CSCE 658: Randomized Algorithms – Spring 2024
Problem Set 2

Due: Tuesday, February 20, 2024, 5:00 pm CT

Problem 1. (30 points total) Concentration and anti-concentration.

Let $p \in (0,1)$ be a fixed constant and suppose a coin that lands HEADS with probability p and TAILS with probability $1-p$ is flipped a total of n times. Let X be the random variable for the total number of HEADS observed.

1. (5 points) What is $\mathbb{E}[X]$? What is $\mathbb{E}[X^2]$? What is $\mathrm{Var}[X]$?
2. (10 points) Show that for any constant $C > 0$, there exists a constant $\gamma > 0$ such that
$$\mathbf{Pr}\left[|X - \mathbb{E}[X]| \geq \gamma\sqrt{pn\log n}\right] \leq \frac{1}{n^C}.$$
3. STOP AND THINK: Before doing the next problem, suppose $p = \frac{1}{2}$. What do you think $\mathbf{Pr}\left[X = \frac{n}{2}\right]$ is? Did the subsequent bounds match your intuition?

   (10 points) Show that for even n and $p = \frac{1}{2}$, there exist constants $C_1, C_2 > 0$ such that
$$\frac{C_1}{\sqrt{n}} \leq \mathbf{Pr}\left[X = \frac{n}{2}\right] \leq \frac{C_2}{\sqrt{n}}.$$

   HINT: For the following problem, use Stirling's formula, so that for all $n \geq 1$,
$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}.$$
4. (5 points) Conclude that for $p = \frac{n}{2}$ and for any constant $C \leq 1$, there exists a constant $\alpha > 0$ such that
$$\mathbf{Pr}\left[\frac{n}{2} - \alpha\cdot\sqrt{n} < X < \frac{n}{2} + \alpha\cdot\sqrt{n}\right] \leq C.$$
   Note that as opposed to concentration inequalities, which upper bound the probability that X deviates from its mean, the above result upper bounds the probability that X is close to its mean. These inequalities are known as *anti-concentration* inequalities.

Problem 2. (30 points total) Markov and Chebyshev.

In class, we saw there are settings where Chebyshev's inequality gives sharper tail bounds than Markov's inequality. In this problem we show that 1) there are settings where Markov's inequality can be more informative than Chebyshev's inequality and 2) there are settings where either inequality is tight.

1. (5 points) Define $p(x) = \begin{cases} \frac{1}{|x|^3} & |x| \geq 1 \\ 0 & \text{otherwise} \end{cases}$.

   Show that $p(x)$ is a valid probability density function.

2. (10 points) Let $p(x)$ be defined as in the previous problem describe the distribution of a random variable X and let $Y = X + 1$. Prove using Markov's inequality that $\mathbf{Pr}[Y \geq 4] \leq \frac{1}{4}$. Then prove that Y does not have finite variance.

   NOTE: As a result of your proof, it follows that we cannot apply Chebyshev's inequality to upper bound $\mathbf{Pr}[Y \geq 4] \leq t$ for any $t < 1$. Hence we can acquire tail bounds using Markov's inequality that do not immediately follow from Chebyshev's inequality.

3. (5 points) Let $\alpha > 1$ be any fixed constant. Prove that Markov's inequality is tight by describing the distribution of a random variable X such that $\mathbf{Pr}[X \geq \alpha \cdot \mathbb{E}[X]] = \frac{1}{\alpha}$.

4. (10 points) Let $\alpha > 1$ be any fixed constant. Prove that Chebyshev's inequality is tight by describing the distribution of a random variable X such that $\mathbb{E}[X] = 0$, $\mathrm{Var}[X] = 1$, and $\mathbf{Pr}[|X - \mathbb{E}[X]| \geq \alpha] = \frac{\mathrm{Var}[X]}{\alpha^2}$.

Problem 3. (30 points total) Exponential tail bounds.

Let $X_1, \ldots, X_n \in \{0, 1\}$ be independent random variables, not necessarily identically distributed, and let $X = X_1 + \ldots + X_n$ and $\mu = \mathbb{E}[X]$.

1. (5 points) Use the inequality $1 + x \leq e^x$ for all $x \in \mathbb{R}$ to show that $\mathbb{E}\left[e^{\lambda X_i}\right] \leq e^{\mathbb{E}[X_i] \cdot (e^\lambda - 1)}$ for all $i \in \{1, \ldots, n\}$ and all $\lambda \in \mathbb{R}$.

2. (5 points) Show that for all $\lambda \in \mathbb{R}$, we have

$$\mathbb{E}\left[e^{\lambda X}\right] \leq e^{e^\lambda - 1) \cdot \mu}.$$

3. (5 points) Use Markov's inequality appropriately to prove that:

$$\mathbf{Pr}[X \geq (1 + \delta) \cdot \mu] \leq \frac{e^{(e^\lambda - 1)\mu}}{e^{\lambda(1+\delta)\mu}}.$$

4. (5 points) Find, with proof, the value of λ for which the inequality is sharpest by minimizing the right hand side of the previous inequality.

5. (5 points) Conclude that

$$\mathbf{Pr}[X \geq (1 + \delta) \cdot \mu] \leq \left(\frac{e^{-\delta}}{(1 + \delta)^{1+\delta}}\right)^\mu.$$

6. (5 points) Use Markov's inequality appropriately with $\lambda = \ln \frac{1}{1-\delta}$ to prove that for any $\delta \in (0, 1)$:

$$\mathbf{Pr}[X \leq (1 - \delta) \cdot \mu] \leq \left(\frac{e^{-\delta}}{(1 - \delta)^{1-\delta}}\right)^\mu.$$

Problem 4. (30 points total) Pairwise independence.

Often, generating and storing a large collection of independent random variables is expensive. Sometimes, our analysis does not require random variables to be fully independent, but only k-wise independent, in which case we can efficiently store realizations of these random variables. In this problem, we will study the case $k = 2$ and how such random variables might be generated.

A collection $X_1, \ldots, X_n$ of random variables is *pairwise independent* if for all $i \neq j$ and all $a, b \in \mathbb{R}$, we have

$$\mathbf{Pr}\left[X_i = a \mid X_j = b\right] = \mathbf{Pr}\left[X_i = a\right].$$

1. (5 points) Let p be a prime number and $\mathbb{Z}_p$ denote the integers mod p. Let r and s be chosen independently and uniformly at random from $\mathbb{Z}_p$. Prove that for fixed A and B, we can solve the system of equations $A \equiv ri + s \pmod{p}$ and $B \equiv rj + s \pmod{p}$ uniquely for r and s.

2. (10 points) Let $p \gg n$ be a prime number and $\mathbb{Z}_p$ denote the integers mod p. Let r and s be chosen independently and uniformly at random from $\mathbb{Z}_p$ and for each $i \in \{1, \ldots, n\}$, let $X_i = ri + s \pmod{p}$. Show that for $i \neq j$, X_i and X_j are uniformly distributed on $\mathbb{Z}_p$ and pairwise independent.

3. (5 points) Storing n fully independent random variables requires n words of space. Describe how we can use two words of space to generate n random variables that are pairwise independent.

4. (10 points) Show that if $X_1, \ldots, X_n$ are pairwise independent random variables and $X = X_1 + \ldots + X_n$, then

$$\mathrm{Var}\left[X\right] = \mathrm{Var}\left[X_1\right] + \ldots + \mathrm{Var}\left[X_n\right].$$