STELLAR CONSENSUS PROTOCOL

HIDENORI SHINOHARA

Abstract. This is my personal notes on the Stellar consensus protocol. This roughly follows the structure of the white paper on https://www.stellar.org/.

Contents

1. Prerequisites

Theorem 1.1. *Let $f \in \mathbb{N}$ be given. Consider a system with $2f+1$ nodes such that any $f+1$ of them constitute a quorum. Then f is the maximum number of fail-stop failures that the system can survive while*

- *maintaining safety (i.e., no two well-behaved nodes will agree on contradictory statements)*
- *maintaining liveness (i.e., all well-behaved nodes can agree on any valid statements)*

Proof. Let b be the number of fail-stop failures and assume $b \leq f$. Then there are $2f+1-b \geq f+1$ well-behaved nodes. Thus each well-behaved node can find a quorum it belongs to that only consists of well-behaved nodes because there are at least $f+1$ well-behaved nodes. This shows the liveness of the system.

Let v_1, v_2 be two well-behaved nodes and suppose they agreed on contradictory statements a_1, a_2, respectively. Let Q_1, Q_2 be the quorums that convinced v_1, v_2 on a_1, a_2, respectively. By the pigeonhole principle, $|Q_1 \cap Q_2| \geq 1$. In other words, there exists a node that agreed on both a_1 and a_2. This is a contradiction because we assumed that nodes are either well-behaved or fail-stop. Therefore, two well-behaved nodes cannot agree on contradictory statements. □

Theorem 1.2. *Let $f \in \mathbb{N}$ be given. Consider a system with $3f+1$ nodes such that any $2f+1$ of them constitute a quorum. Then f is the maximum number of Byzantine failures that the system can survive while*

- *maintaining safety (i.e., no two well-behaved nodes will agree on contradictory statements)*
- *maintaining liveness (i.e., all well-behaved nodes can agree on any valid statements)*

Proof. Let b be the number of Byzantine failures and assume $b \leq f$.

Then there are $3f + 1 - b \geq 2f + 1$ well-behaved nodes. Thus each well-behaved node can find a quorum it belongs to that only consists of well-behaved nodes because there are at least $2f + 1$ well-behaved nodes. This shows the liveness of the system.

Let v_1, v_2 be two well-behaved nodes and suppose they agreed on contradictory statements a_1, a_2, respectively. Let Q_1, Q_2 be the quorums that convinced v_1, v_2 on a_1, a_2, respectively. By the pigeonhole principle, $|Q_1 \cap Q_2| \geq f + 1$. In other words, at least $f + 1$ nodes agreed on both a_1 and a_2. This is a contradiction because we assumed that there are at most $b \leq f$ Byzantine failures. Therefore, two well-behaved nodes cannot agree on contradictory statements.

We have shown that the system can survive while maintaining safety and liveness with b Byzantine failures. We will now show that f is the largest number with such a property.

Let $b > f$ and assume that the system experiences b Byzantine failures. By the pigeonhole principle, each quorum contains a Byzantine failure. We cannot guarantee liveness because Byzantine nodes can all disagree with everything. □

2. Basic Properties of Quorums

Definition 2.1. 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.

Remark 2.2. 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 $Q(v_1) = \{\{v_1, v_2, v_3, v_4\}\} \subset 2^V$.

We explicitly exclude $\{\emptyset\}$ from the co-domain because we want $Q(v) \neq \emptyset$ for all $v \in V$. This is necessary because if $Q(v) = \emptyset$ for some $v \in V$, it satisfies $\forall q \in Q(v), v \in q$.

Definition 2.3. Let $\langle V, Q \rangle$ be an FBAS. $U \subset V$ is called a quorum if and only if $\forall v \in U, \exists q \in Q(v), q \subset U$.

Theorem 2.4. *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 2.5. *The set of quorums of a given FBAS is closed under union.*

Theorem 2.6. *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 2.7. 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 2.8. Let $\langle V, Q\rangle$ be an FBAS. We say $\langle V, Q\rangle$ enjoys quorum intersection if and only if for any pair of quorums U_1, U_2, $U_1 \cap U_2 \neq \emptyset$.

