Problem Set 6 CS265, Fall 2020

Due: October 30 (Friday) at 23:59 (Pacific Time)

Please follow the homework policies on the course website.

---

1. **(4 pt.) [Furthering the second moment method]**

   In class, we saw the second moment method to show that a random variable with large expectation and small variance must be non-zero with good probability. Formally, we saw that for a non-negative random variable X,

   $$\Pr[X = 0] \leq \frac{\mathrm{Var}[X]}{(\mathrm{E}[X])^2}. \tag{1}$$

   While this is often very useful, it does not let us reason about the probability of X being something small but non-zero. In this question, you will prove a similar inequality that **does** let us do such a thing.

   Prove that for a non-negative random variable X and any $0 < t < 1$,

   $$\Pr[X \geq t \cdot \mathrm{E}[X]] \geq (1-t)^2 \frac{(\mathrm{E}[X])^2}{\mathrm{E}[X^2]}. \tag{2}$$

   [**HINT:** *Write* X *as* $X \cdot 1_{\{X < t \cdot E[X]\}} + X \cdot 1_{\{X \geq t \cdot E[X]\}}$. *Use linearity of expectation to compute* $E[X]$ *and use the Cauchy-Schwarz inequality to bound the term* $E[X \cdot 1_{\{X \geq t \cdot E[X]\}}]$.]

   Note: By simple rearrangements of (2), one can observe[1] that

   $$\Pr[X < t \cdot \mathrm{E}[X]] \leq \frac{\mathrm{Var}[X] + (1-(1-t)^2)(\mathrm{E}[X])^2}{\mathrm{E}[X^2]} \leq \frac{\mathrm{Var}[X]}{(\mathrm{E}[X^2])} + (1-(1-t)^2). \tag{3}$$

2. **(5 pt.) [How far do we get in life by walking aimlessly?]**

   Consider an n-step random walk on the integers. That is, let $S_n = X_1 + X_2 + ... + X_n$, where each X_i is a uniformly random $\{+1, -1\}-$valued random variable and represents a random step either to the right or the left on the number line. Think of the walker as having started at the origin of the number line (i.e. 0). Thus, S_n tracks the location of the walker after n steps. We want to understand the typical behaviour of such a random walk: how far does this walk typically get from it's starting spot at 0?

   (a) **(1 pt.)** Show that there exist two constants $0 < c_u$ and $0 < p_u < 1$ such that

   $$\Pr[|S_n - 0| \geq c_u\sqrt{n}] \leq p_u.$$

   That is, the probability that "the distance of the random walk's location from its starting spot after n steps grows faster than $\Theta(\sqrt{n})$" is bounded away from 1.

[1] There is no question you need to answer about this rearrangement. Simply observe this and try to understand how it compares to the inequality (1) from class.

(b) **(4 pt.)** Show that there exist two constants $0 < c_\ell$ and $0 < p_\ell < 1$ such that

$$\Pr[|S_n - 0| < c_\ell \sqrt{n}] \leq p_\ell.$$

That is, the probability that "the distance of the random walk's location from its starting spot after n steps grows slower than $\Theta(\sqrt{n})$" is bounded away from 1.

[**HINT:** *$|S_n - 0| < c_\ell \sqrt{n}$ is equivalent to $S_n^2 < c_\ell^2 n$. We have learnt how to show the probability of non-negative random variables being too small is small in Question 1. You can use results from Question 1 even if you couldn't get it.*]

[**HINT:** *Even though this question looks like it should be a Markov chain problem, remember that this week's HW is on Classes 11 and 12. (Next week's HW will cover Markov chains!)*]

3. **(7 pt.) [On the existence of good error correcting codes]**

Let $H(p) := p \log_2(\frac{1}{p}) + (1-p)\log_2(\frac{1}{1-p})$ for $0 \leq p \leq 1$ denote the binary entropy function[2]. Further define the Hamming distance between two binary strings $x, y \in \{0,1\}^n$ as the number of coordinates at which they differ $d(x,y) := \sum_{i=1}^{n} 1_{x(i) \neq y(i)}$.

