## Probabilistic Methods in Algorithms

## with

# Applications to Computational Biology 

Eli Upfal<br>Brown University<br>Eli_Upfal@brown.edu

## Outline - What I'll try to cover...

- The basic bounds: Bernstein, Chernoff, Hoeffding, Azuma-Hoeffding, McDiarmid. How to create your own bound....
- The Monte-Carlo method and MCMC
- The curse of too many questions: the multi-hypothesis problem and genome-wide association studies
- Two computational biology applications: HotNet and Dendrix


## It's (almost) all in the book:



Expanded second edition coming soon.

## Large Deviation Bounds for CS Analysis:

- Bernstein Inequality: the basic scheme
- Chernoff bound: independent, Bernoulli random variables
- Hoeffding bound: independent, bounded r.v.'s
- Azuma-Hoeffding bound: non-independent, bounded, martingale sequence
- McDiarmid bound: a Doob martingale on a function with bounded variation.


## Why Special Probabilistic Tools for CS?

A typical probability theory statement:

## Theorem (The Central Limit Theorem)

Let $X_{1}, \ldots, X_{n}$ be independent identically distributed random variables with common mean $\mu$ and variance $\sigma^{2}$. Then

$$
\lim _{n \rightarrow \infty} \operatorname{Pr}\left(\frac{\sum_{i=1}^{n} X_{i}-n \mu}{\sigma \sqrt{n}} \leq z\right)=\frac{1}{\sqrt{2 \pi}} \int_{-\infty}^{z} e^{-t^{2} / 2} d t
$$

A typical CS probabilistic tool:

## Theorem (Chernoff Bound)

Let $X_{1}, \ldots, X_{n}$ be independent Bernoulli random variables such that $\operatorname{Pr}\left(X_{i}=1\right)=p_{i}$, then

$$
\operatorname{Pr}\left(\sum_{i=1}^{n} X_{i} \geq(1+\delta) \sum_{i=1}^{n} p_{i}\right) \leq e^{-\mu \delta^{2} / 3}
$$

## We build on Basic Probability Theory

Reminder:
Theorem (Markov Inequality)
If a random variable $X$ is non-negative $(X \geq 0)$ then

$$
\operatorname{Prob}(X \geq a) \leq \frac{E[X]}{a}
$$

Theorem (Chebyshev's Inequality)
For any random variable $X$.

$$
\operatorname{Prob}(|X-E[X]| \geq a) \leq \frac{\operatorname{Var}[X]}{a^{2}}
$$

Both bound are general but relatively weak.

## The Basic Idea of Large Deviation Bounds:

For any random variable $X$, by Markov inequality we have:
For any $t>0$,

$$
\operatorname{Pr}(X \geq a)=\operatorname{Pr}\left(e^{t X} \geq e^{t a}\right) \leq \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t a}}
$$

Similarly, for any $t<0$

$$
\operatorname{Pr}(X \leq a)=\operatorname{Pr}\left(e^{t X} \geq e^{t a}\right) \leq \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t a}}
$$

## The General Scheme:

We obtain specific bounds for particular conditions/distributions by
(1) computing $E\left[e^{t X}\right]$
(2) optimizing

$$
\begin{aligned}
& \operatorname{Pr}(X \geq a) \leq \min _{t>0} \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t a}} \\
& \operatorname{Pr}(X \leq a) \leq \min _{t<0} \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t a}} .
\end{aligned}
$$

(3) symplifying

## Moment Generating Function

## Definition

The moment generating function of a random variable $X$ is defined for any real value $t$ as

$$
M_{X}(t)=\mathbf{E}\left[e^{t X}\right]
$$

## Theorem

Let $X$ be a random variable with moment generating function $M_{X}(t)$. Assuming that exchanging the expectation and differentiation operands is legitimate, then for all $n \geq 1$

$$
\mathbf{E}\left[X^{n}\right]=M_{X}^{(n)}(0)
$$

where $M_{X}^{(n)}(0)$ is the $n$-th derivative of $M_{X}(t)$ evaluated at $t=0$.
Proof.

$$
M_{X}^{(n)}(t)=\mathbf{E}\left[X^{n} e^{t X}\right]
$$

Computed at $t=0$ we get

$$
M_{X}^{(n)}(0)=\mathbf{E}\left[X^{n}\right]
$$

## Theorem

Let $X$ and $Y$ be two random variables. If

$$
M_{X}(t)=M_{Y}(t)
$$

for all $t \in(-\delta, \delta)$ for some $\delta>0$, then $X$ and $Y$ have the same distribution.

