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. Basic Properties of Quorums

Definition 1.1. 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.

Definition 1.2. 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 1.3. *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. $\square$

Theorem 1.4. *In an FBAS (V, Q), 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. $\square$

Example 1.5. One might imagine that the intersection of quorums is always a quorum. However, this is not true in general.

Let $V = \{v_1, \cdots, v_4\}$ 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, $Q(v_i) = \{U \mid U \in 2^V, v_i \in U\}$.

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 1.6. 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 1.7. 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 $\forall v \in V, Q^B(v) = \{q \setminus B \mid q \in Q(v)\}$.

Theorem 1.8. *Definition 1.7 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 1.9. *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 $\langle V, Q\rangle^B$. □

2. DSet

Definition 2.1. 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 the following conditions are satisfied:

- $\langle V, Q\rangle^B$ enjoys quorum intersection.
- $B = V$ or $V \setminus B$ is a quorum in $\langle V, Q\rangle$.

Definition 2.2. 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.

Theorem 2.3. *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 $v \in V$,

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

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 1.3, $V \setminus B$ is a quorum in $\langle V, Q\rangle$.

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

- $U_a \setminus B_1$ is a quorum in $(\langle V, Q\rangle^B)^{B_1} = \langle V, Q\rangle^{B_1}$ by Theorem 1.7.
- Similarly, $U_b \setminus B_1$ is a quorum in $\langle V, Q\rangle^{B_1}$, and $U_a \setminus B_2$ and $U_b \setminus B_2$ are both quorums in $\langle V, Q\rangle^{B_2}$.

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

because U_a is a quorum in $\langle V, Q\rangle^B$. In other words, $(U_a \setminus B_1) \cup (U_a \setminus B_2) \neq \emptyset$. Similarly, $(U_b \setminus B_1) \cup (U_b \setminus B_2) \neq \emptyset$.

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

- $V \setminus B_1$ is a quorum in $\langle V, Q\rangle$ because B_1 is a DSet. Similarly, $V \setminus B_2$ 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, $(V \setminus B_2) \setminus B_1$ is a quorum. By Theorem 1.7, $(V \setminus B_2) \setminus B_1$ is a quorum in $\langle V, Q\rangle^{B_1}$.
- $U_a \setminus B_1$ is a quorum in $(\langle V, Q\rangle^B)^{B_1} = \langle V, Q\rangle^{B_1}$ for the same reason.

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

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

Thus, $U_a \setminus B_2 \neq \emptyset$. Using the same argument, we can show that $U_b \setminus B_1 \neq \emptyset$ and $U_b \setminus B_2 \neq \emptyset$. Since $U_a \setminus B_1$ and $U_b \setminus B_1$ are quorums in $\langle V, Q\rangle^{B_1}$ and B_1 is a DSet, $(U_a \setminus B_1) \cap (U_b \setminus B_1) \neq \emptyset$ by the definition of a DSet. This implies $(U_a \cap U_b) \setminus B_1 \neq \emptyset$. Therefore, $U_a \cap U_b \neq \emptyset$. $\square$

Theorem 2.4. *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 2.3, 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. $\square$

3. Voting

Theorem 3.1. *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. $\square$

Theorem 3.2. *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 1.9, $U_1' = U_1 \setminus B$ 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 $v \in U_1 \setminus B$. $\square$