Definition 2.9. 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 2.10. 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 2.11. *Definition 2.9 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. Let $v \in V \setminus B, q' \in Q^B(v)$ be given. Then $q' = q \setminus B$ for some $q \in Q(v)$. By the definition of an FBAS, $v \in q$. Since $v \notin B$, $v \in q \setminus B = q'$. Therefore, $\langle V, Q\rangle^B$ is an FBAS. □

Theorem 2.12. *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 2.13. One can think of this theorem as "*A quorum in the 'original' universe is a quorum in the 'alternate' universe.*"

Definition 2.14. 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 2.15. Quorum intersection despite B is related to 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. 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 2.16. 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 2.17. *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 2.4. 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 2.18. Theorem 2.17 shows that $\langle V, Q\rangle$ enjoys quorum availability despite B if all nodes in $V\ B$ 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 2.19. 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 2.20. 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 2.21. *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 $q \in Q(v)$. □

Theorem 2.22. *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 $\langle V, Q\rangle^A$. □

Theorem 2.23. *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.

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

□

3. Dispensable Sets

Definition 3.1. 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.

Definition 3.2. 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.

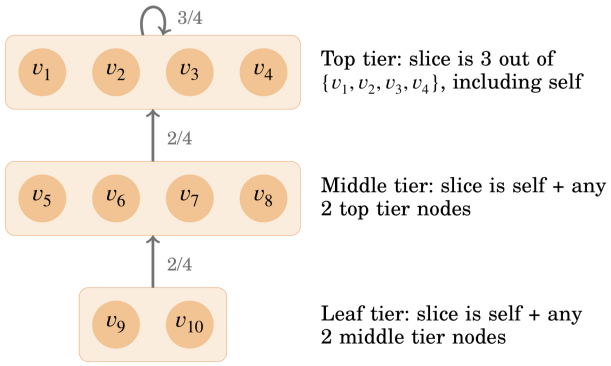

FIGURE 1. Tiered Quroum Example (P.5 of the white paper)

Example 3.3. 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, $V = \{v_1, v_2, v_3, v_4\}$ is a quorum.

    Fix: V is used in two different ways!

    Then $U \cap V = \emptyset$, 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:
    - In prior transactions, v_5 and v_6 act as well-behaved nodes and v_5 obtains 100 dollars in its account.

    - 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 $\{v_5, v_9, v_{10}\}$ and $\{v_6, v_9, v_{10}\}$ are both quorums.
    - Both v_5 and v_6 tell v_9 that v_5 is willing to send v_9 100 dollars. 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_5 to not believe this transaction.
    - Both v_5 and v_6 tell v_{10} that v_5 is willing to send v_{10} 100 dollars. For the same reason, there is no reason for v_{10} to not believe this transaction.
    - Thus v_5 manages to spend the 100 dollars twice, which can lead to some bad results. For instance, v_5 may be able to obtain 100 dollars worth of goods from v_9 and v_{10}.
    - 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 its 100 dollars. v_1 might tell v_5 that v_1 is sending v_5 100 dollars. Similarly, v_1 might tell v_6 that v_1 is sending v_6 100 dollars. However, every quorum slice of v_5 and v_6 contains at least one more tier-1 node. 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 v_5 double spending its 100 dollars. The tier-1 node does not agree with the two transactions and v_1's attempt to double spend money fails.

Theorem 3.4. *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.
For any $v \in V$,

$$\begin{aligned} v \in V \setminus B &\iff v \in V \wedge v \notin B \\ &\iff v \in V \wedge (v \notin B_1 \vee v \notin B_2) \\ &\iff (v \in V \wedge v \notin B_1) \vee (v \in V \wedge v \notin B_2) \\ &\iff (v \in (V \setminus B_1)) \vee (v \in (V \setminus B_2)) \\ &\iff v \in ((V \setminus B_1) \cup (V \setminus B_2)). \end{aligned}$$

Thus, $V \setminus B = (V \setminus B_1) \cup (V \setminus B_2)$. By the definition of a DSet, $V \setminus B_1$ and $V \setminus B_2$ are both quorums in $\langle V, Q \rangle$. By Theorem 2.4, $V \setminus B$ is a quorum in $\langle V, Q \rangle$.

We must now show that $\langle V, Q \rangle$ enjoys quorum intersection despite B. Let U_a, U_b be quorums in $\langle V, Q \rangle^B$.

