CS 491/591 Blockchains, HW 3

Prof. Jared Saia, University of New Mexico

1. At the end of the proof from the Chernoff Bound Lecture, I write "using a symmetric argument, we can bound the probability of deviation below the mean." Give a detailed proof for how to bound this probability, i.e. bound $Pr(X \leq (1-\delta)\mu)$.

2. Now use the above result, along with Lemma 3 to prove the following version of Chernoff bounds that are used in the proof of Theorem 1. For all $0 \leq \delta \leq 1$:

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

   Hint: Set up a target inequality, take the log of both sides, then use calculus.

3. Using the model and algorithm from the Bitcoin Consensus Lecture, calculate (1) the expected number of orphaned blocks from good nodes in Bitcoin Consensus; and (2) use Chernoff bounds to bound deviation from that expectation. Recall that an orphaned block is one that does not eventually wind up in the longest chain.

4. Recall the question from Bitcoin Consensus that asks: Do you see why $\sum_{i,j \in G; i \neq j} p_i p_j \leq \alpha^2$? Prove that this is the case.

5. In this problem, you will (1) write up a proposal for your class project and post it (or a link to it) on the Piazza forum; and (2) do a 5 minute in-class presentation on your proposal. Remember that you are encouraged to work in groups of 2 or 3 on the proposal.

   Your proposal should include the following information, and should be no more than 2 pages, not including bibliography. It should clearly address the following points.

(a) **Research Goal.** What is the key question that you plan to answer in your project or the key goal you hope to achieve. Describe this concisely in a paragraph or two.

(b) **Motivation.** Why is this question important to answer or goal important to achieve?

(c) **Related Work.** List 5 or more papers closely related to your proposal, and give a 1-2 line summary of each. (Google scholar can help find the most important papers since it orders by citation counts).

(d) **Novelty.** What are the new techniques you plan to use, or studies you plan to do? What are the related research papers, and why don't they answer your question?

(e) **Research Plan** List what you need to do and organize it in a timeline. List what you plan to have accomplished by the first checkpoint (1 month)

(f) **Division of Labor.** Who will be working on this proposal and how will tasks be divided up?