CPSC 448 Lecture Notes

Ayush Vora, Nathan Harms

September 2025

1 Chernoff Bound

The Chernoff bound is a pair of inequalities that bound a random variable using its moment generating function.

1.1 Obtaining the Bounds

Let X be a random variable, and $M_X(t)$ be the moment generating function (MGF) of X. We can start with Markov's inequality, and apply it to a function of X, specifically e^{tX} as shown:

$$\begin{aligned}\mathbb{P}[X \geq a] &= \mathbb{P}[e^{tX} \geq e^{ta}] \text{ for } t > 0 \\ &\leq \mathbb{E}[e^{tX}]/e^{ta} \text{ by Markov's Inequality} \\ &= M_X(t)e^{-ta} \text{ by definition of MGF}\end{aligned}$$

Similarly, we see that:

$$\begin{aligned}\mathbb{P}[X \leq a] &= \mathbb{P}[e^{tX} \geq e^{ta}] \text{ for } t < 0 \\ &\leq \mathbb{E}[e^{tX}]/e^{ta} \\ &= M_X(t)e^{-ta}\end{aligned}$$

Because we have these bounds for all values of t, we can choose the tightest bound by choosing t such that $M_X(t)e^{-ta}$ is minimized.

1.2 Bounds for the "Gambler" Random Variable

Suppose a gambler plays n rounds of a game, where each round is independent of each other. Say there is an equal chance of either winning or losing \$1. Let the gambler's winnings of round i be X_i. Then, the total winnings would be $X = \sum_{i=1}^{n} X_i$. We can generate a bound on the winnings. First, note that $M_{X_i}(t) \leq e^{t^2/2}$. We can start by finding $M_X(t)$:

$$
\begin{aligned}
M_X(t) &= \mathbb{E}[e^{tX}] \\
&= \mathbb{E}[e^{t\sum_i X_i}] \\
&= \mathbb{E}\left[\prod_{i=1}^{n} e^{tX_i}\right] \\
&= \prod_{i=1}^{n} \mathbb{E}[e^{tX_i}] \text{ by independence} \\
&\leq \prod_{i=1}^{n} e^{t^2/2} \text{ using } M_{X_i}(t) \\
&= e^{nt^2/2}
\end{aligned}
$$

We can now use this in finding our bound for X:

$$
\begin{aligned}
\mathbb{P}[X \geq a] &\leq M_X(t)e^{-ta} \\
&\leq e^{nt^2/2}e^{-ta} \\
&= e^{nt^2/2-ta}
\end{aligned}
$$

The minimum of $e^{nt^2/2-ta}$, or, equivalently, the minimum of $nt^2/2-ta$ can be found using calculus. We find that it is minimized when $t = a/n$. Substituting these values above, we get that:

$$\mathbb{P}[X \geq a] \leq e^{n(a/n)^2/2-(a/n)a} = e^{-a^2/2n}$$

Using this, we can go back to our example. Say our gambler wants to play 10 games, and wants to make a profit of at least \$6. Then the probability that occurs is:

$$\mathbb{P}[X \geq 6] \leq e^{-6^2/(2\times 10)} = e^{-9/5} \approx 0.1653$$

The exact probability is $56/1024 \approx 0.0547$.

1.3 Exercises

1. Show that our bound in section 1.2 is stronger than that of Chebyshev's inequality.

2. (a) Find the upper Chernoff bound for the Poisson variable $Y \sim \text{Poi}(\lambda)$. You may use that the $M_Y(t) = e^{\lambda(e^t-1)}$.

   (b) Show that this bound is stronger than that of Markov's inequality.

3. In section 1.2, we state that $M_{X_i}(t) \leq e^{t^2/2}$. Show that this is the case. (Hint: use the power series definition of e^x.)

2 Poissonization

The following is heavily inspired by Maryam Aliakbarpour's lecture notes in "Hidden Gems of Sublinear Algorithms".

2.1 Motivation

Suppose we have m balls, and each ball must go in one of n bins. Let the probability that a ball goes into bin i be p_i. We want to look into how many balls are in each bin. Let us define the number of balls in bin i as:

$$X_i \sim \text{Bin}(m, p_i)$$

However, these X_i can sometimes lead to issues when doing further analysis. This is because the X_i's are not independent of each other (shown below). **Poissonization** is a technique that can translate these dependent random variables into independent Poisson random variables, assuming we are okay with getting an approximate answer.

