Prasanna Bartakke
EE19B106
Electrical Engineering
@prasanna648:matrix.org
ee19b106@smail.iitm.ac.in

Module 1 Assignment Version 2

CS 6858 : Jul – Nov, 2022 : John Augustine
Due : 2 PM on Friday, September 16, 2022
(Submission via turnitin)

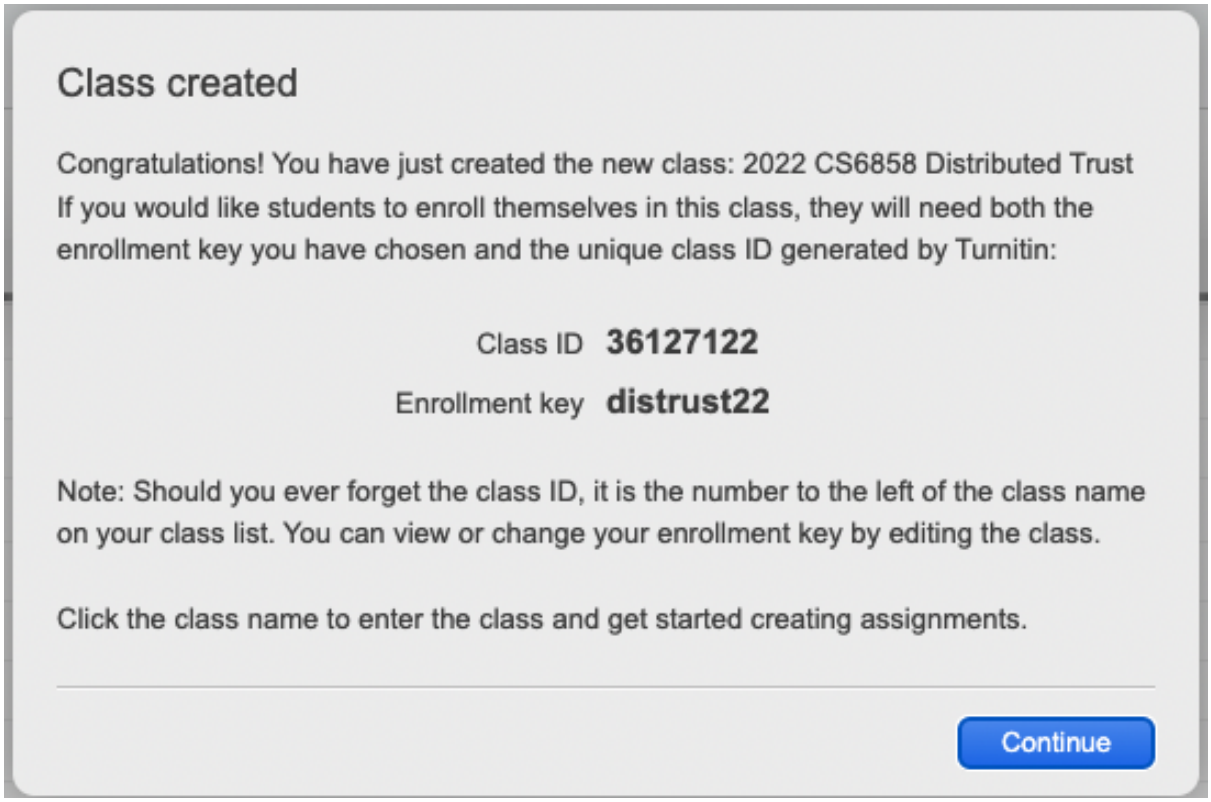


Figure 1: Turnitin Details.