## Theorem

If $X$ and $Y$ are independent random variables then

$$
M_{X+Y}(t)=M_{X}(t) M_{Y}(t) .
$$

## Proof.

$$
M_{X+Y}(t)=\mathbf{E}\left[e^{t(X+Y)}\right]=\mathbf{E}\left[e^{t X}\right] \mathbf{E}\left[e^{t Y}\right]=M_{X}(t) M_{Y}(t)
$$

## Chernoff Bound for Sum of Bernoulli Trials

Let $X_{1}, \ldots, X_{n}$ be a sequence of independent Bernoulli trials with $\operatorname{Pr}\left(X_{i}=1\right)=p_{i}$. Let $X=\sum_{i=1}^{n} X_{i}$, and let

$$
\mu=\mathbf{E}[X]=\mathbf{E}\left[\sum_{i=1}^{n} X_{i}\right]=\sum_{i=1}^{n} \mathbf{E}\left[X_{i}\right]=\sum_{i=1}^{n} p_{i}
$$

For each $X_{i}$ :

$$
\begin{aligned}
M_{X_{i}}(t) & =\mathbf{E}\left[e^{t X_{i}}\right] \\
& =p_{i} e^{t}+\left(1-p_{i}\right) \\
& =1+p_{i}\left(e^{t}-1\right) \\
& \leq e^{p_{i}\left(e^{t}-1\right)}
\end{aligned}
$$

$$
M_{X_{i}}(t)=\mathbf{E}\left[e^{t X_{i}}\right] \leq e^{p_{i}\left(e^{t}-1\right)}
$$

Taking the product of the $n$ generating functions we get for $X=\sum_{i=1}^{n} X_{i}$

$$
\begin{aligned}
M_{X}(t) & =\prod_{i=1}^{n} M_{X_{i}}(t) \\
& \leq \prod_{i=1}^{n} e^{p_{i}\left(e^{t}-1\right)} \\
& =e^{\sum_{i=1}^{n} p_{i}\left(e^{t}-1\right)} \\
& =e^{\left(e^{t}-1\right) \mu}
\end{aligned}
$$

$$
M_{X}(t)=\mathbf{E}\left[e^{t X}\right]=e^{\left(e^{t}-1\right) \mu}
$$

Applying Markov's inequality we have for any $t>0$

$$
\begin{aligned}
\operatorname{Pr}(X \geq(1+\delta) \mu) & =\operatorname{Pr}\left(e^{t X} \geq e^{t(1+\delta) \mu}\right) \\
& \leq \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t(1+\delta) \mu}} \\
& \leq \frac{e^{\left(e^{t}-1\right) \mu}}{e^{t(1+\delta) \mu}}
\end{aligned}
$$

For any $\delta>0$, we can set $t=\ln (1+\delta)>0$ to get:

$$
\operatorname{Pr}(X \geq(1+\delta) \mu) \leq\left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}
$$

## Theorem

Let $X_{1}, \ldots, X_{n}$ be independent Bernoulli random variables such that $\operatorname{Pr}\left(X_{i}=1\right)=p_{i}$.

- For any $\delta>0$,

$$
\begin{equation*}
\operatorname{Pr}(X \geq(1+\delta) \mu) \leq\left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu} \tag{1}
\end{equation*}
$$

- For $0<\delta \leq 1$,

$$
\begin{equation*}
\operatorname{Pr}(X \geq(1+\delta) \mu) \leq e^{-\mu \delta^{2} / 3} \tag{2}
\end{equation*}
$$

