COMS 6998-006 (Foundations of Blockchains)
Homework Set 3 (Sol)

Matin M.Babaei M. Parsa Dini

September 9, 2023

Problem 1

A. Since, Tendermint is a partially-Synchronous model, this highlights the challenge of de facto collusion between the Byzantine nodes and adversarial message delivery. Both Byzantine nodes and the adversary controlling message delivery have to the power to enforce silence from f nodes for an arbitrarily long period of time, and an honest node cannot distinguish whom is the culprit. In effect, each Byzantine node winds up knocking out two honest nodes—one honest node whose contributions are ignored (because they are massively delayed and it gets mistaken for a Byzantine node) and a second honest node whose received messages are cancelled by conflicting messages sent by a Byzantine node. Intuitively, we need one honest node still standing after all these knockouts, meaning $(n - f) - 2f > 0$ or, equivalently, $f < n/3$. Thus , if $(n - f) - 2f \leq 0$ and $f \geq n/3$, no protocol satisfies consistency including Tendermint protocol partially-synchrony.(We have proved this impossiblity result more precisely before)

B. Let's first recall the exact definitions of liveness:

Liveness (Strong Version): If a transaction is known to at least one honest node, that transaction is eventually added to every honest node's local history.

Liveness (Weak Version): If a transaction is known to all honest nodes, that transaction is eventually added to every honest node's local history.

Here we are talking about the strong version definition. This property actually doesn't hold for the version of the Tendermint protocol described in this lecture—if a transaction tx is known to only one honest node i, it is possible that i will never get any of its block proposals finalized and thus tx is effectively censored, never added to any node's local history. (Proving this fact is a slightly easy test for checking if you thoroughly understand the Tendermint protocol.) See more here.

Problem 2

Problem 3

A. In order to prove that there exists a constant $c1$ such that, with probability at least $1 - \delta$, a random leader sequence of length at least $c_1 \ln(\frac{1}{\delta})$ has a strict majority of honest leaders, we'll use the Chernoff bound and manipulate the equations. Here's the proof step by step: Firstly, We want to show that the strict majority of leaders are honest, which means at least $\frac{n}{2} + 1$ leaders are honest in a sequence of length n.

Assuming that a leader is Byzantine with probability α and honest with probability $1 - \alpha$, the probability of having exactly k honest leaders in the sequence follows a binomial distribution (let H, B denote the set of honest nodes and Byzantine nodes, respectively.):

$$\mathbb{P}[|B| = n - k] = \mathbb{P}[|H| = k] = \binom{n}{k}(1 - \alpha)^k \alpha^{n-k} \tag{1}$$

To ensure a strict majority of honest leaders, we need to consider the cumulative probability of having at least $n/2n$ honest leaders:

$$\mathbb{P}[|B| \leq \frac{n}{2}] = \mathbb{P}[|H| \geq \frac{n}{2}] = \sum_{k=0}^{\frac{n}{2}} \binom{n}{k} (1-\alpha)^k \alpha^{n-k} \tag{2}$$

Now we can bound this probability using the Chernoff bound:

$$\mathbb{P}[|B| \leq \frac{n}{2}] = \mathbb{P}[|H| \geq \frac{n}{2}] \leq \exp(-\frac{\gamma^2 \mu}{2}) \tag{3}$$

where $\gamma = 1 - \frac{n}{2n} = \frac{1}{2}$ (as we want a strict majority) and $\mu = n(1-\alpha)$ (expected(mean) number of honest leaders).
Now (2) and (3) imply that:

$$\mathbb{P}[|H| \geq \frac{n}{2}] \leq \exp(-\frac{n^2(1-\alpha)^2}{8}) \tag{4}$$

Now we wish to find a $c_1 \in \mathbb{R}$ such that:

$$\exp(-\frac{n^2(1-\alpha)^2}{8}) \leq \delta \tag{5}$$

Now getting logarithm from both sides implies that:

$$n^2(1-\alpha)^2 \geq 8|\ln(\delta)| \rightarrow n \geq \sqrt{\frac{8|\ln(\delta)|}{(1-\alpha)^2}} \tag{6}$$

Thus, if we choose $c_1 = \sqrt{8}$ then we have(Note that $\delta \in (0,1) : |\ln(\delta)| = \ln(\frac{1}{\delta})$ and also $\frac{1}{1-\alpha} \geq 1$): $n \geq \sqrt{8}\ln(\frac{1}{\delta})\frac{1}{1-\alpha} \geq c_1 \ln(\frac{1}{\delta})$. So we are done.
In summary, by using the Chernoff bound and manipulating the equations, we've shown that there exists a constant c_1 (specifically $c_1 = \sqrt{8}$) such that, with probability at least $1-\delta$, a random leader sequence of length at least $c_1 \ln(\frac{1}{\delta})$ has a strict majority of honest leaders.