Theorem 2.1. The outcomes X_i are dependent on each other.

Proof. First, notice that because we have exactly m balls, and every ball is in a bin, we have that:

$$\sum_{i=1}^{n} X_i = m$$

and that m is constant. Because the variance of a constant is 0, it follows:

$$\text{Var}\left(\sum_{i=1}^{n} X_i\right) = \text{Var}(m) = 0$$

Now, for the sake of contradiction, assume that X_i are independent. Then from the properties of independent random variables and binomial random variables, we have that:

$$\text{Var}\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} \text{Var}\left(X_i\right) = \sum_{i=1}^{n} mp_i(1-p_i) \neq 0$$

This is a contradiction. □

2.2 Benefits of the Poisson Distribution

The Poisson distribution can help us solve this issue! To start off, recall that if $Y_1 \sim \text{Poi}(\lambda_1)$ and $Y_2 \sim \text{Poi}(\lambda_2)$, then $Y_1 + Y_2 \sim \text{Poi}(\lambda_1 + \lambda_2)$.

The main goal of Poissonization is to generate a different set of independent outcomes $Y_i \sim \text{Poi}(mp_i)$ as a "replacement" for the dependent X_i's. We will

show how we generate these Y_i in section 2.3. First, we will show that our new random variables, conditioned on a set sum is identical to original distribution.

Let $k_1, ..., k_n \in \mathbb{N}$ such that $\sum_{i=1}^{n} k_i = k$.

Theorem 2.2. The joint distribution of $(Y_1, ..., Y_n)$ conditioned on $\sum_{i=1}^{n} Y_i = k$ is identical to the joint distribution of $(X_1, ..., X_n)$.

To show that they are identical, it is sufficient to show that their probability mass functions (PMF) are equal.

Proof. Because the joint distribution of $(X_1, ..., X_n)$ is multinomial, the PMF of it is:

$$p_{X_1,...,X_n}(k_1, ..., k_n) = \frac{k!}{n^k \prod_{i=1}^{n} k_i!}$$

The joint conditional PMF of $(Y_1, ..., Y_n)$ is:

$$\begin{aligned}
p_{Y_1,...,Y_n \mid \sum Y_i = k}(k_1, ..., k_n) &= \frac{p_{Y_1,...,Y_n}(k_1, ..., k_n)}{\mathbb{P}[\sum_i Y_i = k]} \\
&= \frac{\prod_{i=1}^{n} p_{Y_i}(k_i)}{\mathbb{P}[\sum Y_i = k]} \text{ by independence of random variables} \\
&= \frac{\prod_{i=1}^{n} p_{Y_i}(k_i)}{p_{\sum Y_i}(k)} \text{ as } \sum_{i=1}^{n} Y_i \sim \text{Poi}(m) \\
&= \frac{k!}{e^{-m} m^k} \prod_{i=1}^{n} \frac{e^{-m/n}(m/n)^{k_i}}{k_i!} \text{ by Poisson PMF} \\
&= \left(\frac{k!}{e^{-m} m^k}\right) \left(e^{-m/n}\right)^n \left(\frac{m}{n}\right)^k \left(\frac{1}{\prod_{i=1}^{n} k_i!}\right) \\
&= \frac{k!}{n^k \prod_{i=1}^{n} k_i!} \\
&= p_{X_1,...,X_n}(k_1, ..., k_n)
\end{aligned}$$

as needed.

□

This shows us that we can successfully approximate the X_i's using the Y_i's. This leaves us one main question: How do we generate these Y_i's?

2.3 Generating Independent Outcomes

Let P be a probability distribution over $[n]$. Let $p_i = \mathbb{P}_{S \sim P}[S = i]$. Assume that we draw m samples $S_1, ..., S_m \sim P$. These samples can be thought of as the location of a ball from our example above. Let X_i be a random variable indicating how many samples S_j take the value i. Specifically:

$$X_i = \sum_{j=1}^{m} \mathbb{1}[S_j = i] \sim \text{Bin}(m, p_i)$$

Similar to how we established above, these X_i are not independent. To generate independence, do the following:

1. Let $\hat{m} \sim \text{Poi}(m)$. Our value $\hat{m}$ will be an approximation for m. Draw this value.
2. Draw $\hat{m}$ samples $S_1, ..., S_{\hat{m}}$ from P.
3. Let $Y_i = \sum_{j=1}^{\hat{m}} \mathbb{1}[S_j = i]$.

