Chernoff Bounds and Bitcoin Orphaned Blocks

Adam Fasulo, Christopher Jarek, Evelyn Sanchez

April 3, 2025

1 Bounding the Probability of Deviation Below the Mean

Objective

We aim to derive a lower tail Chernoff bound for the sum of independent Bernoulli random variables. Specifically for $X = \sum_{i=1}^{n} X_i$ where $X_i \sim \text{Bernoulli}(p_i)$ are independent with $\mathbb{E}[X] = \mu = \sum_{i=1}^{n} p_i$ we want to bound,

$$\Pr(X \leq (1-\delta)\mu) \quad \text{for} \quad 0 \leq \delta \leq 1$$

Recap of Chernoff Bound for Upper Deviation

The upper tail Chernoff bound is well known,

$$\Pr(X \geq (1+\delta)\mu) \leq \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu}$$

This bound is derived using the moment generating function (MGF) and Markov's inequality.

Lower Tail Chernoff Bound

We now derive the analogous bound for the lower tail.

1 Moment Generating Function (MGF) Approach

For any $t > 0$ by Markov's inequality,

$$\Pr(X \leq (1-\delta)\mu) = \Pr(e^{-tX} \geq e^{-t(1-\delta)\mu}) \leq \frac{\mathbb{E}[e^{-tX}]}{e^{-t(1-\delta)\mu}}$$

2 MGF of X

Since the X_i are independent,

$$\mathbb{E}[e^{-tX}] = \prod_{i=1}^{n} \mathbb{E}[e^{-tX_i}] = \prod_{i=1}^{n} \left(1 - p_i + p_i e^{-t}\right)$$

Using the inequality $1 + x \le e^x$ for $x = p_i(e^{-t} - 1)$ we get,

$$\mathbb{E}[e^{-tX}] \le \prod_{i=1}^{n} e^{p_i(e^{-t}-1)} = e^{\mu(e^{-t}-1)}$$

3 Optimizing t

Substitute the MGF bound into the inequality,

$$\Pr(X \le (1-\delta)\mu) \le \frac{e^{\mu(e^{-t}-1)}}{e^{-t(1-\delta)\mu}} = e^{\mu(e^{-t}-1+t(1-\delta))}$$

To minimize the exponent we set the derivative with respect to t to zero,

$$\frac{d}{dt}\left[e^{-t} - 1 + t(1-\delta)\right] = -e^{-t} + (1-\delta) = 0 \implies e^{-t} = 1 - \delta$$

Solving for t,

$$t = -\ln(1-\delta)$$

Substituting back,

$$e^{-t} - 1 + t(1-\delta) = (1-\delta) - 1 - (1-\delta)\ln(1-\delta) = -\delta - (1-\delta)\ln(1-\delta)$$

Thus the bound becomes,

$$\Pr(X \le (1-\delta)\mu) \le e^{\mu(-\delta-(1-\delta)\ln(1-\delta))} = \left(e^{-\delta}(1-\delta)^{1-\delta}\right)^{\mu}$$

Simplification for Small δ

For $0 \le \delta \le 1$ we can approximate $\ln(1-\delta)$ using its Taylor series,

$$\ln(1-\delta) = -\delta - \frac{\delta^2}{2} - \frac{\delta^3}{3} - \cdots$$

Keeping terms up to δ^2,

$$-\delta - (1-\delta)\ln(1-\delta) \approx -\delta - (1-\delta)\left(-\delta - \frac{\delta^2}{2}\right) = -\delta + \delta + \frac{\delta^2}{2} - \delta^2 - \frac{\delta^3}{2} \approx -\frac{\delta^2}{2}$$

Thus for small δ,

$$\Pr(X \le (1-\delta)\mu) \le e^{-\mu\delta^2/2}$$

2 Proving the Given Chernoff Bounds Using Lemma 3

Given Lemma 3

For all $\delta > 0$,

$$\Pr(X \geq (1+\delta)\mu) \leq e^{-\mu(\delta-(1+\delta)\ln(1+\delta))}$$

and for $0 \leq \delta \leq 1$,

$$\Pr(X \leq (1-\delta)\mu) \leq e^{-\mu(\delta+(1-\delta)\ln(1-\delta))}$$

Goal

Show for $0 \leq \delta \leq 1$,

1. $\Pr(X \leq (1-\delta)\mu) \leq e^{-\delta^2\mu/2}$
2. $\Pr(X \geq (1+\delta)\mu) \leq e^{-\delta^2\mu/3}$

Proof for Lower Tail (1)

From Problem 1 we have,

$$\delta + (1-\delta)\ln(1-\delta) \geq \frac{\delta^2}{2}$$

Thus,

$$\Pr(X \leq (1-\delta)\mu) \leq e^{-\mu\delta^2/2}$$

Proof for Upper Tail (2)

