Homework 3 - Distributed Systems

Foundations of Blockchain Technology and cryptocurrencies

Fall 2019

Sharif Blockchain Lab
Sharif University of Technology
Department of Electrical Engineering

Deadline: Sunday 1398/8/26 At the beginning of the class

(The Homeworks will be collected at the beginning of the class. 3 minutes after the start of the class the homeworks will not be accepted).

Section 1) Leader Election

1. For the *LCR* algorithm (slide 16),

   (5 points) a. Give a UID assignment for which $\Omega(n^2)$ messages are sent.

   (5 points) b. Give a UID assignment for which only $O(n)$ messages are sent.

   (10 points) c. Show that the average number of messages sent is $O(nlogn)$, where this average is taken over all the possible orderings of the processes on the ring, each assumed to be equally likely.

Section 2) Synchronous Consensus with Link Failure

2. **(15 points)** Show that a solution to the (deterministic) coordinated attack problem for any nontrivial connected graph implies a solution for the simple graph consisting of two processes connected by one edge. (Therefore, this problem is unsolvable in any nontrivial graph.)

Section 3) Synchronous Consensus with Stopping Failures

3. **(10 points)** Consider the *FloodSet* algorithm (slide 47) for f failures. Suppose that instead of running for $f + 1$ rounds, the algorithm runs for only f rounds, with the same decision rule. Describe a particular execution in which the correctness requirements are violated.

4. **(15 points)** Trace the execution of the *EIGStop* algorithm for four processes and two failures, where the processes have initial values 1, 0, 0, and 0, respectively. Suppose that processes 1 and 2 are faulty, with process 1 failing in the first round after sending to 2 only, and process 2 failing in the second round after sending to 1 and 3 but not to 4.

Section 4) Synchronous Consensus with Byzantine Failures

5. **(15 points)** We proved that it is impossible to reach consensus if $\geq \frac{1}{3}$ of the processors are faulty. Now suppose that each processor has a secret private key and it's signature is verifiable for other processors. With respect to the correctness conditions mentioned for byzantine agreement what can we say about the lower bound on the number of processors required to tolerate f failures in this situation? describe an algorithm for solving byzantine agreement in this scenario. Analyze time and message complexity of your algorithm.

6. **(15 points)** Consider a Synchronous Consensus with Byzantine Failures problem for n processes with general agreement and termination conditions and a validity condition which states that the decided value must be the input of at least one node. Suppose that each process has an initial value that is an integer in $[0, m-1]$ (m different values). Show that with the presence of f byzantine processes, a consensus is possible if and only if $n \geq f \times max(3, m) + 1$.

Section 5) Consensus with Bandwidth Limitations

7. We have investigated Consensus in a fully connected network with no failure and unlimited bandwidth where each node can send its value to all other nodes. However, in practice, bandwidth limitations are often of great importance as well as failures. Now we consider a network of nodes with unique IDs (e.g. 1 to n) where there is no crash, and every node can only send one message containing one value to one neighbor per round.

   (10 points) a. Develop an algorithm that solves consensus in this scenario. Optimize your algorithm for runtime!

   (5 points) b. What is the runtime of your algorithm?

   (5 points) c. Assume that you not only need to solve consensus, but the more challenging task that every node must learn the input values of all nodes. Show that this problem requires at least $n - 1$ time units!

Section 6) Synchronous Consensus in a Grid

8. Consider a 2-dimensional grid network such that every process has up to 4 neighbors. The width of the grid is w, the height is h. Width and height are defined in terms of edges: A 2×2 grid contains 9 nodes! The grid is big, meaning that $w + h$ is much smaller than $w \times h$.

   (5 points) a. Assume every node knows w and h. Write a short protocol to reach consensus.

   (10 points) b. From now on the nodes do not know the size of the grid. Write a protocol to reach consensus and optimize it according to runtime. How many rounds does your protocol require?

   Assume there are Byzantine nodes and that you are the adversary who can select which nodes are Byzantine.

   (10 points) c. What is the smallest number of Byzantine nodes that you need to prevent the system from reaching agreement, and where would you place them?

Section 7) FLP

9. Answer the following questions regarding the proof of lemma 3 of the FLP impossibility result

   (10 points) a. Using contradiction we assume that there are both 0-valent and 1-valent configurations in D. Argue why this assumption is valid.

   (15 points) b. Argue why there must be configurations $C0$ and $C1$ in C and $D0$ and $D1$ in D such that:

   - $C1$ = "$C0$ followed by some event $e' = (p', m')$"
   - $D0$ = "$C0$ followed by event $e = (p, m)$"
   - $D1$ = "$C1$ followed by event $e = (p, m)$"
   - $D0$ is 0-valent and $D1$ is 1-valent