Following the process above, we can generate Y_i that are independent Poisson random variables. To use the theorem above, we only require to show that $Y_i \sim \text{Poi}(mp_i)$

Theorem 2.3. $Y_i \sim \text{Poi}(mp_i)$

Proof. It is sufficient to show that $\mathbb{P}[Y_i = k] = \frac{e^{mp_i}(mp_i)^k}{k!}$, the PMF of the Poisson distribution.

$$\begin{aligned}
\mathbb{P}[Y_i = k] &= \sum_{t=0}^{n} \mathbb{P}[\hat{m} = t]\mathbb{P}[Y_i = k | \hat{m} = t] \text{ by law of total probability} \\
&= \sum_{t=0}^{k-1} \mathbb{P}[\hat{m} = t]\mathbb{P}[Y_i = k | \hat{m} = t] + \sum_{t=k}^{n} \mathbb{P}[\hat{m} = t]\mathbb{P}[Y_i = k | \hat{m} = t] \\
&= \sum_{t=k}^{n} \mathbb{P}[\hat{m} = t]\mathbb{P}[Y_i = k | \hat{m} = t] \text{ See note (1)} \\
&= \sum_{t=k}^{n} \left(\frac{e^{-m} m^t}{t!} \right) \left(\binom{t}{k} p_i^k (1 - p_i)^{t-k} \right) \text{ by Poisson and Binomial PMF.} \\
&= \frac{e^{-m} p_i^k}{k!} \sum_{t=k}^{n} \frac{m^t (1 - p_i)^{t-k}}{(t-k)!} \\
&= \frac{e^{-m} p_i^k m^k}{k!} \sum_{t=k}^{n} \frac{m^{t-k} (1 - p_i)^{t-k}}{(t-k)!} \\
&= \frac{e^{-m} p_i^k m^k e^{m(1-p_i)}}{k!} \text{ By power series definition of } e^x \\
&= \frac{e^{mp_i} (mp_i)^k}{k!}
\end{aligned}$$

as needed.

(1): We can think of t as the number of balls that we have, and k as the number of balls in bin i. If we consider the case where we have $t < k$, that

would be saying that we have more balls in bin i than we have total balls. The probability of this happening is 0. Hence, $\sum_{t=0}^{k-1} \mathbb{P}[\hat{m} = t]\mathbb{P}[Y_i = k|\hat{m} = t] = 0$. □

2.4 Use in Randomized Algorithms

This situation of counting the number of instances given a sample shows up often in randomized algorithms. Doing statistical analysis on these may be difficult due to the dependence between the random variables. However, Poissonization solves this problem for us. In particular, if we have an algorithm $\mathcal{A}(P, m, \delta)$ that does the following:

1. Pull m samples from distribution P. Call these samples $S_1, ...S_m$.
2. Let $X_i = \sum_{j=1}^{m} \mathbb{1}(S_j = i)$.
3. Run function $\mathcal{A}^*(X_1, ..., X_n)$ with $\mathbb{P}(\text{Fail}) \leq \delta$. We can think of $\mathcal{A}^*$ as the "remaining code" of our algorithm.

We can modify this algorithm to ensure that the variables for $\mathcal{A}^*$ are independent.

Theorem 2.4. If there exists an algorithm $\mathcal{A}(P, m, \delta)$ that uses m samples from P where $\mathbb{P}(\text{Fail}) \leq \delta$, then there exists an algorithm $\mathcal{A}'(P, m, \delta)$ that uses $\text{Poi}(2m)$ samples from P where $\mathbb{P}(\text{Fail}) \leq 2\delta$ given that $m \geq \frac{\ln(\delta)}{\ln(2)-1}$.

