar{a}}$. This implies that $v$ voted for both $a$ and $\bar{a}$. However, the definition of voting(Definition 1.3.1) explicitly prohibits that. In other words, $v$ must be ill-behaved, which is a contradiction to our assumption. $\square$

**Theorem 1.3.8.** *Let $\langle V, Q\rangle$ be an FBAS and $B \subset V$. Suppose that $B$ contains all the ill-behaved nodes and $\langle V, Q\rangle^B$ enjoys quorum intersection. Let $v_1 \neq v_2 \in V \setminus B$. If $v_1$ ratifies a statement $a$, then $v_2$ cannot ratify any statement that contradicts $a$.*

*Proof.* Suppose that the theorem is false and let $U_1, U_2$ be quorums of $v_1, v_2$ that ratify $a, \bar{a}$, respectively, where $a$ and $\bar{a}$ are contradictory. Since $v_1 \in U_1 \setminus B$, $U_1 \setminus B \neq \emptyset$. By Theorem 1.1.12, $U_1' = U_1 \setminus B$ is a quorum in $\langle V, Q\rangle^B$. Similarly, $U_2' = U_2 \setminus B$ is a quorum in $\langle V, Q\rangle^B$. Since $\langle V, Q\rangle^B$ enjoys quorum intersection, $U_1' \cap U_2' \neq \emptyset$. Choose $v \in U_1' \cap U_2'$ arbitrarily. Then $v \in U_1 \cap U_2$. In order for $U_1, U_2$ to ratify $a, \bar{a}$, respectively, $v$ must vote for both $a$ and $\bar{a}$. However, this is against the definition of voting. $v$ must be an ill-behaved node, so $v \in B$, which is a contradiction because $v \in U_1' \cap U_2' \subset U_1' = U_1 \setminus B$ and $B$ contains all the ill-behaved nodes. □

**Theorem 1.3.9.** *Let $\langle V, Q\rangle$ be an FBAS with quorum intersection. Then two intact nodes in $V$ cannot ratify contradictory statements.*

*Proof.* Let $v \neq v'$ be two intact nodes in $V$. Let $B \subset V$ be the set of befouled nodes. Then $v \notin B$ and $v' \notin B$. Since $\langle V, Q\rangle$ is an FBAS with quorum intersection, $B$ is a DSet by Theorem 1.2.7. By the definition of a DSet (Definition 1.2.1), $\langle V, Q\rangle^B$ enjoys quorum intersection. By Theorem 1.3.8, $v, v'$ cannot ratify contradictory statements. □

**Lemma 1.3.10.** *Let $\langle V, Q\rangle$ be an FBAS enjoying quorum intersection and $B$ be the set of befouled nodes. If $a$ is accepted by an intact node in $V$, then $a$ is ratified by some intact node in $\langle V, Q\rangle^B$.*

*Proof.* Suppose that $a$ is accepted by one or more intact nodes in $V$. Since $V$ is finite, there has to be an intact node $v$ such that no intact nodes in $V$ accepted $a$ before $v$.

By the definition of accepting(Definition 1.3.3), $v$ accepted $a$ because either

- There was a quorum $U$ of $v$ such that every element of $U$ either voted for $a$ or broadcast that it has accepted $a$, or
- There existed a $v$-blocking set such that every element in it broadcast that it has accepted $a$.

We claim that it could not have been the second one. On the contrary, suppose that it was the second one. Since no intact nodes in $V$ accepted $a$ before $v$, such a $v$-blocking set must have only had befouled nodes. Therefore, such a $v$-blocking set must be a subset of $B$. Since $\langle V, Q\rangle$ enjoys quorum intersection, $B$ is a DSet by Theorem 1.2.7. By Theorem 1.2.8, $B$ is not $v$-blocking. By taking the contrapositive of Theorem 1.1.21, we conclude that no subset of $B$ is $v$-blocking.

Therefore, it must have been the first case. In other words, there must have existed a quorum $U$ of $v$ such that, before $v$ accepted $a$, every member of $U$ either voted for $a$ or broadcast that it has accepted $a$. Since no intact node accepted $a$ before $v$, every intact node in $U$ must have voted for $a$ before $v$ accepted $a$. In other words, every node in $U \setminus B$ voted for $a$. By Theorem 1.1.12, $U \setminus B$ is a quorum in $\langle V, Q\rangle^B$. Thus $U \setminus B$ ratified $a$ in $\langle V, Q\rangle^B$, and thus $v$ ratified $a$ in $\langle V, Q\rangle^B$. Finally, $v$ is indeed an intact node in $\langle V, Q\rangle^B$ because $\langle V, Q\rangle^B$ contains no ill-behaved nodes.