- For $R \geq 6 \mu$,

$$
\begin{equation*}
\operatorname{Pr}(X \geq R) \leq 2^{-R} \tag{3}
\end{equation*}
$$

$$
M_{X}(t)=\mathbf{E}\left[e^{t X}\right]=e^{\left(e^{t}-1\right) \mu}
$$

Applying Markov's inequality we have for any $t>0$

$$
\begin{aligned}
\operatorname{Pr}(X \geq(1+\delta) \mu) & =\operatorname{Pr}\left(e^{t X} \geq e^{t(1+\delta) \mu}\right) \\
& \leq \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t(1+\delta) \mu}} \\
& \leq \frac{e^{\left(e^{t}-1\right) \mu}}{e^{t(1+\delta) \mu}}
\end{aligned}
$$

For any $\delta>0$, we can set $t=\ln (1+\delta)>0$ to get:

$$
\operatorname{Pr}(X \geq(1+\delta) \mu) \leq\left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}
$$

This proves (1).

We show that for $0<\delta<1$,

$$
\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}} \leq e^{-\delta^{2} / 3}
$$

or that

$$
f(\delta)=\delta-(1+\delta) \ln (1+\delta)+\delta^{2} / 3 \leq 0
$$

in that interval. Computing the derivatives of $f(\delta)$ we get

$$
\begin{aligned}
f^{\prime}(\delta) & =1-\frac{1+\delta}{1+\delta}-\ln (1+\delta)+\frac{2}{3} \delta=-\ln (1+\delta)+\frac{2}{3} \delta \\
f^{\prime \prime}(\delta) & =-\frac{1}{1+\delta}+\frac{2}{3}
\end{aligned}
$$

$f^{\prime \prime}(\delta)<0$ for $0 \leq \delta<1 / 2$, and $f^{\prime \prime}(\delta)>0$ for $\delta>1 / 2$.
$f^{\prime}(\delta)$ first decreases and then increases over the interval $[0,1]$. Since $f^{\prime}(0)=0$ and $f^{\prime}(1)<0, f^{\prime}(\delta) \leq 0$ in the interval $[0,1]$. Since $f(0)=0$, we have that $f(\delta) \leq 0$ in that interval. This proves (2).

For $R \geq 6 \mu, \delta \geq 5$.

$$
\begin{aligned}
\operatorname{Pr}(X \geq(1+\delta) \mu) & \leq\left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu} \\
& \leq\left(\frac{e}{6}\right)^{R} \\
& \leq 2^{-R}
\end{aligned}
$$

that proves (3).

## Theorem

Let $X_{1}, \ldots, X_{n}$ be independent Bernoulli random variables such that $\operatorname{Pr}\left(X_{i}=1\right)=p_{i}$. Let $X=\sum_{i=1}^{n} X_{i}$ and $\mu=\mathbf{E}[X]$. For $0<\delta<1$ :

$$
\begin{equation*}
\operatorname{Pr}(X \leq(1-\delta) \mu) \leq\left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}\right)^{\mu} \tag{4}
\end{equation*}
$$

$$
\begin{equation*}
\operatorname{Pr}(X \leq(1-\delta) \mu) \leq e^{-\mu \delta^{2} / 2} \tag{5}
\end{equation*}
$$

Using Markov's inequality, for any $t<0$,

$$
\begin{aligned}
\operatorname{Pr}(X \leq(1-\delta) \mu) & =\operatorname{Pr}\left(e^{t X} \geq e^{(1-\delta) t \mu}\right) \\
& \leq \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t(1-\delta) \mu}} \\
& \leq \frac{e^{\left(e^{t}-1\right) \mu}}{e^{t(1-\delta) \mu}}
\end{aligned}
$$

For $0<\delta<1$, we set $t=\ln (1-\delta)<0$ to get:

$$
\operatorname{Pr}(X \leq(1-\delta) \mu) \leq\left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}\right)^{\mu}
$$

This proves (4).
We need to show:

$$
f(\delta)=-\delta-(1-\delta) \ln (1-\delta)+\frac{1}{2} \delta^{2} \leq 0
$$

We need to show:

$$
f(\delta)=-\delta-(1-\delta) \ln (1-\delta)+\frac{1}{2} \delta^{2} \leq 0
$$

Differentiating $f(\delta)$ we get

$$
\begin{aligned}
f^{\prime}(\delta) & =\ln (1-\delta)+\delta \\
f^{\prime \prime}(\delta) & =-\frac{1}{1-\delta}+1
\end{aligned}
$$

