Distributed Trust
Module 1 Exam

FE19B106 Prasanna Bartakke

1. Finding an adversarial strategy such that at the end of each day $i \leq b$, there will be at least 2 guilt-free friends such that one of them knows the rumor while the other does not.

Part 1

The adversary has the power to make any person guilty at any time. For the above condition, the adversary follows the following strategy:

On each day i, the rumor should be spread to a new person. The person who is responsible for spreading the rumor on day i, is made guilty after the first call.

The above strategy ensures that only one person can spread a rumor on each day, and only 1 new person gets to know about the rumor.

Since the adversary has the ability to make upto b people guilty, with the above strategy we can ensure that for each day $i \leq b$, there is one guilt free friend who knows the secret and at least one guilt-free friend who does not know the secret.

Part 2

Consistency

At the end of day $b+1$, either all guilt-free friends know the secret or none of the guilt-free nodes know the secret.

Assuming that the adversary follows the same strategy from part 1.
The adversary can either make the person guilty or decide to not make the person guilty.

① → When the adversary does not use his power.
If a person knows the secret and the person is guilt-free, he will tell the secret to all the remaining guilt-free nodes.
If there is no guilt-free person who knows the secret, all guilt-free people will not know the secret.
Thus, consistency is proved in this case

② → The adversary uses his power to make 1 friend guilty every day. The adversary can make upto b people guilty. This can happen till the end of the b^{th} day.
If the adversary does not follow this strategy on any day, the first case can be used to prove consistency.
On the $(b+1)^{th}$ day, the adversary cannot use his power if he has used his power on one person till now every day

Thus, we can use ① again to prove consistency.

We can summarise the proof as follows.
Case ① proves that if the adversary decides not to use his power on a particular day, depending on whether any person (guilt-free) knows the secret or not, all the guilt-free nodes will either know the secret or not know the secret at the end of the current day.

Case ② proves that due to the limit on the power of the adversary we reach case ① eventually on the $(b+1)^{th}$ day.

Thus, consistency is proved.

Now, assume that the adversary can follow any strategy. Case ① is still correct.
~~The adversary has to necessari~~ The maximum number of days the adversary can avoid reaching case ① due to the limit on its power is b days. Thus, irrespective of the strategy used by the adversary, we will reach case ① on or before the $(b+1)$ th day.

Thus, consistency is proved.

2. Streamlet scenarios

Part 1

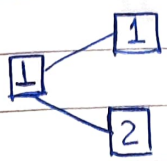
Two notarized chains,
1 - 1 - 3 - 5 and 1 - 2 - 4 - 6.

Initially, we start with the genesis block 1. In epoch 1, the leader of that epoch proposes the block [1]. All nodes receive the block and vote for it. Due to network delays, the votes are unable to reach to the nodes and thus the block is not notarized.

Now, in epoch 2, the leader proposes a block [2] that extends from the genesis block as it was not able to notarize the block proposed by the leader of epoch 1. The nodes vote for this block and as more than $2n/3$ votes are received for this block, [2] is notarized. This happens because all nodes feel that [2] is a valid block as the node sent by leader of epoch 1 is not notarized yet.

Now, the votes which were stuck due to the network delay arrive, and as more than $\frac{2n}{3}$ votes are received for the block sent by the leader of epoch 1, the block [1] is notarized.

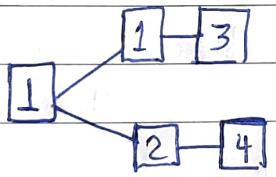
Following is the state of the chain



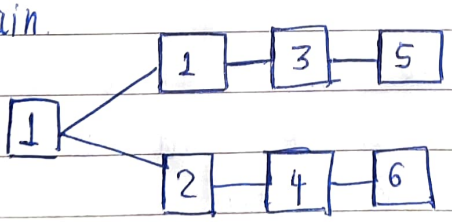
Now, in epoch 3, the leader can choose

to extend from one of the two longest notarized chains. Suppose the leader of epoch 3 decides to extend from block [1], and proposes its block [3]. All nodes vote for the block, but due to network delays, the votes are unable to reach to other nodes, and the block [3] is not notarized.

Now, in epoch 4, the leader sees the same state of the chain as seen by the leader of the 3rd epoch. It decides to extend from the block [2], and proposes its block [4]. All nodes vote for it and it gets notarized. Now, the votes for block [3] arrive and it too gets notarized.
Following is the state of the chain:



Now, in epoch 5 and 6 the same thing happens, resulting in the following state of the chain.



Thus, the scenario 1's chain is POSSIBLE

Part 2

1 - 3 - 4 - 5 and 1 - 1 - 2 - 4 - 5 - 6

↳ B1 ↳ B2

From the uniqueness lemma we know:
Suppose $f < \frac{n}{3}$. Then for epoch e, there can be at most one notarized block with the epoch e in honest view.