In conclusion, $v$ is an intact node in $\langle V, Q\rangle^B$ and $v$ ratified $a$ in $\langle V, Q\rangle^B$. □

**Theorem 1.3.11.** *Two intact nodes in an FBAS $\langle V, Q\rangle$ enjoying quorum intersection cannot accept contradictory statements.*

By Theorem 1.3.5, ratifying is a stronger condition than accepting. Therefore, Theorem 1.3.11 is a stronger version of Theorem 1.3.9.

*Proof.* Suppose otherwise. Let $a, \bar{a}$ be contradictory statements accepted by two intact nodes in $\langle V, Q \rangle$. Let $B$ denote the set of befouled nodes. By Lemma 1.3.10, $a, \bar{a}$ are ratified by some intact nodes in $\langle V, Q \rangle^B$. By the definition of a DSet(Definition 1.2.1), $\langle V, Q \rangle$ enjoys quorum intersection despite $B$.

This means that $\langle V, Q \rangle^B$ enjoys quorum intersection and two contradictory statements are ratified by some intact nodes in $\langle V, Q \rangle^B$. However, this is a direct contradiction to Theorem 1.3.9. Hence, two contradictory statements cannot be accepted by two intact nodes in $\langle V, Q \rangle$. $\square$

1.4. **Confirmation.**

**Definition 1.4.1 (Irrefutable).** A statement $a$ is irrefutable in an FBAS if no intact node can ever vote against it.

**Definition 1.4.2 (Confirm).** A quorum $U_a$ in an FBAS confirms a statement $a$ if and only if every element in $U_a$ broadcasts that it has accepted $a$. A node confirms $a$ if and only if it is in such a quorum.

**Theorem 1.4.3.** *Ratifying is stronger than confirming, and confirming is stronger than accepting.*

*Proof.* Let $\langle V, Q\rangle$ and $v \in V$ be given. Suppose that $v$ ratifies a statement $a$. Then there exists a quorum $U$ such that $v \in U$ and every member in $U$ votes for $a$. For any $u \in U$,

- $u$ has never accepted a statement contradicting $a$ by the definition of voting (Definition 1.3.1), and
- $U$ is a quorum such that $u \in U$ and every memeber of $U$ voted for $a$.

Therefore, $u$ accepts $a$. In other words, every member of $U$ accepts $a$. $U$ confirms $a$ and thus $v$ confirms $a$. Thus ratifying is stronger than confirming.

The definition of confirming(Definition 1.4.2) shows that a node must first accept a statement before confirming. Therefore, confirming is stronger than accepting. □

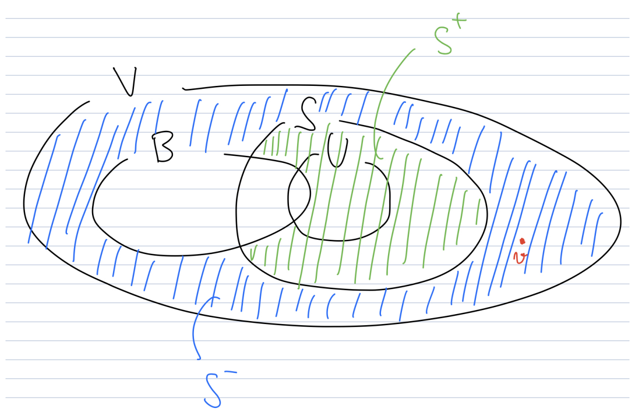


Figure 2. Lemma 1.4.4

**Lemma 1.4.4.** *Let $\langle V, Q\rangle$ be an FBAS with quorum intersection. Let $B$ denote the set of befouled nodes. Let $U$ be a quorum containing an intact node, and let $S$ be a set containing $U$. Let $S^+$ be the set of intact nodes in $S$, and let $S^-$ be the set of intact nodes not in $S$. Either $S^- = \emptyset$, or $\exists v \in S^-$ such that $S^+$ is $v$-blocking. (See Figure 2.)*

*Proof.* Note that $S^+ = S \setminus B$ and $S^- = (V \setminus S) \setminus B = (V \setminus B) \setminus S^+$. If $\exists v \in S^-$ such that $S^+$ is $v$-blocking, then we are done.