Since $f^{\prime \prime}(\delta)<0$ for $\delta \in(0,1), f^{\prime}(\delta)$ decreasing in that interval. Since $f^{\prime}(0)=0, f^{\prime}(\delta) \leq 0$ for $\delta \in(0,1)$. Therefore $f(\delta)$ is non increasing in that interval.
$f(0)=0$. Since $f(\delta)$ is non increasing for $\delta \in[0,1), f(\delta) \leq 0$ in that interval, and (5) follows.

## Example: Coin flips

Let $X$ be the number of heads in a sequence of $n$ independent fair coin flips.

$$
\begin{aligned}
& \operatorname{Pr}\left(\left|X-\frac{n}{2}\right| \geq \frac{1}{2} \sqrt{6 n \ln n}\right) \\
= & \operatorname{Pr}\left(X \geq \frac{n}{2}\left(1+\sqrt{\frac{6 \ln n}{n}}\right)\right) \\
+ & \operatorname{Pr}\left(X \leq \frac{n}{2}\left(1-\sqrt{\frac{6 \ln n}{n}}\right)\right) \\
\leq & e^{-\frac{1}{3} \frac{n}{2} \frac{6 \ln n}{n}}+e^{-\frac{1}{2} \frac{n}{2} \frac{6 \ln n}{n}} \leq \frac{2}{n} .
\end{aligned}
$$

Markov Inequality gives

$$
\operatorname{Pr}\left(X \geq \frac{3 n}{4}\right) \leq \frac{n / 2}{3 n / 4} \leq \frac{2}{3} .
$$

Using the Chebyshev's bound we have:

$$
\operatorname{Pr}\left(\left|X-\frac{n}{2}\right| \geq \frac{n}{4}\right) \leq \frac{4}{n}
$$

Using the Chernoff bound in this case, we obtain

$$
\begin{aligned}
\operatorname{Pr}\left(\left|X-\frac{n}{2}\right| \geq \frac{n}{4}\right) & =\operatorname{Pr}\left(X \geq \frac{n}{2}\left(1+\frac{1}{2}\right)\right) \\
& +\operatorname{Pr}\left(X \leq \frac{n}{2}\left(1-\frac{1}{2}\right)\right) \\
& \leq e^{-\frac{1}{3} \frac{1}{2} \frac{1}{4}}+e^{-\frac{1}{2} \frac{n}{2} \frac{1}{4}} \\
& \leq 2 e^{-\frac{n}{24}} .
\end{aligned}
$$

## Example: Estimating a Parameter

- Evaluating the probability that a particular DNA mutation occurs in the population.
- Given a DNA sample, a lab test can determine if it carries the mutation.
- The test is expensive and we would like to obtain a relatively reliable estimate from a minimum number of samples.
- $p=$ the unknown value;
- $n=$ number of samples, $\tilde{p} n$ had the mutation.
- Given sufficient number of samples we expect the value $p$ to be in the neighborhood of sampled value $\tilde{p}$, but we cannot predict any single value with high confidence.


## Confidence Interval

Instead of predicting a single value for the parameter we give an interval that is likely to contain the parameter.

## Definition

A $1-q$ confidence interval for a parameter $T$ is an interval
$[\tilde{p}-\delta, \tilde{p}+\delta]$ such that

$$
\operatorname{Pr}(T \in[\tilde{p}-\delta, \tilde{p}+\delta]) \geq 1-q
$$

We want to minimize $2 \delta$ and $q$, with minimum $n$.
Using $\tilde{p} n$ as our estimate for $p n$, we need to compute $\delta$ and $q$ such that

$$
\operatorname{Pr}(p \in[\tilde{p}-\delta, \tilde{p}+\delta])=\operatorname{Pr}(n p \in[n(\tilde{p}-\delta), n(\tilde{p}+\delta)]) \geq 1-q .
$$