From the two chains we can see that there are 2 blocks B1, B2 with epoch = 4. This validates the above lemma for the streamlit protocol.

Thus, scenario 2's chains are NOT POSSIBLE.

Part 3

1 - 3 - 4 - 5 and 1 - 1 - 2 - 7 - 8 - 9

From the consistency theorem of the streamlit protocol we know:
If some honest node sees a notarized chain with three adjacent blocks B_0, B_1, B_2 with consecutive epoch numbers e, e+1 and e+2, then there cannot be a conflicting block $B \neq B1$ that also gets notarized in honest view at the same height as B1.

Thus, we can conclude that once 1-3-4-5 is notarized, the chain 1-1-2 cannot grow further.

Thus, scenario 3's chains are NOT POSSIBLE.

3. Streamlet protocol with $f < \frac{n}{4}$.

We can get the minimum number of votes required from the proof of the uniqueness lemma.

Suppose two blocks B and B', both of epoch e get notarized in honest view. At least x nodes (set S) signed block B, and at least x nodes (set S') signed block B'. Since we have n nodes in total and $S \cap S'$ can be ~~less than~~ at least $\frac{n}{4}$, we get the following inequality,

$$n = x + x - \{S \cap S'\}$$

$$\{S + S'\} = 2x - n$$

$$\therefore 2x - n \geq \frac{n}{4}$$

$$\therefore x \geq \frac{5n}{8}$$

Thus at least $5n/8$ votes are needed to notarize a block.

As uniqueness lemma holds for number of votes required to notarize $\geq \frac{5n}{8}$, it can be used to prove consistency.
The consistency proof discussed in class can be used with the updated def^n of uniqueness as discussed above.

4. Three nodes cannot reach byzantine agreement with all-same validity if one node among them is byzantine.

The statement given is true.

The following line in the proof:
"a correct node must decide on its own value if another node supports that value"
is incorrect.

A correct node must decide on its own value only if the another node which supports that value is a correct node.

The byzantine node is able to fool the correct nodes as they do not check if the node is byzantine.
Thus, although this proof proves the correct statement, it is not complete.

We need to look at all the 3 cases as in the FLP proof.

5. Part 1, Part 2

To find the smallest number of people, s, who know the secret initially.

Case I: $s < k$

If $s < k$, on day 1 they can spread the secret to $2s$ people. The adversary can make k people forget the secret. Thus, at the end of day 1, $2s - k$ people know the secret.

As $s < k$, $2s - k < s$.

That is the number of people who know the secret is decreasing. Thus, this case is not valid.

Case II: $s = k$

At the end of day 1, the number of people who know the secret is $2s - k = k$.

As the number of people who know the secret is constant (k) and $k < \frac{n}{2}$, this case is not valid.

Case III: $s = k + 1$.

At the end of day 1, the number of people who know the secret is $2s - k = k + 2$.

Thus, at the end of the i^{th} day the number of people who know the secret is $\min(n, k + 2^i)$

Number of days required to reach collective memory = d

$$k + 2^d \geq \frac{n}{2}$$

$$\therefore 2^d \geq \left(\frac{n}{2} - k\right)$$

$$\therefore d \geq \log_2\left(\frac{n}{2} - k\right)$$

$$\therefore d = \text{ceil}\left[\log_2\left(\frac{n}{2} - k\right)\right]$$

Part 1: smallest number of people who should initially know the secret $s = k + 1$.

Part 2: If $s = k+1$, In the worst case it will take $\text{ceil}\left[\log_2\left(\frac{n}{2} - k\right)\right]$ days to reach collective memory.

Part 3:
For collective memory, the initial value of s should be such that the people who know the secret should increase over time.
Thus, for the given randomized strategy, we need to find the value of s such that the probability of the number of people who know the secret is more than s is greater than $1 - 1/n$.

total number of ways to select next round people = $n C_s$

number of ways to select next round people such that after the adversary uses its power, >s people know the secret

$$= {}^{s}C_0 \; {}^{n-s}C_s + {}^{s}C_1 \; {}^{n-s}C_{s-1} + \dots {}^{s}C_{s-k-1} \; {}^{n-s}C_{k+1}$$

probability of reaching collective memory $> 1 - \frac{1}{n}$

$$\therefore \frac{\sum_{i=0}^{k-1} {}^{s}C_i \; {}^{n-s}C_{s-i}}{{}^{n}C_s} > 1 - \frac{1}{n}$$

$k = n/10$

$$\therefore \frac{\sum_{i=0}^{(\frac{n}{10})-1} {}^{s}C_i \; {}^{n-s}C_{s-i}}{{}^{n}C_s} > 1 - \frac{1}{n}$$

solve the inequality to get the value of s