Proof. Consider the following algorithm $\mathcal{A}'(P, m, \delta)$:

1. Let $m' \sim \text{Poi}(2m)$.
2. If $m' < m$, fail.
3. Pull m' samples from P, call them $S_1, ..., S_{m'}$.
4. Let $Y_i = \sum_{j=1}^{m'} \mathbb{1}(S_j = i)$.
5. Run function $\mathcal{A}^*(Y_1, ..., Y_n)$ with $\mathbb{P}(\text{Fail}) \leq \delta$.

This algorithm fails when either $\mathcal{A}^*$ fails, or $m' < m$. We will show that this probability is less than 2δ.

$$\begin{aligned}
\mathbb{P}(\mathcal{A}^* \text{ fails } \cup m' < m) &\leq \mathbb{P}(\mathcal{A}^* \text{ fails}) + \mathbb{P}(m' < m) \text{ by Union Bound} \\
&= \delta + \mathbb{P}(m' < m) \\
&\leq \delta + \mathbb{P}(m' \leq m) \\
&\leq \delta + (m/2m)^{-m} e^{m-2m} \text{ by Chernoff Bound} \\
&= \delta + (e/2)^{-m} \\
&\leq \delta + \delta \text{ for } m \geq \frac{\ln(\delta)}{\ln(2) - 1} \\
&= 2\delta
\end{aligned}$$

□

We can also do this proof in the other direction, where we have an algorithm $\mathcal{B}(P, m, \delta)$ that uses $m' \sim \text{Poi}(m)$ samples with failure rate δ. We can construct an algorithm $\mathcal{B}'(P, m, \delta)$ that uses $2m$ samples with failure rate 2δ.

Theorem 2.5. If there exists an algorithm $\mathcal{B}(P, m, \delta)$ that uses $m' \sim \text{Poi}(m)$ samples from P where $\mathbb{P}(\text{Fail}) \leq \delta$, then there exists an algorithm $\mathcal{B}'(P, m, \delta)$ that uses $2m$ samples from P where $\mathbb{P}(\text{Fail}) \leq 2\delta$ given that $m \geq \frac{\ln(\delta)}{1-\ln(4)}$.

Proof. We can construct it similar to the algorithms in the above proof. We will focus on showing the error probability.

$$\begin{aligned}
\mathbb{P}(B^* \text{ fails } \cup m' > 2m) &\leq \mathbb{P}(B^* \text{ fails}) + \mathbb{P}(m' > 2m) \text{ by Union Bound} \\
&= \delta + \mathbb{P}(m' > 2m) \\
&\leq \delta + \mathbb{P}(m' \geq 2m) \\
&\leq \delta + (2m/m)^{-2m} e^{2m-m} \text{ by Chernoff Bound} \\
&= \delta + (e/4)^m \\
&\leq \delta + \delta \text{ for } m \geq \frac{\ln(\delta)}{1 - \ln(4)} \\
&= 2\delta
\end{aligned}$$

□

2.5 Exercises

1. In the fourth equality of Theorem 2.3, we assume that Y_i conditioned on $\hat{m}$ follows $\text{Bin}(t, p_i)$. Explain why we assume so.

3 Important terms in the Paper

3.1 The Problem: Distribution Support Size and Distinct Elements

Definition 3.1. Distribution Support Size (DSS): Given a parameter n and access to independent samples from a distribution where each element appears with probability $1/n$, approximate the distribution support size.

Definition 3.2. Distinct Elements (DE): Given access to a sequence of length n, approximate the number of distinct elements (or "colours") in the sequence.

Instance of DE.

3.2 Probability

Definition 3.3. (In paper, 4.1) Collisions and histograms. Consider s samples taken by an algorithm. an l-way collision occurs if a colour appears exactly l times in the sample. For $l = 0, 1, ..., s$, let F_l be the number of l-way collisions in the sample. The histogram F of the sample is the vector $(F_1, ..., F_s)$, indicating for each non-zero l how many colours appear exactly l times in the sample.

Definition 3.4. (In paper, 4.2) Frequency Variable. Suppose we have an instance of DE with n/d colours. Group colours into "types" according to how many times they appear in the input: say, a p_i fraction of the colours are of type i and each of them appear a_i times. Consider a mental experiment where we choose a colour uniformly at random and count how many times it occurs in the instance. The frequency variable X is a random variable representing the number of balls of a colour chosen uniformly at random, as described in the experiment. Note that $E[X] = d$.