B. Given a leader sequence of length T, let X_i be the random variable representing whether the leader i is honest ($X_i = 1$) or Byzantine ($X_i = 0$). Furthermore, let $Y = \sum_{i=1}^{T} X_i$ represent the total number of honest leaders in the sequence. The goal is to show that the leader sequence is $c_2(\ln(\frac{1}{\delta}) + \ln(T))$-balanced, meaning that the difference between the number of honest and Byzantine leaders is bounded.

We want to show that:

$$P[|Y - (1-\alpha)T| > c_2(\ln(\frac{1}{\delta}) + \ln(T))] \leq \delta \tag{7}$$

By using the Chernoff bound, we can bound the probability that Y deviates significantly from its expected value:

$$P[|Y - \mathbb{E}[Y]| > t] \leq 2\exp(-\frac{t^2}{2\mathbb{E}[Y] + \frac{t}{3}}) \tag{8}$$

where t is a threshold that we will set later.
It is obvious that $\mathbb{E}[Y] = (1-\alpha)T$, as each leader is honest with probability $1-\alpha$. Let $t = c_2(\ln(\frac{1}{\delta}) + \ln(T))$. Substituting into the Chernoff bound formula suggests that:

$$P[|Y - (1-\alpha)T| > (c_2(\ln(\frac{1}{\delta}) + \ln(T)))] \leq 2\exp(-\frac{(c_2(\ln(\frac{1}{\delta}) + \ln(T)))^2}{2(1-\alpha)T + \frac{2}{3}c_2(\ln(\frac{1}{\delta}) + \ln(T))}) \tag{9}$$

By choosing c_2 such that $\frac{2}{3}c_2 \geq (1-\alpha)$ we can simplify the denominator of the exponential expression to: $2(1-\alpha)T + \frac{2}{3}c_2(\ln(\frac{1}{\delta}) + \ln(T)) \leq 2(1-\alpha)T + 2(1-\alpha)T = 4(1-\alpha)T$. By plugging this back into the bound, we get:

$$P[|Y - (1-\alpha)T| > (c_2(\ln(\frac{1}{\delta}) + \ln(T)))] \leq 2\exp(-\frac{(c_2(\ln(\frac{1}{\delta}) + \ln(T)))^2}{4(1-\alpha)T}) \tag{10}$$

Therefore, we need to find a c_2 such that the *R.H.S.* of the equation above is less than δ. So we must have:

$$2\exp(-\frac{(c_2(\ln(\frac{1}{\delta})+\ln(T)))^2}{4(1-\alpha)T}) \leq \delta \rightarrow c_2^2(\ln(\frac{1}{\delta})+\ln(T))^2 \geq \frac{4(1-\alpha)T\ln(\frac{1}{\delta})}{\ln(2)} \tag{11}$$

which suggests:

$$c_2(\ln(\frac{1}{\delta})+\ln(T)) \geq \sqrt{\frac{4(1-\alpha)T\ln(\frac{1}{\delta})}{\ln(2)}} \rightarrow c_2 \geq \sqrt{\frac{4(1-\alpha)\ln(\frac{1}{\delta})}{\ln(2)}} \geq \sqrt{\frac{4(1-\alpha)}{\ln(2)}} \tag{12}$$

In summary, by using the Union bound along with the Chernoff bound and manipulating the equations, we've shown that there exists a constant c_2 (specifically $c_2 = \sqrt{\frac{4(1-\alpha)}{\ln(2)}}$) such that, with probability at least $1-\delta$, a length-T leader sequence is $c_2(\ln(\frac{1}{\delta})+\ln(T))$-balanced.

C. We want to find the value of k (number of unconfirmed blocks at the end of the longest chain) such that, over the next $T = 1000$ blocks, the consistency of the blockchain (i.e., no blocks getting rolled back) is ensured with a probability of at least 90%.
In the context of the provided analysis, we are looking for a value of$k$ that guarantees the system to be $c_2(\ln(\frac{1}{\delta})+\ln(T))$-balanced with with $c_2 = 4(1-\alpha)\ln(2)$ and $\delta = 0.1$ (for a 90% confidence level).
The formula for k in this case is(given that $T = 1000, \delta = 0.1, \alpha = 0.4$ or equivalently 40% Byzantine nodes):

$$k = c_2(\ln(\frac{1}{\delta})+\ln(T)) = \sqrt{\frac{4(0.6)}{\ln(2)}}(\ln(10)+\ln(1000)) \tag{13}$$

After plugging in the values and calculating, you will get the value of k that ensures consistency with at least 90% confidence over the next 1000 blocks for the given parameters.

Problem 4

Problem 5

Firstly, we are going to state each theorem and then we will prove it:

A. **Theorem 1:** Let $G_1 \subseteq G_2 \subseteq ... \subseteq G_T$ denote a sequence of in-trees, with each in-tree G_i having one more block than the previous one G_{i-1}. If the common prefix property (with a given value of k) holds in each of $G_1, G_2, ..., G_T$, then:

$$B_k(G_1) \subseteq B_k(G_2) \subseteq ... \subseteq B_k(G_T) \tag{14}$$

Proof 1:

B. **Theorem 2:**

Proof 2:

C. **Theorem 3: Proof 3:**