- The random variable here is the interval $[\tilde{p}-\delta, \tilde{p}+\delta]$ (or the value $\tilde{p}$ ), while $p$ is a fixed (unknown) value.
- $n \tilde{p}$ has a binomial distribution with parameters $n$ and $p$, and $\mathrm{E}[\tilde{p}]=p$. If $p \notin[\tilde{p}-\delta, \tilde{p}+\delta]$ then we have one of the following two events:
(1) If $p<\tilde{p}-\delta$, then $n \tilde{p} \geq n(p+\delta)=n p\left(1+\frac{\delta}{p}\right)$, or $n \tilde{p}$ is larger than its expectation by a $\frac{\delta}{p}$ factor.
(2) If $p>\tilde{p}+\delta$, then $n \tilde{p} \leq n(p-\delta)=n p\left(1-\frac{\delta}{p}\right)$, and $n \tilde{p}$ is smaller than its expectation by a $\frac{\delta}{p}$ factor.

$$
\begin{aligned}
& \operatorname{Pr}(p \notin[\tilde{p}-\delta, \tilde{p}+\delta]) \\
= & \operatorname{Pr}\left(n \tilde{p} \leq n p\left(1-\frac{\delta}{p}\right)\right)+\operatorname{Pr}\left(n \tilde{p} \geq n p\left(1+\frac{\delta}{p}\right)\right) \\
\leq & e^{-\frac{1}{2} n p\left(\frac{\delta}{p}\right)^{2}}+e^{-\frac{1}{3} n p\left(\frac{\delta}{p}\right)^{2}} \\
= & e^{-\frac{n \delta^{2}}{2 p}}+e^{-\frac{n \delta^{2}}{3 p}}
\end{aligned}
$$

But the value of $p$ is unknown, A simple solution is to use the fact that $p \leq 1$ to prove

$$
\operatorname{Pr}(p \notin[\tilde{p}-\delta, \tilde{p}+\delta]) \leq e^{-\frac{n \delta^{2}}{2}}+e^{-\frac{n \delta^{2}}{3}} .
$$

Setting $q=e^{-\frac{n \delta^{2}}{2}}+e^{-\frac{n \delta^{2}}{3}}$, we obtain a tradeoff between $\delta, n$, and the error probability $q$.

$$
q=e^{-\frac{n \delta^{2}}{2}}+e^{-\frac{n \delta^{2}}{3}}
$$

If we want to obtain a $1-q$ confidence interval $[\tilde{p}-\delta, \tilde{p}+\delta]$,

$$
n \geq \frac{3}{\delta^{2}} \ln \frac{2}{q}
$$

samples are enough.

Chernoff's vs. Chebyshev's Inequality
Assume for all $i$ we have $p_{i}=p ; 1-p_{i}=q$.

$$
\mu=\mathbf{E}[X]=n p
$$

$$
\operatorname{Var}[X]=n p q
$$

If we use Chebyshev's Inequality we get

$$
\operatorname{Pr}(|X-\mu|>\delta \mu) \leq \frac{n p q}{\delta^{2} \mu^{2}}=\frac{n p q}{\delta^{2} n^{2} p^{2}}=\frac{q}{\delta^{2} \mu}
$$

Chernoff bound gives

$$
\operatorname{Pr}(|X-\mu|>\delta \mu) \leq 2 e^{-\mu \delta^{2} / 3}
$$

## Set Balancing

Given an $n \times n$ matrix $\mathcal{A}$ with entries in $\{0,1\}$, let

$$
\left(\begin{array}{cccc}
a_{11} & a_{12} & \ldots & a_{1 n} \\
a_{21} & a_{22} & \ldots & a_{2 n} \\
\ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots \\
a_{n 1} & a_{n 2} & \ldots & a_{n n}
\end{array}\right)\left(\begin{array}{c}
b_{1} \\
b_{2} \\
\ldots \\
\ldots \\
b_{n}
\end{array}\right)=\left(\begin{array}{c}
c_{1} \\
c_{2} \\
\ldots \\
\ldots \\
c_{n}
\end{array}\right)
$$

Find a vector $\bar{b}$ with entries in $\{-1,1\}$ that minimizes

$$
\|\mathcal{A} \bar{b}\|_{\infty}=\max _{i=1, \ldots, n}\left|c_{i}\right|
$$

## Theorem

For a random vector $\bar{b}$, with entries chosen independently and with equal probability from the set $\{-1,1\}$,

$$
\operatorname{Pr}\left(\|\mathcal{A} \bar{b}\|_{\infty} \geq \sqrt{4 n \ln n}\right) \leq \frac{2}{n}
$$

The $\sum_{i=1}^{n} a_{j, i} b_{i}$ (excluding the zero terms) is a sum of independent $-1,1$ random variable. We need a bound on such sum.