Definition 3.5. (In paper, 5.2) Statistical (or Total Variance) Difference. Distributions P and Q over a domain S have statistical difference δ if $\max_{S' \subseteq S} |P(S') - Q(S')| = \delta$. We write $P \approx_\delta Q$ to denote that P and Q have a statistical difference of at most δ. For random variables $X \sim P, Y \sim Q$, we say that X and Y have a statistical difference δ ($X \approx_\delta Y$) when $P \approx_\delta Q$.

3.3 Proportional Moments

Definition 3.6. (In paper, 4.3) Proportional Moments. Random variables $\hat{X}$ and $\tilde{X}$ have $k-1$ proportional moments if

$$\frac{E[\tilde{X}]}{E[\hat{X}]} = \frac{E[\tilde{X}^2]}{E[\hat{X}^2]} = ... = \frac{E[\tilde{X}^{k-1}]}{E[\hat{X}^{k-1}]}$$

Definition 3.7. (In paper, 4.4) Moments Condition. Random variables $\hat{X}$ and $\tilde{X}$ satisfy the moment's condition with parameters k, B if $\hat{X}$ and $\tilde{X}$ have $k-1$ proportional moments, and $E[\tilde{X}]/E[\hat{X}] \geq B$

3.4 Algorithms

Poissonization

Definition 3.8. (In paper, 3.2) Uniform Algorithm. An algorithm is uniform if it takes independent samples with replacement and only gets to see the "colours" of the samples, but not the input positions corresponding to them.

Definition 3.9. (In paper, 5.1) Poisson Algorithm. A uniform algorithm is called a Poisson-s algorithm if the number of samples that it takes is a random variable $\sim \text{Poi}(s)$.

3.5 An instance of DE: D_X

4 Important Theorems in the Paper

Theorem 4.1. (In paper, 4.5) For all integers $k > 1$ and $B > 1$, There exist random variables $\hat{X}$ and $\tilde{X}$ over positive integers $a_0 < a_1 < ... < a_{k-1}$ that satisfy the moment's condition with parameters k and B. Moreover, for these variables, $a_i = (B+3)^i, E[\tilde{X}] > B, E[\hat{X}] < 1 + \frac{1}{B}$

Definition 4.1. (In paper, 5.4) D_X. For $k > 1$, let $a_0 < a_1 < ... < a_{k-1}$ be integers, and let X be a random variable over these integers such that $\mathbb{P}[X = a_i] = p_i$. Observe that $E[X] = \sum_{i=0}^{k-1} p_i a_i$. Let $M_X = \sum_{i=0}^{k-1} \left\lfloor \frac{np_i}{E[X]} \right\rfloor + n - \sum_{i=0}^{k-1} a_i \left\lfloor \frac{np_i}{E[X]} \right\rfloor$. If, for all i, $\frac{np_i}{E[X]}$ is an integer, then $M_X = \frac{n}{E[X]}$. Let D_X be an instance of DE of length n (that is, a string in $[n]^n$) that contains M_X colours. For $i = 0, ..., k-1$, instance D_X contains $\left\lfloor \frac{np_i}{E[X]} \right\rfloor$ colours of type i, each appearing a_i times. In addition, there are $n - \sum_{i=0}^{k-1} \left\lfloor \frac{np_i}{E[X]} \right\rfloor a_i$ colours that appear once each. We refer to these singleton colours as being of type k and set $a_k = 1$.

Lemma 4.2. (In paper, 5.9) For both instances $D_{\tilde{X}}, D_{\hat{X}}$, the probability of a collision involving $k > 1$ or more balls is at most

$$\delta_1 = O\left(\frac{a_{k-1}^{k-1} s^k}{k! n^{k-1}}\right)$$

Lemma 4.3. (In paper, 5.10) For both instances $D_{\tilde{X}}, D_{\hat{X}}$, $F_1, .., F_{k-1}$ are close to independent. That is, $(F_1, ..., F_{k-1}) \approx_{\delta_2} (F'_1, ..., F'_{k-1})$, where the variables F'_l are independent, for each l the distributions of F_l, F'_l are identical, and $\delta_2 \leq \frac{2ksa_{k-1}}{n}$.