Suppose that $\forall v \in S^-$, $S^+$ is not $v$-blocking in $\langle V, Q\rangle$. We want to show that $S^- = \emptyset$.

- $S^+$ and $S^-$ form a partition of $V \setminus B$,
- $S^+$ is not $v$-blocking in $\langle V, Q\rangle$ for any arbitrary $v \in S^-$,

By Theorem 1.1.22, $S^+$ is not $v$-blocking in $\langle V, Q\rangle^B$ for any $v \in S^-$. Since $S^- = (V \setminus B) \setminus S^+$, $S^+$ is not $v$-blocking in $\langle V, Q\rangle^B$ for any $v \in (V \setminus B) \setminus S^+$. By applying Theorem 1.1.23 to the FBAS $\langle V, Q\rangle^B$ and subset $S^+$, $\langle V, Q\rangle^B$ enjoys quorum availability despite $S^+$.

By the definition of quorum availability(Definition 1.1.16), $(V \setminus B) \setminus S^+$ is a quorum in $\langle V, Q\rangle^B$, or $V \setminus B = S^+$. Suppose $(V \setminus B) \setminus S^+$ is a quorum in $\langle V, Q\rangle^B$. This leads to two contradictory claims:

- Claim 1: $\langle V, Q\rangle$ enjoys quorum intersection despite $B$.
  - Since $\langle V, Q\rangle$ enjoys quorum intersection, $B$ is a DSet by Theorem 1.2.7. By the definition of a DSet(Definition 1.2.1), $\langle V, Q\rangle^B$ enjoys quorum intersection.
- Claim 2: $\langle V, Q\rangle$ does not enjoy quorum intersection despite $B$.
  - $U \setminus B$ is nonempty since $U$ contains an intact node. Thus $U \setminus B$ is a quorum in $\langle V, Q\rangle^B$ by Theorem 1.1.12. We also assumed that $(V \setminus B) \setminus S^+$ is a quorum in $\langle V, Q\rangle^B$.

$$\begin{aligned}(U \setminus B) \cap ((V \setminus B) \setminus S^+) &= (U \setminus B) \cap S^- \\ &\subset (S \setminus B) \cap S^- \\ &\subset S^+ \cap S^- \\ &= \emptyset.\end{aligned}$$

    Therefore, $\langle V, Q\rangle^B$ does not enjoy quorum intersection.

Therefore, $(V \setminus B) \setminus S^+$ must not be a quorum in $\langle V, Q\rangle^B$, so $V \setminus B$ must be $S^+$. In other words, $S^+$ contains all the intact nodes, so $S^- = \emptyset$, which is exactly what we wanted to show. $\square$

**Theorem 1.4.5.** *If an intact node in an FBAS $\langle V, Q\rangle$ with quorum intersection confirms a statement $a$, then every intact node will accept and confirm $a$ once sufficient messages are delivered.*

*Proof.* Let $B$ denote the set of befouled nodes. When an intact node confirms $a$, some quorum containing such an intact node confirms $a$. In other words, there exists a quorum $U \not\subset B$ such that every node in $U$ broadcast that it accepted $a$. Some nodes may decide to accept $a$ upon hearing that nodes in $U$ broadcast that it accepted $a$. This may, in turn, make more nodes accept $a$. Thus we may experience a gradual increase in the number of nodes that accept $a$ over time. Since $V$ only contains finitely many nodes, there will be a point at which the number of nodes that accept $a$ stops increasing. Let $S$ be the set of nodes that accept $a$ at that point. We claim that $S$ contains all intact nodes.

- $U$ is a quorum containing an intact node.
- $U \subset S \subset V$ because every node in $U$ accepted $a$ in the beginning.
- Let $S^+ = S \setminus B$ be the set of intact nodes in $S$, and let $S^- = (V \setminus S) \setminus B$ be the set of intact nodes not in $S$.