## Chernoff Bound for Sum of $\{-1,+1\}$ Random Variables

## Theorem

Let $X_{1}, \ldots, X_{n}$ be independent random variables with

$$
\operatorname{Pr}\left(X_{i}=1\right)=\operatorname{Pr}\left(X_{i}=-1\right)=\frac{1}{2}
$$

Let $X=\sum_{1}^{n} X_{i}$. For any $a>0$,

$$
\operatorname{Pr}(X \geq a) \leq e^{-\frac{a^{2}}{2 n}}
$$

de Moivre - Laplace approximation: For any $k$, such that $|k-n p| \leq a$

$$
\binom{n}{k} p^{k}(1-p)^{n-k} \approx \frac{1}{\sqrt{2 \pi n p(1-p)}} e^{-\frac{a^{2}}{2 n p(1-p)}}
$$

For any $t>0$,

$$
\mathbf{E}\left[e^{t X_{i}}\right]=\frac{1}{2} e^{t}+\frac{1}{2} e^{-t} .
$$

$$
e^{t}=1+t+\frac{t^{2}}{2!}+\cdots+\frac{t^{i}}{i!}+\ldots
$$

and

$$
e^{-t}=1-t+\frac{t^{2}}{2!}+\cdots+(-1)^{i} \frac{t^{i}}{i!}+\ldots
$$

Thus,

$$
\begin{aligned}
\mathbf{E}\left[e^{t X_{i}}\right] & =\frac{1}{2} e^{t}+\frac{1}{2} e^{-t}=\sum_{i \geq 0} \frac{t^{2 i}}{(2 i)!} \\
& \leq \sum_{i \geq 0} \frac{\left(\frac{t^{2}}{2}\right)^{i}}{i!}=e^{t^{2} / 2}
\end{aligned}
$$

$$
\begin{gathered}
\mathbf{E}\left[e^{t X}\right]=\prod_{i=1}^{n} \mathbf{E}\left[e^{t X_{i}}\right] \leq e^{n t^{2} / 2} \\
\operatorname{Pr}(X \geq a)=\operatorname{Pr}\left(e^{t X}>e^{t a}\right) \leq \frac{\mathbf{E}\left[e^{t X}\right]}{e^{t a}} \leq e^{t^{2} n / 2-t a}
\end{gathered}
$$

Setting $t=a / n$ yields

$$
\operatorname{Pr}(X \geq a) \leq e^{-\frac{a^{2}}{2 n}}
$$

## By symmetry we also have

## Corollary

Let $X_{1}, \ldots, X_{n}$ be independent random variables with

$$
\operatorname{Pr}\left(X_{i}=1\right)=\operatorname{Pr}\left(X_{i}=-1\right)=\frac{1}{2}
$$

Let $X=\sum_{i=1}^{n} X_{i}$. Then for any $a>0$,

$$
\operatorname{Pr}(|X|>a) \leq 2 e^{-\frac{\partial^{2}}{2 n}}
$$

## Application: Set Balancing

## Theorem

For a random vector $\bar{b}$, with entries chosen independently and with equal probability from the set $\{-1,1\}$,

$$
\begin{equation*}
\operatorname{Pr}\left(\|\mathcal{A} \bar{b}\|_{\infty} \geq \sqrt{4 n \ln n}\right) \leq \frac{2}{n} \tag{6}
\end{equation*}
$$

- Consider the $i$-th row $\bar{a}_{i}=a_{i, 1}, \ldots, a_{i, n}$.
- Let $k$ be the number of 1 's in that row.
- $Z_{i}=\sum_{j=1}^{k} a_{i, i_{j}} b_{i_{j}}$.
- If $k \leq \sqrt{4 n \ln n}$ then clearly $Z_{i} \leq \sqrt{4 n \ln n}$.

