STELLAR CONSENSUS PROTOCOL(SUB-NOTES)

HIDENORI SHINOHARA

Abstract. This is a collection of things that are related to SCP, but not enough to make it to the main notes.

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. $\square$