Lemma 4.4. (In paper, 5.12) For $l = 1, ..., k-1$, $\hat{F}_l \approx_{\delta_3} \tilde{F}_l$, where

$$\delta_3 = O\left(\frac{ksa_{k-1}}{n} + \frac{(a_{k-1}/n)^{k-1} s^k}{\lfloor k/2 \rfloor! \lceil k/2 \rceil!} \cdot\right)$$

Theorem 4.5. (In paper, 5.8) For $s \leq \frac{n}{2a_{k-1}}$, the statistical difference between histogram random variables $(\hat{F}_1, \hat{F}_2, ...)$ and $(\tilde{F}_1, \tilde{F}_2, ...)$ is

$$O\left(\frac{k^2 a_{k-1} s}{n} + \frac{k}{\lfloor \frac{k}{2} \rfloor! \lceil \frac{k}{2} \rceil!} a_{k-1}^{k-1} \frac{s^k}{n^{k-1}}\right)$$

Theorem 4.6. (In paper, 5.6) Let $\hat{X}, \tilde{X}$ be random variables over positive integers $a_0 < a_1 < ... < a_{k-1}$ that have $k-1$ proportional moments. For any Poisson-s algorithm $\mathcal{A}$ that only looks at histograms and takes $s \leq \frac{n}{2a_{k-1}}$ samples in expectation,

$$\left|\mathbb{P}[\mathcal{A}(D_{\hat{X}})=1]-\mathbb{P}[\mathcal{A}(D_{\tilde{X}})=1]\right| = O\left(\frac{k^2 a_{k-1} s}{n} + \frac{k}{\lfloor \frac{k}{2} \rfloor ! \lceil \frac{k}{2} \rceil !} a_{k-1}^{k-1} \frac{s^k}{n^{k-1}}\right)$$

Corollary 4.6.1. (In paper, 5.7) Let $\hat{X}, \tilde{X}$ be fixed (w.r.t n) random variables with $k-1$ proportional moments. If $s = o(n^{1-1/k})$, then for any Poisson-s algorithm $\mathcal{A}$, we have

$$\left|\mathbb{P}[\mathcal{A}(D_{\hat{X}})=1]-\mathbb{P}[\mathcal{A}(D_{\tilde{X}})=1]\right| = o(1)$$

Lemma 4.7. (In paper, 3.4) Let $C_1 = C_1(n)$ and $C_2 = C_2(n)$, where $0.1C_1 > C_2$. If every uniform algorithm needs at least s queries to distinguish DE instances with at least C_1 colours from DE instances with at most C_2 colours, then every algorithm needs $\Omega(s)$ queries to distinguish between DE instances with at least $0.1C_1$ colours form DE instances with at most C_2 colours.

Theorem 4.8. (In paper, 2.1) For all $T \geq 2n^{3/4}\sqrt{\log(n)}$, if we set

$$k = k(n,T) = \left\lfloor \sqrt{\frac{\log(n)}{\log(n) - \log(T) + \frac{1}{2}\log(\log(n)) + 1}} \right\rfloor$$

then the following hold:

1. Every uniform algorithm for DE needs to perform $\Omega(n^{1-2/k})$ queries to distinguish inputs with at least $n-T$ colours from inputs with at most T colours. The same bound holds for DSS, even under the promise that probabilities are integer multiples of $1/n$.
2. Every algorithm for DE, regardless of how it accesses the input, needs to perform $\Omega(n^{1-2/k})$ queries to distinguish between inputs with at least $n/11$ colours from inputs with at most T colours.

Corollary 4.8.1. (In paper, 2.2)

1. If $\frac{5\log(\log(n))+10}{\log(n)} \leq \epsilon \leq \frac{1}{16}$, then distinguishing inputs of DE with at least $n/11$ colours from inputs with at most $n^{1-\epsilon}$ colours requires $\Omega(n^{1-3\sqrt{\epsilon}})$ queries.
2. If $\epsilon < \frac{5\log(\log(n))+10}{\log(n)}$, then distinguishing inputs of DE with at least $n/11$ colours from inputs with at most $n^{1-\epsilon}$ colours requires $n^{1-O(\sqrt{\log(\log(n))/\log(n)})}$ queries.

For both cases, the input with $n/11$ colours may be taken to have $n - n^{1-\epsilon}$ colours when the algorithm is uniform or when the problem to be solved is DSS.

References