The University of Melbourne
School of Computing and Information Systems
COMP90020 Distributed Algorithms

Tutorial Week 8: Distributed Consensus

Notes

Note all of the following assume the system is synchronous (why?). Coordinated attack assumes possible channel faults. Byzantine Agreement and Byzantine Broadcast assume possible byzantine (arbitrary) faults.

Coordinated Attack

We have $n \geq 2$ nodes. The messages received in round $i+1$ is always a subset (possibly empty, communication unreliable) of the set sent in round i. Each node starts with an input $v_i \in \{0,1\}$ and must decide on $d_i \in \{0,1\}$ in a bounded number of rounds.

- **Agreement:** $d_i = d_j$ for all nodes.
- **Integrity:** If $v_i = v_j$ for all pairs of nodes and no messages are lost, all processes have the same output $d_i = d_j$.
- **Termination:** All processes terminate in a bounded number of rounds.

Byzantine Broadcast (BB)

Some node ($p_j \in p_1, ..., p_n$) broadcasts v_j to every node ($\forall p_i \in \{p_1, ..., p_n\}$), and each correct node must agree on the message received. If p_j is correct then all correct nodes must agree $d_i = v_j$.

- **Agreement:** $d_i = d_j$ for each correct node.
- **Integrity:** If p_j is a correct, then all correct nodes must agree on ouput $d_i = v_j$.
- **Termination:** eventually $d_i \neq \perp$ for each correct node where initially $d_i = \perp$.

Commonly described in terms of Generals and lieutenants.

Byzantine Agreement (BA)

Each node ($\forall p_i \in p_1, ..., p_n$) begins holding an input v_i and they must come to an an agreement on their output.

- **Agreement:** $d_i = d_j$ for all correct nodes.
- **Integrity:** If $v_i = v$ for all correct nodes, then $d_i = v$ for all correct nodes.
- **Termination:** eventually $d_i \neq \perp$ for each correct node where initially $d_i = \perp$.

Exercises

36. Two loyal generals are planning to coordinate their actions for conquering a strategic town. To conquer the town, they need to both agreee on: attack or retreat; otherwise, if only one of them attacks and the other does not, then the generals are likely to be defeated. To plan the attack, they send messages back and forth via trusted messengers. The communication is synchronous. However, the messengers can be killed or captured so the communication is unreliable.

In this example is it possible to satisfy *agreement*, *integrity* and *termination* as stated in **Coordinated Attack**? Provide justification.

37. Construct an execution of the EIG algorithm to solve byzantine agreement (BA) where there are 3 processes, 1 process exhibits byzantine faults and integrity is not satisfied (draw two EIG trees and show they have a different λ).

38. When considering Byzantine Agreement (BA) and Byzantine Broadcast (BB):

(a) Is it possible to construct a solution to BB using a solution to BA? Briefly explain.

(b) Is it possible to construct a solution to BA using a solution to BB? Briefly explain (assume $f < \frac{n}{2}$).

39. Seven members of a family interviewed a candidate for the open position of a cook. If the communication is purely asynchronous and message-based, and decisions are based on majority votes, then describe a scenario to show how the family can remain undecided, when one member disappears after the interview.

40. Using oral messages in the context of generals reaching consensus on an attack where each p_i initially has some $v_i \in \{0, 1\}$, a solution to byzantine agreement (BA) can reach consensus when less than one-third of the generals are traitors (byzantine). However, it does not suggest how to identify the traitors. Examine if the traitors can be identified without any ambiguity if the number of traitors is known.