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/.

1. defn

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 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 $\forall v \in U, \exists q \in Q(v), q \subset U$.

Definition 1.3. 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 1.4. Let $\langle V, Q\rangle$ be an FBAS and $B \subset V$. Then $\langle V, Q\rangle^B$ is defined to be $\langle V \setminus B, Q'\rangle$ where $\forall v \in V, Q'(v) = \{q \setminus B \mid q \in Q(v)\}$.

2. Theorems

Theorem 2.1. *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 $\langle V, Q\rangle^B$. □

Theorem 2.2. *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 2.3. *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 2.1, $U_1' = U_1 \setminus B$ 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 $v \in U_1 \setminus B$. $\square$