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

because $U_a \cap B = \emptyset$. This implies that $(U_a \setminus B_1) \cup (U_a \setminus B_2) \neq \emptyset$. In other words, at least one of $U_a \setminus B_1$ or $U_b \setminus B_2$ is non-empty. We will show that both $U_a \setminus B_1$ and $U_b \setminus B_2$ are non-empty.

Without loss of generality, assume that $U_a \setminus B_1 \neq \emptyset$.

- $V \setminus B_1 \neq \emptyset$ is a quorum in $\langle V, Q \rangle$ because B_1 is a DSet. Similarly, $V \setminus B_2 \neq \emptyset$ 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, $(V \setminus B_2) \setminus B_1 \neq \emptyset$. $(V \setminus B_2) \setminus B_1$ is a quorum in $\langle V, Q \rangle^{B_1}$ by Theorem 2.12 because $V \setminus B_2$ is a quorum in $\langle V, Q \rangle$ and $(V \setminus B_2) \setminus B_1 \neq \emptyset$.
- $U_a \setminus B_1$ is a quorum in $\langle V, Q \rangle^{B_1}$ by Theorem 2.12 because U_a is a quorum in $\langle V, Q \rangle$ and $U_a \setminus B_1 \neq \emptyset$.

Because B_1 is a DSet in $\langle V, Q \rangle$, $\langle V, Q \rangle^{B_1}$ enjoys quorum intersection. Therefore, $(U_a \setminus B_1) \cap ((V \setminus B_2) \setminus B_1) \neq \emptyset$.

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

Thus, $U_a \setminus B_2 \neq \emptyset$. As a result, we know that $U_a \setminus B_1$ is a quorum in $\langle V, Q \rangle^{B_1}$ and $U_a \setminus B_2$ is a quorum in $\langle V, Q \rangle^{B_2}$ by Theorem 2.12.

Using the same argument, we can show that $U_b \setminus B_1 \neq \emptyset$ and $U_b \setminus B_2 \neq \emptyset$. Again, $U_b \setminus B_1$ is a quorum in $\langle V, Q \rangle^{B_1}$ and $U_b \setminus B_2$ is a quorum in $\langle V, Q \rangle^{B_2}$ by Theorem 2.12.

By putting these results together, we know that $U_a \setminus B_1$ and $U_b \setminus B_1$ are both quroums in $\langle V, Q \rangle^{B_1}$.

Since B_1 is a DSet, $\langle V, Q \rangle^{B_1}$ enjoys quorum intersection. Thus $(U_a \setminus B_1) \cap (U_b \setminus B_1) \neq \emptyset$. This implies $(U_a \cap U_b) \setminus B_1 \neq \emptyset$. Therefore, $U_a \cap U_b \neq \emptyset$. $\square$

Remark 3.5. Theorem 3.4 states that the intersection of two DSets is a DSet. However, the union of two Dsets is not a DSet in general. Consider the FBAS $\langle V, Q\rangle$ where $V = \{v_1, v_2, v_3, v_4\}$ and $Q(v_i) = \{U \subset V \mid v_i \in U, |U| = 3\}$. Then $B = \{v_1\}$ is a DSet because

- 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.
- $V \setminus B = \{v_2, v_3, v_4\}$ 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 3.6. *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. By Theorem 3.4, B is a DSet.

- Case 1: $v \in B$. Then there exists no DSet B_v such that B_v contains all ill-behaved nodes and $v \notin B_v$. Therefore, v is not an intact node. In other words, v is a befouled node.
- Case 2: $v \notin B$. Then there exists a DSet B_v that contains all ill-behaved nodes and $v \notin B_v$. In other words, v is intact and thus v is not a befouled node.

Therefore, B is precisely the set of befouled nodes and it is a DSet. □

Theorem 3.7. *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 3.2, a node $v \in V$ is intact if and only if $v \notin B$. By Theorem 2.23, $\langle V, Q\rangle$ 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. □

4. Voting, Accepting, and Ratifying

Definition 4.1. 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 against a in the future.

Definition 4.2. 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.
- It determines that either
  - There exists a quorum 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.

Note that it is possible for a node to accept a statement it did not vote for. Furthermore, it is possible for a node to accept a statement after voting for a contradictory statement.