Contents

Problem 1. Tossing Random Coins With PKI

In this problem, we will design attack strategies to foil protocols for tossing global coins. Consider a synchronous message passing complete network with n nodes $\{1, 2, \ldots, n\}$; you may assume PKI. Nodes can perform any required computation instantaneously at any time and this includes tossing coins to generate uniformly random bits. Up to b nodes are Byzantine for some $b < n$; b is common knowledge among the nodes. Time runs synchronously starting from round 1. Within each round, each node can send a finite-sized message to every other node during the first half of the round; nodes can also refrain from sending anything. Any good node must send the same message to all other nodes (within a round) whereas bad nodes can send different messages to different nodes. In the second half of the round, the messages will be delivered. We are exploring the challenges in designing algorithms that guarantees that

(agreement) all good nodes output the same bit r and

(valid randomness) the probability that $r = 1$ is exactly $1/2$.

You can imagine the output bit at each node to be a "write-once" bit that cannot be edited after the first (and only) write operation.
Your goal is to design attack strategies for the following algorithms. The attack strategies must be simple, precise and succeed with the ***smallest*** possible value for b.

Part 1. Using the Dolev-Strong Byzantine Broadcast protocol.

Part 2. Relying on $b + 1$ signatures

Problem 2. Leader Election by Passing a Token

Part 1. Analysis – Consistency

Part 2. Analysis – Byzantine Strategy

Part 3. Analysis – Via Experimentation

Part 4. Analysis – Conjecture

Problem 3. Incorrect Implementations of the Dolev-Strong Protocol

In this problem, you are asked to help analyze two buggy implementations of the Dolev-Strong protocol. You must provide specific examples (and attack strategies) illustrating the mistake. Your example in each case must be small and the attack strategy must be as simple as possible. (This problem is taken from the book by Elaine Shi – Exercise 6 on Page 19).

Part 1. Lanie's Mistake

Part 2. Elanna's Mistake

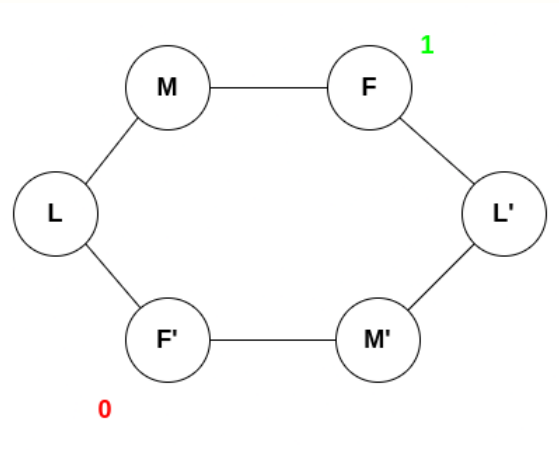
Problem 4. Randomized Lower Bound

Part 1. Reading Assignment

Provide your answer in this space.

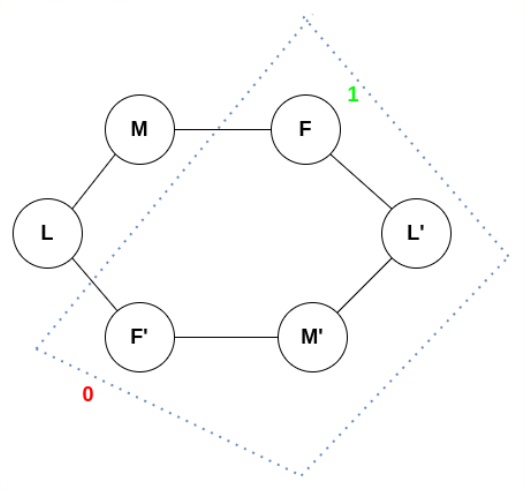
Part 2. Randomized Lower Bound

Assume the probability of error to be δ. We want to prove that it is impossible to achieve BB with $\delta \leq \frac{1}{3}$ when $f \geq \frac{n}{3}$. Validity with δ error is defined as follows: If an honest sender has an input bit b, with probability at least $1 - \delta$, all the honest nodes must output b at the end of the protocol. Agreement is defined as follows: with probability at least $1 - \delta$, all the honest nodes output the same bit at the end of the protocol.
Six nodes F, L, M, F', L' and M' are connected in a cyclic manner.