By Lemma 1.4.4, $S^-$ is empty, or $S^+$ is $v$-blocking for some $v \in S^-$. Suppose $S^-$ is nonempty. Then $v$ accepts $a$ because $S^+$ is $v$-blocking and every element of $S^+$ broadcast that it has accepted $a$. This is a contradiction because we assumed that the number of nodes that accept $a$ stopped increasing. Therefore, $S^-$ must be empty. If $S^-$ is empty, then that implies that every intact node accepted and confirmed $a$ assuming sufficient messages are delivered because

- Since $S^-$ is empty, $S^+$ contains all intact nodes in $V$. $S^+ \subset S$, so $S$ contains all intact nodes. Since every node in $S$ accepted $a$, every intact node accepted $a$.
- Since $\langle V, Q \rangle$ enjoys quorum intersection, $B$ is a DSet by Theorem 1.2.7. By the definition of a DSet, $V \setminus B$ is a quorum. In other words, the set of all intact nodes is a quorum.
- Since $V \setminus B$ is a quorum in which every node accepted $a$, every intact node confirmed $a$.

$\square$

## 2. Stellar Consensus Protocol

2.1. **Nomination Protocol.** Nomination is done through voting, accepting, and confirming a special type of statement in the form of *nominate* $x$.

**Definition 2.1.1 (Nominate).** A node $v$ is said to nominate a value $x$ if and only if it votes for the statement *nominate* $x$.

**Definition 2.1.2 (Candidate).** A node $v$ considers a value $x$ to be a candidate if and only if $v$ has confirmed the statement *nominate* $x$. Alternatively, we say that a node $v$ has a candidate value $x$.

**Definition 2.1.3 (Weight, Neighbors, and Priority).** Let $H$ be a cryptographic hash function whose range can be interpreted as a set of integers $\{0, \cdots, h_{\max} - 1\}$. Let $G_i(m) = H(i, x_{i-1}, m)$ be a slot-specific hash function for slot $i$, where $x_{i-1}$ is the value chosen for the slot preceding $i$. Let $N, P$ are arbitrary constants. Given a slot $i$, a round number $n$ and node $v$, we define

$$\begin{aligned}\text{weight}(v, v') &= \frac{|\{q \in Q(v) \mid v' \in q\}|}{|Q(v)|}\\ \text{neighbors}(v, n) &= \{v' \mid G_i(N, n, v') < h_{\max} \cdot \text{weight}(v, v')\}\\ \text{priority}(n, v') &= G_i(P, n, v')\end{aligned}$$

*Remark* 2.1.4. In Stellar Core, $N$ and $P$ are always 1 and 2.

**Example 2.1.5 (Weight, Neighbors, and Priority(Part 1)).**

proofread!

We will calculate the weight, neighbors, and priority for $v_5$ in Figure 1 as an example. Since each quorum slice consists of $v_5$ along with two nodes from $\{v_1, v_2, v_3, v_4\}$ as in

$$Q(v_5) = \{\{v_1, v_2, v_5\}, \{v_1, v_3, v_5\}, \{v_1, v_4, v_5\}, \cdots, \{v_3, v_4, v_5\}\},$$

$Q(v_5)$ has $\binom{4}{2} = 6$ slices.

We will first calculate the weight of $v_1$.

$$\begin{aligned}\text{weight}(v_5, v_1) &= \frac{|\{q \in Q(v_5) \mid v_1 \in q\}|}{|Q(v_5)|}\\ &= \frac{|\{v_1, v_2, v_5\}, \{v_1, v_3, v_5\}, \{v_1, v_4, v_5\}|}{6}\\ &= \frac{3}{6} = \frac{1}{2}.\end{aligned}$$

By symmetry, $\text{weight}(v_5, v_i) = \frac{1}{2}$ for each $i = 1, 2, 3, 4$. $\text{weight}(v_5, v_5) = 1$ because every quorum slice in $Q(v_5)$ contains $v_5$. Finally, $\text{weight}(v_5, v_i) = 0$ for all $i = 6, 7, 8, 9, 10$ because no quorum slice in $Q(v_5)$ contains any of $v_6, v_7, \cdots, v_{10}$. Therefore, we obtain the following table:

| $v_i$ | $\text{weight}(v_5, v_i)$ |
|---|---|
| $i = 1, 2, 3, 4$ | $1/2$ |
| $i = 5$ | $1$ |
| $i = 6, 7, 8, 9, 10$ | $0$ |

For this example, we will suppose that $h_{max} = 100$. Let $N, P, i, n$ be fixed. Then we will calculate the neighbors. First, we will start with $v_1, v_2, v_3, v_4$.