FACT: *For $\delta \in (0, \frac{1}{2})$, the volume of a Hamming ball of radius δn around any point $x \in \{0,1\}^n$ is $2^{nH(\delta) \pm o(n)}$. That is,*

$$|y \in \{0,1\}^n : d(x,y) \leq \delta n| = 2^{nH(\delta) \pm o(n)}.$$

It is a major open question in the theory of *error correcting codes* whether, for all large enough n, there exists some constant $0 < \delta < 1/2$ and set $S \subseteq \{0,1\}^n$ so that

- $|S| \geq 2^{(1-H(\delta)+0.001)n}$ and
- $\forall x, y \in S$, we have $d(x,y) > \delta n$.

(But you don't need to know anything about error correcting codes to do this problem).

(a) **(2 pt.)** Your friend has just learnt the LLL and they think they can show the existence of such a set. Their strategy is the following:

i. Let $S \subseteq \{0,1\}^n$ be a random set where each $x \in \{0,1\}^n$ is included independently with probability $2^{-n(H(\delta)-0.001)+1}$ (we choose δ with $H(\delta) > 0.001$ and assume that n is sufficiently large so that the probability is less than 1). Then $\mathbb{E}|S| = 2^{(1-H(\delta)+0.001)n+1}$, and by a Chernoff bound $|S|$ is at least $\mathbb{E}|S|/2 = 2^{(1-H(\delta)+0.001)n}$ with overwhelming probability.

ii. For any $x, y \in \{0,1\}^n$ such that $d(x,y) \leq \delta n$, let A_{xy} denote the bad event that both x and y are contained in S. Clearly, $\Pr[A_{xy}] = 2^{-2n(H(\delta)-0.001)+2}$. Then we can use the LLL to show that no bad events happen.

iii. A_{xy} is only dependent with

- A_{xz} for z such that $d(x,z) \leq \delta n$.

[2] Let $0 \log_2 0 = 0$.

- A_{zy} for z such that $d(z, y) \leq \delta n$.

By the FACT, there are $2 \cdot 2^{n(H(\delta)\pm o(1))} = 2^{n(H(\delta)\pm o(1))}$ of these dependent events.

iv. Hence when we use the LLL, we can set "d" (the number of dependent events) to be $2^{n(H(\delta)\pm o(1))}$.

v. We can apply the LLL whenever $4pd < 1$ which is equivalent to $4 \cdot 2^{-2n(H(\delta)-0.001)+2} \cdot 2^{n(H(\delta)\pm o(1))} < 1$. This holds for many positive constants δ, such as $\delta = 0.25$.

Hence by the LLL your friend concludes that such a set S exists.

As awesome as it would be if your friend had solved this problem, unfortunately there's a problem with the proof strategy above. **What is the flaw in this reasoning?**

(b) **(5 pt.)** Use the LLL to show that for any constant $\delta \in (0, 1/2)$ and for large enough n, there exists a set S of size $|S| \geq 2^{n(1-H(\delta)-0.001)}$ so that $\forall x, y \in S$, we have $d(x, y) > \delta n$.

[**HINT:** *Choose a random multi-set* $S \in \{0,1\}^n$ *by choosing* $2^{n(1-H(\delta)-0.001)}$ *randomly, independently with replacement.*]

[**HINT:** *Try and justify that any set* S *constructed via the previous hint that has the desired distance properties must also have the desired size property.*]

(c) **(0 pt.)** [**Optional: This part will not be graded.**]

For any constant $\delta \in (0, 1/2)$, let S be a random subspace of $\{0,1\}^n$ of dimension $n(1 - H(\delta) - 0.001)$. Note that $|S| = 2^{n(1-H(\delta)-0.001)}$. Show that with probability at least 0.99, the Hamming distance between any two distinct strings in S is greater than δn.

Note that sampling a random subspace can be done computationally efficiently, which is why this is a more interesting result than the one from part (b).

(d) **(0 pt.)** [**Optional: This part will not be graded.**]

Your friend is pretty excited about part (b), since they claim that it means that the constructive LLL gives an efficient Las Vegas algorithm to find a set as in part (b). Your friend heard that it is also a major open problem to find such a set with a Las Vegas algorithm in expected time poly(n), and they are looking forward to winning the Shannon award for this. What is your friend missing? (They are correct that this is a major open problem).