We need to show,

$$\delta - (1+\delta)\ln(1+\delta) \geq \frac{\delta^2}{3}$$

Consider the function,

$$f(\delta) = \delta - (1+\delta)\ln(1+\delta) - \frac{\delta^2}{3}$$

We analyze $f(\delta)$ for $\delta \in [0,1]$

At $\delta = 0$,

$$f(0) = 0 - 1 \cdot 0 - 0 = 0$$

For $\delta \in (0,1]$ we use the Taylor expansion of $\ln(1+\delta)$,

$$\ln(1+\delta) = \delta - \frac{\delta^2}{2} + \frac{\delta^3}{3} - \cdots$$

Substituting,

$$f(\delta) \approx \delta - (1+\delta)\left(\delta - \frac{\delta^2}{2} + \frac{\delta^3}{3}\right) - \frac{\delta^2}{3}$$

Expanding and simplifying,

$$f(\delta) \approx \delta - \delta + \frac{\delta^2}{2} - \frac{\delta^3}{3} - \delta^2 + \frac{\delta^3}{2} - \frac{\delta^4}{3} - \frac{\delta^2}{3} = -\frac{\delta^2}{2} + \frac{\delta^3}{6} - \frac{\delta^4}{3}$$

For small δ the dominant term is $-\frac{\delta^2}{2}$ but this contradicts our goal. Instead we use an alternative approach.

From Lemma 3 we have,

$$\delta - (1+\delta)\ln(1+\delta) \geq \frac{\delta^2}{2} - \frac{\delta^3}{6}$$

We need to show,

$$\frac{\delta^2}{2} - \frac{\delta^3}{6} \geq \frac{\delta^2}{3}$$

Simplifying,

$$\frac{1}{2} - \frac{\delta}{6} \geq \frac{1}{3} \implies \frac{1}{6} \geq \frac{\delta}{6} \implies \delta \leq 1$$

Thus for $\delta \in [0,1]$,

$$\Pr(X \geq (1+\delta)\mu) \leq e^{-\mu\delta^2/3}$$

3 Orphaned Blocks in Bitcoin Consensus

Model Recap

In Bitcoin's consensus protocol,

- Good nodes produce blocks at total rate λ
- Adversarial nodes produce blocks at total rate β
- Orphaned blocks are those not included in the longest chain

Expected Number of Orphaned Blocks

Orphaned blocks occur when two blocks are mined within time Δ of each other causing a temporary fork.

1 Rate of Orphaned Blocks

The probability that a block is orphaned is the probability that another block (good or bad) is mined within Δ time. The total mining rate is $\lambda + \beta$. The probability of at least one block in Δ time is,

$$p_{\text{orphan}} \approx 1 - e^{-(\lambda+\beta)\Delta} \approx (\lambda+\beta)\Delta \quad \text{(for small } (\lambda+\beta)\Delta\text{)}$$

Thus the expected number of orphaned blocks in time T is,

$$\mathbb{E}[\text{Orphaned blocks}] = \lambda \cdot (\lambda+\beta)\Delta \cdot T$$

2 Chernoff Bounds for Deviation

Let X be the number of orphaned blocks. Applying Chernoff bounds,

- For deviation above the mean,

$$\Pr(X \geq (1+\delta)\mathbb{E}[X]) \leq e^{-\frac{\delta^2 \mathbb{E}[X]}{3}}$$

- For deviation below the mean,

$$\Pr(X \leq (1-\delta)\mathbb{E}[X]) \leq e^{-\frac{\delta^2 \mathbb{E}[X]}{2}}$$

4 Summing $p_i p_j$ and Showing $\sum_{i,j \in G} p_i p_j \leq \alpha^2$

Objective

Show that for $\alpha = \sum_{i \in G} p_i$,

$$\sum_{i,j \in G} p_i p_j \leq \alpha^2$$

Solution

The sum of pairwise products is,

$$\sum_{i,j \in G} p_i p_j = \left(\sum_{i \in G} p_i \right)^2 = \alpha^2$$

This holds because,

$$\left(\sum_{i \in G} p_i \right)^2 = \sum_{i \in G} p_i^2 + 2 \sum_{i<j} p_i p_j \geq \sum_{i,j \in G} p_i p_j$$

Equality occurs when all p_i are zero except one but generally the sum of products equals the square of the sum.

Let,

$$\sum_{i \in G} \alpha_i = \vec{i}, \sum_{j \in G} \alpha_j = \vec{j}$$

$$\sum_{i \in G} \sum_{j \in G} \alpha_i \alpha_j \leq (\sum_{i \in G} \alpha_i)^2$$

Then the above inequality becomes:

$$\vec{i} \cdot \vec{j} \leq \vec{i}^2$$

Expanding the right side gives us:

$$||\vec{i}||||\vec{j}||cos\theta \leq \vec{i}^2$$

Considering $cos\theta \leq 0$, the inequality is true.

Problem 5

Click here Proposal