Advanced Proof-Systems | Winter 2024

Problem Set 1

Lecturer: Ron Rothblum | Due: 7/2/2024

1 Chernoff Bound and Sequential Repetition

The Chernoff bound is a quantitative version of the law of large numbers. It basically says that the sum of independent random variables is highly concentrated around the expectation.

In this exercise you will prove the Chernoff bound. We start by proving a quantitatively much weaker bound, called Markov's inequality, which is applicable to any non-negative random variable (in contrast to Chernoff which is applicable only to a sum of independent RVs).

1.1 Markov's Inequality

Remark 1.1. *It is not too hard to convince yourself that the probability that a non-negative random variable is more than double its expectation can be at most* $1/2$ *(otherwise the expectation would be larger!). Markov's inequality is a simple generalization of this fact.*

Let X be a random variable taking only non-negative values. Let $\mu = \mathrm{E}[X]$. Show that for every $\alpha > 1$,

$$\Pr[X > \alpha\mu] < 1/\alpha.$$

1.2 Chernoff Bound

Let $X_1, \ldots, X_n \sim \{0,1\}$ be i.i.d. (independently and identically distributed) random variables, where $X_i = 1$ with probability p and $X_i = 0$ with probability $1-p$. Let $X = \frac{1}{n}\sum_{i=1}^{n} X_i$. Prove that for every $\varepsilon \in (0, p]$ it holds that $\Pr\left[|X - p| > \varepsilon\right] < 2^{-\Omega(\varepsilon^2 n)}$.

Guideline 1.2. *We will bound only* $\Pr\left[X - p > \varepsilon\right]$ *and the other direction can be bounded similarly.*

1. *First, define auxiliary random variables* $\bar{X}_i = X_i - E[X_i] = X_i - p$. *Also define* $\bar{X} = \frac{1}{n}\sum_{i\in[n]} \bar{X}_i$. *With this terminology, we need to upper bound* $\Pr[\bar{X} > \varepsilon]$. *(The reason for doing so is that it is more convenient to work with RVs whose expectation is* 0*.)*

2. *Observe that to bound the latter, it suffices to bound*

$$\Pr\left[e^{\lambda\cdot\bar{X}} > e^{\lambda\cdot\varepsilon}\right], \tag{1}$$

   for some $\lambda > 0$ *(we will choose* λ *later to optimize the bound, for now it can be safely ignored).*

3. *Use Markov's inequality to obtain an upper bound on Eq. (1) involving the expression* $\mathrm{E}[e^{\lambda\cdot\bar{X}}]$.

4. *Use independence of the random variables to upper bound* $\mathrm{E}[e^{\lambda \cdot \bar{X}}]$. *Specifically, show that* $\mathrm{E}[e^{\lambda \cdot \bar{X}}] \leq e^{\frac{\lambda^2}{n} p(1-p)}$.

   Hint: *express* $\bar{X}$ *as the sum of the* $\bar{X}_i$*'s. Then, use the independence of the* $\bar{X}_i$*'s and the fact that* $e^z \leq 1 + z + z^2$ *for all* $|z| \leq 1$ *(which follows from the Taylor series of* e^z*).*

5. *Set* $\lambda = \frac{n \cdot \varepsilon}{2p(1-p)}$ *to obtain an upper bound of* $e^{-\frac{\varepsilon^2}{4p(1-p)} \cdot n} = 2^{-\Omega(\varepsilon^2 \cdot n)}$ *on the probability of the bad event.*

1.3 Statistics Fun

The world's population is about 8 billion people. We would like to figure out what is the percentage of people who prefer cats to dogs. Suppose[1] that you can sample uniformly at random people for a survey. How many people would you need to participate in the survey to get an answer that with 99% probability is at most 5% off from the truth?

Remark 1.3. *No need to submit this problem - it's just intended to help digest what the Chernoff bound says (and for fun).*

1.4 Sequential Repetition of Interactive Proofs

Remark 1.4. *In class we showed that sequential repetition reduces the soundness error when we have* perfect completeness. *In this question you are asked to extend the proof to the case that we start with completeness and soundness errors of* 1/3.