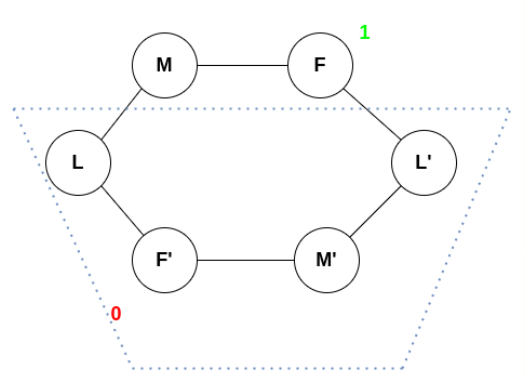
Node F has an input of 1, and node F' has an input of 0. We will assume that there exists a protocol P, that satisfies consistency and validity when $f \geq \frac{n}{3}$ with a probability of error less than $\frac{1}{3}$. We will consider 3 different interpretations of our model.

- *Interpretation 1*: Consider nodes L and M are honest, and node F is corrupt. Node F simulates the nodes F, F', L' and M'.



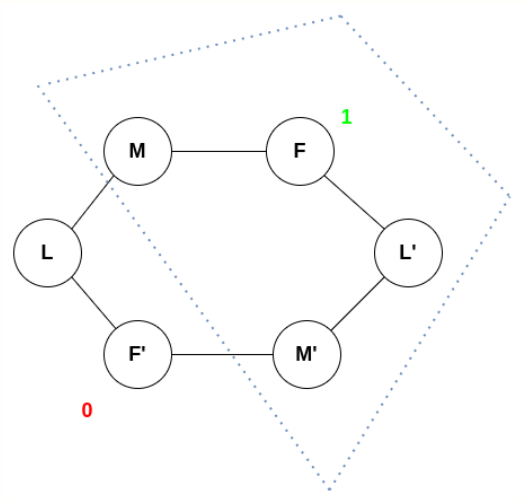
Using this interpretation, we conclude that nodes L and M must output the same bit with probability $\geq \frac{2}{3}$.

- *Interpretation 2*: Node L is corrupt, simulating all the nodes L, L', F' and M', whereas nodes F and M are honest.



Using this interpretation, by validity, we conclude that M should output F's input bit, that is 1 with probability $\geq \frac{2}{3}$.

- *Interpretation 3*: Node M is corrupt, simulating all the nodes M, M', F, and L', whereas F' and L are honest.



Using this interpretation, by validity, we conclude that L should output the input bit of F', that is, 0 with probability $\geq \frac{2}{3}$.

Consider event A when the output of L and M are the same. Consider event B when the output of M is 1 and event C when the output of L is 0. Let B' be the event that the output of M is 0. We can say that $P(B) + P(B') = 1$. Using the inclusion-exclusion principle, we can say $P(B' \bigcup C) = P(B') + P(C) - P(B' \bigcap C)$. The event $B' \bigcap C$ is A. Thus $P(B' \bigcup C) - P(C) + P(B' \bigcap C) = P(B')$. Finding a lower limit on $P(B')$ we get, $P(B') \geq \frac{2}{3} - 1 + \frac{2}{3}$, i.e. $P(B') \geq 1/3$ and thus $P(B) < \frac{2}{3}$. According to this argument probability that the output of M is 1 should be less than $\frac{2}{3}$ which contradicts with the result of interpretation 2.
Thus from the results of the 3 interpretations, we reach a contradiction about the probability of what L and M will output. Hence we have successfully proved that a protocol does not exist that achieves BB with a probability of error $\delta \leq \frac{1}{3}$.

Problem 5. Going Viral

Part 1. Experimental Setup

Part 2. Randomized Lower Bound

Acknowledgments

I would like to thank the following people with whom I discussed ideas.

- Pranav Phatak - for discussing why my approach was wrong in the original Q1, which ended up being the incorrect protocol in the updated Q1.
- Rajdeep Paul