Your Name
Your Roll Number
Your Department
Your Element ID
Your email address

Module 1 Test

CS 6858 : Jul – Nov, 2022 : John Augustine
Due : 1 PM on Sunday, Oct 02, 2022
(Submission via MOODLE)

Instructions

1. You are NOT allowed to discuss with others
2. I will be happy to clarify questions on moodle. You must only post in the forum titled "Module 1 Test Questions and Clarifications."
3. You can handwrite your solutions, scan, and upload them into moodle.
4. Clearly indicate the question number and the sub-part number in your answer sheets.
5. Please note that late submissions will not be accepted, so please submit well before the cutoff time.

Contents

Problem 1. A rumor among friends (2+3 = 5)

Consider n friends numbered $1, 2, \ldots, n$. One of them (wlog, friend 1) learned of a rumor on day 0. Each day (starting on day 1), those who received the rumor on the day before call up all the other friends (in some arbitrary order) and pass on the rumor. However, some of them are suddenly overcome with guilt and stop making any more phone calls. Note that such guilt can occur at any time during any day (but not during a phone call). The total number of friends who are overcome with guilt is at most $b < n$.

Part 1. Inconsistency among the guilt-free up to day b

Suppose an adversary who is observing the process of rumor spreading has the power to decide when each friend feels guilt (and therefore stops making the calls). Prove that at the end of each day $i \leq b$, there will be at least two friends who are guilt-free at that time such that one of them knows the rumor while the other does not

Part 2. Consistency among the guilt-free

Prove that at the end of day $b + 1$, either (a) all guilt-free friends know the rumor or (b) none of the guilt-free friends know the rumor.

Problem 2. Streamlet Scenarios (2+2+2=6)

Consider an execution of the Streamlet protocol where $n = 99$. Suppose that strictly fewer than $n/3$ nodes are corrupt. For each of the following scenarios, please answer (**giving full details**) whether such a scenario can possibly occur during the execution. If so, provide an explanation of how such a scenario can occur. If not, explain why. For each scenario, if it is possible to occur, please also state which blocks are considered final by the relevant nodes. (Note: this is exercise 13 from Shi's book.)

Start each scenario by clearly stating whether it is possible or not before providing further details.

Part 1. Scenario 1

The two notarized chains $\perp - 1 - 3 - 5$ and $\perp - 2 - 4 - 6$ will both be in honest view.

Part 2. Scenario 2

An honest node P observes a notarized chain of the form $\perp - 3 - 4 - 5$, and another honest node Q observes a notarized chain of the form $\perp - 1 - 2 - 4 - 5 - 6$.

Part 3. Scenario 3

An honest node P observes a notarized chain of the form $\perp - 3 - 4 - 5$, and another honest node Q observes a notarized chain of the form $\perp - 1 - 2 - 7 - 8 - 9$.

Problem 3. Streamlet under a Tighter Assumption (2)

As a software engineer, Victor is given a task to implement a consensus protocol for a core service of his company. Victor decided to implement the Streamlet protocol. However, his manager told him that it is OK to assume that strictly less than $n/4$ nodes can be corrupt. (Recall that in the original protocol, we assume that strictly less than $n/3$ nodes can be corrupt.) Being an expert on Streamlet, Victor wants to modify the protocol to make use of this stronger assumption in order to maximize system efficiency. What is the minimum number of votes we need to notarize a block in this case? (Recall that in the original protocol, we need 2/3 fraction of the nodes to vote to get a notarization.) Please prove consistency. (This is based on Exercise 14 of Shi's book.)

Problem 4. Lower Bound Argument (2)

Part 1. Reading Assignment

Read Theorem 17.12 in `https://disco.ethz.ch/courses/podc_allstars/lecture/chapter17.pdf` along with some context around it.

Part 2. Is the proof correct?

Justify your answer.
If you think the proof is correct, argue that the proof we discussed in class (frame number 83 onwards) is overkill.
If you think the proof is not correct, point out precisely where it fails. Also, can we salvage the proof to some extent?

Problem 5. Censorship Resistance (3+2+2=7)

There are n people in a village. Initially, some s of these villagers have found a secret recipe for the world's tastiest laddus. Unfortunately for them, there is a laddu mafia that wishes to control all laddu sales and they do not want the secret recipe to spread.

Each day, each person a who knows the secret recipe finds one other person b who does not know the recipe and conveys the secret to b; if there is no such b, a just takes the day off and makes some laddu for herself/himself. The mafia is also active. At the end of each day, they find up to k villagers (for some $k < n/2$) who know the recipe and surreptitiously administer a forgetfulness drug so that they forget the recipe. The drug only has a one-time effect each time it is administered. From the next day, the person will be back to normal and capable of learning the recipe and teaching to others.

Part 1. Finding s given k

Given a value of $k < n/2$, your goal is to find the smallest number of people s who should initially learn the recipe to make sure the recipe reaches and stays within the collective memory of the village. (We say that the recipe is in the collective memory of the village at some point if at least $n/2$ people know the recipe at all times thereafter.)

Part 2. Time to Collective Memory

Suppose s is sufficiently large to ensure that collective memory of the recipe is achieved. How many days (in the worst case) will it take for the recipe to reach collective memory?

Part 3. Randomized Spreading (Extra Credit)

In this variation, each person who knows the recipe can only choose another person at random and teach them the recipe (if they don't already know it). The power of the mafia remains unchanged. Work out the value of s when $k = n/10$ such that, with probability at least $1 - 1/n$, the recipe gets into the collective memory of the village.