|  |  |  |
| --- | --- | --- |
|  | **Distributed Algorithms - Exercise**  **Winter term 2017/18** | **Danh Le Phuoc**  **Qian Liu**  **ODS** |
| *Exercise sheet 4* | | |

**Exercise 4.1: Distributed Consensus**

**Questions**

**Describe the agreement of the byzantine generals and explain the recursive algorithm for oral messages.**

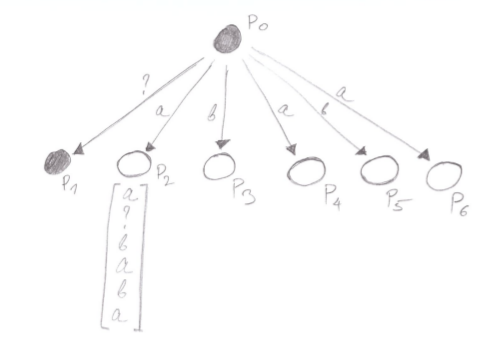
Byzantine generals problem is a common problem in achieving consensus among processes, who may be faulty. One distinguishable process proposes a single value, and all other processes must agree on that value. Problem is that some of the processes are faulty. Even the proposing process can be faulty, so byzantine problem can be defined as proposing a value by a single process and:

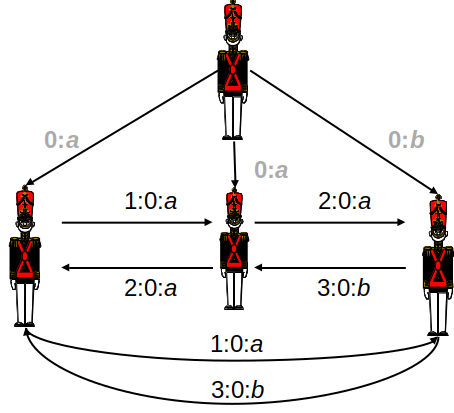
* All correct processes should agree on the single value
* If a proposing process is not faulty, the value, agreed upon, should correspond to proposed value

let n be the number of generals and m the number of faulty generals.

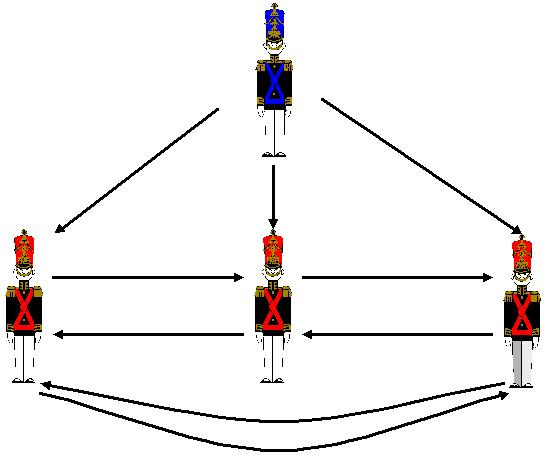
To reach an agreement, the following must stand : or

When a general receives the command from the commander, it is not sure if the commander is faulty. Therefore, each general sends its message to other generals. Each general decides on the most likely value, shown on Figure 1. In some scenarios, there can be draws (Figure 2). To handle these situations, every general starts an instance of an algorithm with n-1 processes with the value which it received from its commander.

  
Figure 2: Ilustration in which a faulty process can introduce a draw problem among other processes. In order to prevent this scenario, additional reqursions are required

  
Figure 1: Decision is made by each general regardless of the fact that commander is faulty. Each general adopts most likely value

**Implement the agreement of the byzantine generals for m faulty generals using pseudo-codes. Do your implementation in a way that it is possible to distinguish between faulty and non-faulty generals as well as between the commanding general and the lieutenant generals. Explain your implementations with graphs and texts, Messages shall visualize their message path and the actual value, as well as integrity (message has been corrupted). Demonstrate your implementation given the following scenarios:**



