RUNI: Blockchains and Cryptocurrencies

Homework 3

Fall Semester 2022-23 TASHPAG

Submitted by: **Yarden Fogel (yarden.fogel@post.runi.ac.il)**
Date: January 25, 2023

Question 1A: Cryptographic Sortition - Part 1

Claim. *For every constant $q < \frac{1}{2}$ and every corruption strategy for the adversary, Pr[$\boldsymbol{bad}_{k,n}$] =* $2^{-\Omega(k)}$

Assumptions:

- Since q is constant, $\Pr[\mathbf{bad}_{k,n}]$ can depend on q; however, it cannot be a function of n
- **Chernoff Bound:** If X_1,...,X_m are independent random variables taking values in $0, 1$. Let X denote their sum and let $\mu = E[X]$ denote the sum's expected value. Then for any $\delta \in [0, 1]$, Pr $[X \leq (1 - \delta)\mu] \leq e^{\frac{-\delta^2\mu}{2}}$

Proof. $(C_0, ...C_{k-1})$ is a committee of size k out of a total of n miners. $\mathbf{bad}_{k,n}$ is the event where $> \frac{k}{2}$ of the chosen committee members are corrupt. Since each miner has the same constant probability of being corrupt, denoted q, which is the fraction of all the n total miners that are corrupted, the probability distribution of the *i.i.d.* random variable X_i takes the form of a Binomial distribution, or a series of Bernouli trials.

The variable X_i takes on values of either 1 if corrupt, with probability of q, or 0 if honest, with probability of $(1-q)$. X_i denotes miner j in committee index i , i.e. $C_i = j$ being either corrupt $X_i = 1$ or honest $X_i = 0$.

$\forall i \in [0, k-1], X$ denotes the sum $\Sigma_{i=0}^{k-1} \cdot X_i$, or the set of corrupt miners out of the total k committee members. It then follows that $\mu = E[X] = E[X_0 + ... + X_{k-1}] = k \cdot q$, by virtue of the given parameters μ and σ for a binomial distribution, as well as linearity of expectations.

We could use various manipulations for assumptions for δ, but for the sake of simplicity, let $\delta = (1 - \frac{1}{2q})$, and doing so equates $(1-\delta)\mu$ to $\frac{k}{2} \longrightarrow since(1-(1-\frac{1}{2q})\cdot kq = \frac{kq}{2q} = \frac{k}{2}$. This neatly aligns with our constraint for $\mathbf{bad}_{k,n}$, such that the $\Pr[\mathbf{bad}_{k,n}] = \Pr[X \leq (1-\delta)\mu]$, allowing us to use the Chernoff Bound in our proof.

Therefore, $\Pr[\mathbf{bad}_{k,n}]= \Pr[X > \frac{k}{2}] = \Pr[X \leq (1-\delta)\mu] \leq \exp\frac{-\delta^2\mu}{2} = e^{\frac{-(1-\frac{1}{2q})^2\cdot kq}{2}} = e^{\frac{-k\cdot(1-\frac{1}{2q})^2\cdot q}{2}}$

Simplifying 'everything but the k' in the exponent to some constant c, since q is constant, we can simplify that expression to $e^{-k\cdot c}$ or rather $e^{-c\cdot k}$. So we have $\Pr[\mathbf{bad}_{k,n}] \leq e^{-c\cdot k}$ which by the inequality of $2 < e$ and $2^{-x} \geq e^{-x}$, $\Pr[\mathbf{bad}_{k,n}] \leq e^{-c(k)} \leq 2^{-c(k)} = 2^{-\Omega(k)}$, whereby the constant c with all the q's in it $= \Omega$......... *Q.E.D.*

□

Compiled with LaTeX on January 25, 2023.

Question 1B: Cryptographic Sortition - Part 2

Claim. *Sampling committee members uniformily is not sufficient by itself*

Explicit Randomized Algorithm $Sample(k, n)$ **Satisfying:**

- for all $j < n$, $i < k$: $Pr[C_i = j] = \frac{1}{n}$ i.e. every committee member is uniformly selected, but
- for all $q < \frac{1}{2}$ and $k > 0$, there exists an adversary that corrupts $q \cdot n$ miners such that $Pr[bad_{k,n}] \geq q$
- **Bonus:** Algorithm satisfies $Pr[bad_{k,n}] \geq 2q$

Proof. The algorithm is as follows below, which demonstrates clearly that uniform selection of committee members is not sufficient to guarantee avoiding $\mathbf{bad}_{k,n}$. One salient conclusion from the below is that introducing some degree of dependency between the selections (and within the context of uniform selection) facilitates the selection being increasingly $\mathbf{bad}_{k,n}$.

Algorithm 1 Explicit Randomized Algorithm - Sample (k, n)

```
1. Randomly divide the $n$ total miners into two equal groups, denoted $n_1$ and $n_2$
2. While $len(C) < k$ do:
3.     randomly choose one of the two groups
4.     from the chosen group, uniformly randomly select a miner to the committee, C.append(miner)
5.     If miner selected is corrupt, continue randomly selecting from the same group
6.     Else if selected miner is honest, circle back to step 3 and repeat
```

Satisfying All 2.5 Conditions:

- **Uniform selection of committee members:** The total set of miners n is randomly divided into 2 equal subgroups. The groups are then randomly selected, and within the randomly selected groups, the miners are selected at random, clearly satisfying the random uniform selection condition.
- **Pr[bad$_{k,n}$] $\geq q$:** To prove the second condition that an adversary corrupting $q \cdot n$ miners results in Pr[bad$_{k,n}$] $\geq q$ $\forall q < \frac{1}{2}$ and $k > 0$, and also satisfies the bonus goal that Pr[bad$_{k,n}$] $\geq 2q$, let's consider the two extreme scenarios for our random group division and resulting allocation of corrupted miners...
- **Scenario 1 - Perfectly even split of corrupted miners between** $n_1 and n_2$ **subgroups:** Given the uniform random selection process, the algorithm will oscillate between the groups, and over many trials, will converge to an expectation of exactly $q \cdot k$ corrupt miners in the committee, as in Part 1 / Question 1A above, and Pr[bad$_{k,n}$] $= q$. This still satisfies this second condition, but note of the many possible random splits between the two subgroups, this is really the worst-case scenario for the adversary.

◦ **Scenario 2 - Perfectly *un*even split of corrupted miners between $n_1 and n_2$ subgroups, with all the corrupted miners being in n_1:** In this other extreme scenario for the corrupted-miner split between the two subgroups, once n_1 is randomly selected, the algorithm steers it to continue going 'back to the well' and potentially ALL of the committee members will be corrupt, with $\Pr[\text{bad}_{k,n}]$ potentially **FAR** exceeding $2q$ (unless of course q is juuuust under $\frac{1}{2}$). In fact, any split that is different than 50-50 between the subgroups will begin to diverge above q for $\Pr[\text{bad}_{k,n}]$, and increasingly so as the split gets more and more lopsided, with the extreme all and none scenario described above as the upper bound.

As the conditions have clearly been satisfied, providing a uniform random selection of committee members, guaranteeing a $\Pr[\text{bad}_{k,n}]$, in most cases strictly $> q$ and in many cases $\geq 2q$, it's thus clearly proven that sampling committee members uniformly is itself not sufficient to ensure a $\mathbf{good}_{k,n}$ outcome for the committee's composition and integrity.

Q.E.D.

□

Compiled with LaTeX on January 25, 2023.