Let Π be an interactive proof with completeness and soundness errors 1/3. Show that if we repeat the protocol t times (where the verifier rules by majority), then we get an interactive proof with completeness and soundness errors $2^{-\Omega(t)}$.

2 Perfect Soundness

Let $\mathsf{IP}^{\mathsf{ps}}$ be the class of interactive proofs in which the soundness error is 0 (and completeness error is 1/3 as usual). That is, for every $x \notin L$ and prover strategy P^*, the verifier accepts with probability 0 when interacting with P^*. Prove that $\mathsf{IP}^{\mathsf{ps}} = \mathsf{NP}$.

Remark 2.1. *The fact that* $\mathsf{IP}^{\mathsf{ps}} = \mathsf{NP}$ *means that we essentially gain nothing by introducing randomness and interaction, if we insist on having perfect soundness.*

In contrast, in the tutorial you will see that the class of interactive proofs in which the completeness error *is* 0 *(and soundness error is* 1/3*) is equal to* IP.

3 Naive Set Lower Bound

Recall that the set lower bound protocol that we saw in class allows the prover to convince the verifier that a set $S \subseteq U$ is somewhat large. In particular if $|S| > t$ there is a strategy that makes the verifier accept with probability 0.99 and if $|S| < t/100$ then any prover strategy will make it accept with probability at most 0.01.

[1] And this is a BIG assumption.

Consider the following much simpler protocol (which doesn't even involve the prover): the verifier chooses k random elements $u_1, \ldots, u_k \in U$ (with repetition), where k is a parameter to be determined below. It then checks what fraction of these elements fall in the set S. If the fraction is more than $\left(\frac{t}{|U|}\right)/2$ then the verifier accepts and otherwise it rejects.

1. How large does k need to be to guarantee the same properties as the set lower bound protocol? (i.e., if $|S| \geq t$ the verifier accepts with probability 0.99 and if $|S| \leq t/100$ it accepts with probability 0.01).

   Hint: Use the Chernoff Bound.

2. Explain why we cannot replace the set lower bound from class with this simple protocol (in the transformation of private-coin interactive proofs into public-coin).

4 Matrix Multiplication

This problem focuses on the algorithmic task, given matrices $A, B \in \mathbb{F}^{n \times n}$, where $\mathbb{F}$ is some finite field, to compute their matrix product $A \cdot B$.

4.1 Naive Algorithm

Describe an $O(n^3)$ time algorithm that computes matrix multiplication. You may assume that field operations can be done at unit cost.

Remark 4.1 (Historical Context)**.** *Given the above, the complexity of matrix multiplication is between $O(n^3)$ and $\Omega(n^2)$ (the lower bound comes from the fact that it takes $\Omega(n^2)$ time to even just print the solution).*

In a groundbreaking result in 1969, Strassen famously showed a time $O(n^{2.81})$ algorithm for this problem. This has since been improved and the world record (from October 2022) is $O(n^{2.37188})$.

In the following problem you will show that in contrast to *computing* matrix multiplication, verifying a given solution can be done (easily) in $O(n^2)$ time. To do so we'll first establish the following important fact:

4.2 Random Subset Sum Principle

Let $x \in \mathbb{F}^n$ be a non-zero vector. Show that $\Pr_{y \in \mathbb{F}^n}\left[\langle x, y\rangle = 0\right] = 1/|\mathbb{F}|$, where $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$ denotes the inner product of the two vectors.

4.3 Randomized Verification of Matrix Multiplication

Describe a randomized $O(n^2)$ time algorithm that given matrices $A, B, C \in \mathbb{F}^n$ outputs 1 with probability 1 if $C = A \cdot B$ and outputs 0 with probability at least $1/2$ if $C \neq A \cdot B$.

Guideline 4.2. *Choose a random vector x and compare $(A \cdot B) \cdot x$ vs. $C \cdot x$.*