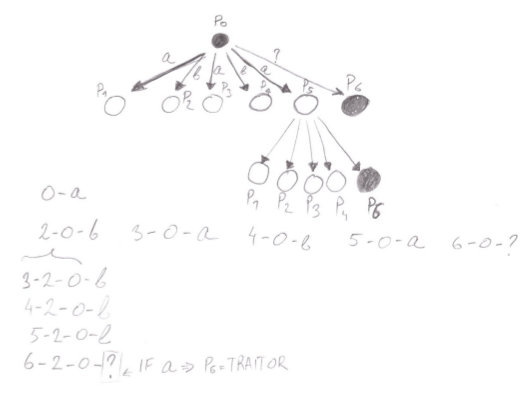
* 1. **n = 4 (4 generals), m = 1 (one randomly chosen general is faulty).**
  2. **n = 7 (7 generals), m = 2 (two randomly chosen generals are faulty).**
  3. **n = 10 (10 generals), m = 3 (three randomly chosen generals are faulty).**

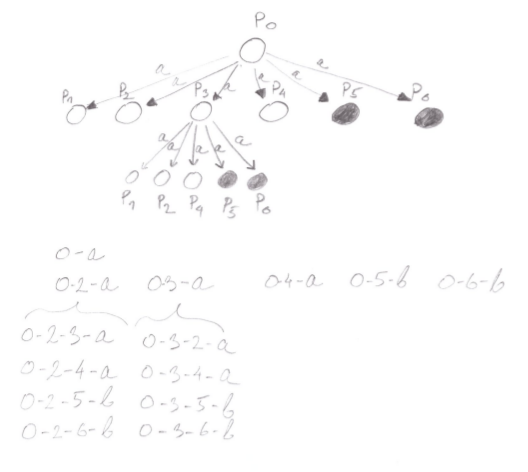
This algorithm is based on the recursive properties. Out of n-1 processes, each is recursively initiating the algorithm on n-2 other processes (his predecessor and himself excluded). The messages are comprised from two fields:

* Path
* Value

Upon each process appends its ID to the path of the broadcasted message, so at the resulting leafs it is possible to fully reconstruct paths from all broadcasts.

At the liefs of the resulting tree, each process can decide upon a given value, and identify which of other processes are traitors. Each process makes a traitor list. As two different processes can make different traitor lists, it is necessary to exchange traitor lists among “non-traitor” processes. A “non-traitor” process appends traitors to its list as long as they originate from a process, who is not in the traitor list.

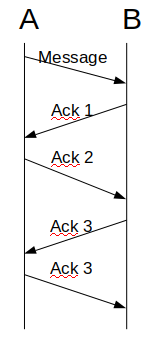
  
Figure 4: Illustration in which a faulty general can iduce further "draw" problems. By having ID path embedded in the message, correct processes can eliminate faulty processes

  
Figure 3: Ilustration in which two faulty processes influence decisions of correct processes. The correct value is assigned at leaf level of recursion

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

**Argue why it is impossible for the two generals to coordinate their actions of attacking at the same time.**

**(Hint: Unlike the byzantine generals problem, here all generals are loyal, but the communication is unreliable. If general A sends a message attack at 2 a.m. to general B, then he will want an acknowledgment from B; otherwise, he won’t attack in the fear of moving alone. But B also will ask for an acknowledgment of the acknowledgment. Now you see the rest of the story.)**



As can be seen from Figure 5, general A sends a proposal to general B. To be certain in the reception of the message, he awaits mack 1. When B responds, he remains uncertain if the acknowledgement was delivered. Upon receiving an acknowledgement, process A acknowledges(Ack 2) that he received an acknowledgement(Ack 1). At that point, he is uncertain that B received Ack 2, and waits for further acknowledgements.

This is repetitive and at each iteration, one of the processes is uncertain in the acknowledgement reception on the other side, and will therefore remain inactive.

**Exercise 4.2: Distributed Transactions**

**Questions**

**Two-phase locking works for distributed transactions. As an alternative, consider this: There are n (n > 1) servers; each server manages m objects (m > 1). Each server will allow transaction sequential access to the locks on the objects managed by it. Is this sufficient for serializability? Is this sufficient to avoid deadlocks? Explain.**

**Specify two execution histories H1 and H2 over a set of transactions, so that (a) H1 is permissible under 2PL, but not under basic time stamp ordering, and (b) H2 is permissible under basic time stamp ordering, but not under 2PL.**