Definition 4.3. 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 4.4. *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 4.1, v has never accepted a statement contradicting a. By Definition 4.2, v accepts a. □

Theorem 4.5. *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, this goes against the definition of voting. In other words, v must be ill-behaved, which is a contradiction to our assumption. □

Theorem 4.6. *Let $\langle V, Q\rangle$ be an FBAS. Let $B \subsetneq V$ be a subset containing all the ill-behaved nodes and suppose that $\langle V, Q\rangle^B$ 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 2.12, $U_1' = U_1 \setminus B$ 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, $U_1' \cap U_2' \neq \emptyset$. Let $v \in U_1' \cap U_2'$. 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 $v \in U_1 \setminus B$. □

Theorem 4.7. *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 3.6. By the definition of a DSet (Definition 3.1), $\langle V, Q\rangle^B$ enjoys quorum intersection. By Theorem 4.6, v, v' cannot ratify contradictory statements. □

Lemma 4.8. *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. Since V is finite, there has to be an intact node v such that no intact nodes in V accepted a before v.

Since $\langle V, Q\rangle$ enjoys quorum intersection, B is a DSet by Theorem 3.6. By Theorem 3.7, B is not v-blocking. Therefore, by Definition 4.2, there must exist 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. Because of the way we picked 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 2.12, 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. □

Theorem 4.9. *Two intact nodes in an FBAS $\langle V, Q\rangle$ enjoying quorum intersection cannot accept contradictory statements.*

Note that Theorem 4.9 is a stronger version of Theorem 4.7 by Theorem 4.4.

Proof. Suppose otherwise. Let $a, \bar{a}$ be contradictory statements accepted by two intact nodes in $\langle V, Q\rangle$. By Lemma 4.8, $a, \bar{a}$ are ratified by some intact nodes in $\langle V, Q\rangle^B$. By Definition 3.1, $\langle V, Q\rangle$ enjoys quorum intersection despite B. In other words, $\langle V, Q\rangle^B$ enjoys quorum intersection. By Theorem 4.7, $a, \bar{a}$ cannot be ratified by v, v' in $\langle V, Q\rangle^B$, which is a contradiction. □

5. Confirmation

Definition 5.1. A statement a is irrefutable in an FBAS if no intact node can ever vote against it.

Definition 5.2. 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.

Lemma 5.3. *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. Let S be a set such that $U \subset S \subset V$. 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. Either $S^- = \emptyset$, or $\exists v \in S^-$ such that S^+ is v-blocking.*

Proof. 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 $\langle V, Q\rangle$. By Theorem 2.22, S^+ is not v-blocking in $\langle V, Q\rangle^B$ for any $v \in S^- = (V \setminus B) \setminus S^+$. By Theorem 2.23, $\langle V, Q\rangle^B$ enjoys quorum availability despite S^+. By Definition 2.16, $(V \setminus B) \setminus S^+$ is a quorum in $\langle V, Q\rangle^B$, or $V \setminus B = S^+$. If $V \setminus B = S^+$, then $S^- = \emptyset$, and we are done. Suppose $(V \setminus B) \setminus S^+$ is a quorum in $\langle V, Q\rangle^B$.

- $U \setminus B$ is a quorum in $\langle V, Q\rangle^B$ by Theorem 2.12.
- Since B is a DSet by Theorem 3.6, $\langle V, Q\rangle^B$ enjoys quorum intersection by Definition 3.1.
- However,

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

This is a contradiction. □

Theorem 5.4. *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. Then there exists a quorum $U \not\subset B$ such that every node in U broadcast that it accepted a. After every node in U has broadcast that it accepted a, there may be a node v that accept a since U is v-blocking. After all such nodes broadcast that they accepted a, there may be other nodes that accept a as well. Since V is a finite set, there is a point in time where the number of nodes that accept a does not increase. Let S be the set of all nodes that accepted a and broadcast it.

- U is a quorum containing an intact node.
- $U \subset S \subset V$.
- 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 5.3, S^- is empty, or S^+ is v-blocking for some $v \in S^-$. However, the latter is impossible because it would imply that v would accept a. Therefore, S^- is empty, and thus every intact node accepted a. □

6. Nomination

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

Definition 6.1. A node v is said to nominate a value x if and only if it votes for the statement *nominate* x.

Definition 6.2. 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 6.3.