If $k>\sqrt{4 n \log n}$, the $k$ non-zero terms in the sum $Z_{i}$ are independent random variables, each with probability $1 / 2$ of being either +1 or -1 .
Using the Chernoff bound:

$$
\operatorname{Pr}\left\{\left|Z_{i}\right|>\sqrt{4 n \log n}\right\} \leq 2 e^{-4 n \log n /(2 k)} \leq \frac{2}{n^{2}}
$$

where we use the fact that $n \geq k$.
The result follows by union bound ( $n$ rows).

## Hoeffding's Inequality

Large deviation bound for more general random variables:

## Theorem (Hoeffding's Inequality)

Let $X_{1}, \ldots, X_{n}$ be independent random variables such that for all $1 \leq i \leq n, E\left[X_{i}\right]=\mu$ and $\operatorname{Pr}\left(a \leq X_{i} \leq b\right)=1$. Then

$$
\operatorname{Pr}\left(\left|\frac{1}{n} \sum_{i=1}^{n} X_{i}-\mu\right| \geq \epsilon\right) \leq 2 e^{-2 n \epsilon^{2} /(b-a)^{2}}
$$

## Lemma

(Hoeffding's Lemma) Let $X$ be a random variable such that $\operatorname{Pr}(X \in[a, b])=1$ and $E[X]=0$. Then for every $\lambda>0$,

$$
\mathbf{E}\left[E^{\lambda X}\right] \leq e^{\lambda^{2}(a-b)^{2}} / 8
$$

## Proof of the Lemma

Since $f(x)=e^{\lambda x}$ is a convex function, for any $\alpha \in(0,1)$ and $x \in[a, b]$,

$$
f(X) \leq \alpha f(a)+(1-\alpha) f(b) .
$$

Thus, for $\alpha=\frac{b-x}{b-a} \in(0,1)$,

$$
e^{\lambda x} \leq \frac{b-x}{b-a} e^{\lambda a}+\frac{x-a}{b-a} e^{\lambda b} .
$$

Taking expectation, and using $\mathrm{E}[X]=0$, we have

$$
E\left[e^{\lambda x}\right] \leq \frac{b}{b-a} e^{\lambda a}+\frac{a}{b-a} e^{\lambda b} \leq e^{\lambda^{2}(b-a)^{2} / 8} .
$$

## Proof of the Bound

Let $Z_{i}=X_{i}-\mathbf{E}\left[X_{i}\right]$ and $Z=\frac{1}{n} \sum_{i=1}^{n} X_{i}$.

$$
\operatorname{Pr}(Z \geq \epsilon) \leq e^{-\lambda \epsilon} \mathbf{E}\left[e^{\lambda Z}\right] \leq e^{-\lambda \epsilon} \prod_{i=1}^{n} \mathbf{E}\left[e^{\lambda X_{i} / n}\right] \leq e^{-\lambda \epsilon+\frac{\lambda^{2}(b-a)^{2}}{8 n}}
$$

Set $\lambda=\frac{4 n \epsilon}{(b-a)^{2}}$ gives

$$
\operatorname{Pr}\left(\left|\frac{1}{n} \sum_{i=1}^{n} X_{i}-\mu\right| \geq \epsilon\right)=\operatorname{Pr}(Z \geq \epsilon) \leq 2 e^{-2 n \epsilon^{2} /(b-a)^{2}}
$$

## A More General Version

## Theorem

Let $X_{1}, \ldots, X_{n}$ be independent random variables with $\mathrm{E}\left[X_{i}\right]=\mu_{i}$ and $\operatorname{Pr}\left(B_{i} \leq X_{i} \leq B_{i}+c_{i}\right)=1$, then

$$
\operatorname{Pr}\left(\left|\sum_{i=1}^{n} X_{i}-\sum_{i=1}^{n} \mu_{i}\right| \geq \epsilon\right) \leq e^{-\frac{2 \epsilon^{2}}{\sum_{i=1}^{2} c_{i}^{2}}}
$$