Suppose

$$G_i(N, n, v_1) = 41$$
$$G_i(N, n, v_2) = 72$$
$$G_i(N, n, v_3) = 19$$
$$G_i(N, n, v_4) = 84.$$

The condition for a node $v'$ to be in $\text{neighbors}(v_5, n)$ is $G_i(N, n, v') < 100 \cdot \text{weight}(v_5, v')$. Therefore, $v_1, v_3 \in \text{neighbors}(v_5, n)$. (e.g., $G_i(N, n, v_1) = 41 < 50 = 100 \cdot 1/2 = 100 \cdot \text{weight}(v_5, v_1)$.)

Moreover, $v_5 \in \text{neighbors}(v_5, n)$ since $\text{weight}(v_5, v_5) = 1$. Finally, $v_i \in \text{neighbors}(v_5, n)$ for each $i = 6, 7, \cdots, 10$ because $\text{weight}(v_5, v_i) = 0$.

Therefore, we have

$$\text{neighbors}(v_5, n) = \{v_1, v_3, v_5\}.$$

This is a reasonable choice of neighbors because

- $v_5$ trusts $v_1, \cdots, v_4$, so it is a good thing that we have $v_1, v_3$ in $\text{neighbors}(v_5, n)$.
- $v_5$ trusts $v_5$.
- Since $v_5$ does not trust $v_6, \cdots, v_{10}$, $v_5$ has no quorum slice containing any of them. Thus it is a good thing that $\text{neighbors}(v_5, n)$ does not contain any of them.

Finally, suppose

$$\text{priority}(n, v_1) = G_i(P, n, v_1) = 17$$
$$\text{priority}(n, v_3) = G_i(P, n, v_3) = 86$$
$$\text{priority}(n, v_5) = G_i(P, n, v_5) = 25.$$

Then $v_5$ will simply nominate the same value as $v_3$.

*Remark* 2.1.6.

- weight is not symmetric in general. In other words, $\text{weight}(v_i, v_j) \neq \text{weight}(v_j, v_i)$ in general.
- $\text{neighbors}(v_i)$ is a set of nodes calculated locally at each $v_i$. In general, $\text{neighbors}(v_i) \neq \text{neighbors}(v_j)$ for any $i \neq j$.
- $\text{priority}(n, v)$ is *global* in a sense that the values of $\text{priority}(n, v)$ calculated at node $w$ and $w'$ must be identical for it only depends on $n$, the hash function $G_i$ and the constant $P$.

**Example 2.1.7 (Weight, Neighbors, and Priority(Part 2)).** Suppose that $\text{priority}(n, v_i) = G_i(P, n, v_i)$ for each $i$ is as follows:

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\text{priority}(n, v_i)$ | 26 | 3 | 60 | 89 | 18 | 56 | 35 | 19 | 61 | 27 |

Moreover, suppose that each node's neighbors is as follows:

| $i$ | neighbors($v_i$) |
|---|---|
| 1 | $\{v_1, v_3\}$ |
| 2 | $\{v_1, v_4\}$ |
| 3 | $\{v_2, v_3, v_4\}$ |
| 4 | $\{v_1, v_2, v_4\}$ |
| 5 | $\{v_2, v_5\}$ |
| 6 | $\{v_1, v_3, v_6\}$ |
| 7 | $\{v_1, v_2, v_3, v_7\}$ |
| 8 | $\{v_3, v_8\}$ |
| 9 | $\{v_6, v_7, v_8, v_9\}$ |
| 10 | $\{v_{10}\}$ |

Then each node's leader (the node whose nominations it will renominate) will be as follows:

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $v_i$'s leader | $v_3$ | $v_4$ | $v_4$ | $v_4$ | $v_5$ | $v_3$ | $v_3$ | $v_3$ | $v_9$ | $v_{10}$ |

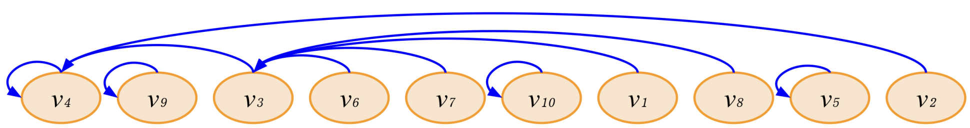


FIGURE 3. Leader Relation Graph

As you can see, this is a directed graph such that the only cycles are self-loops. In this particular case, $v_4, v_9, v_{10}, v_5$ will produce new values, and other nodes will simply renominate those values.

### 2.2. **Ballot Protocol.**