Outline

Chernoff Bounds

Schwartz-Zippel
Theorem

Let $X_1, \ldots, X_n$ be independent boolean random variables such that $\Pr[X_i = 1] = p_i$. Then, for $X = \sum_i X_i$, $\mu = \mathbb{E}[X]$, and $\delta > 0$,

$$\Pr[X > (1 + \delta)\mu] < \left[ \frac{e^\delta}{(1 + \delta)^{1+\delta}} \right]^\mu$$

Other versions: For $0 < \delta \leq 1$

$$\Pr[X \geq (1 + \delta)\mu] \leq e^{-\delta^2 \mu / 3}$$

$$\Pr[X \leq (1 - \delta)\mu] \leq e^{-\delta^2 \mu / 2}$$
Chernoff Bound: Proof of Upper Tail (1/2)

Proof.

- For any $t > 0$: $\mathbb{P}[X > (1 + \delta)\mu] = \mathbb{P}[e^{tX} > e^{t(1+\delta)\mu}]$
- Apply Markov inequality:

$$\mathbb{P}\left[e^{tX} > e^{t(1+\delta)\mu}\right] < \mathbb{E}[e^{tX}] / e^{t(1+\delta)\mu}$$

- By independence:

$$\mathbb{E}[e^{tX}] = \mathbb{E}\left[e^{t \sum_i X_i}\right] = \mathbb{E}\left[\prod_i e^{tX_i}\right] = \prod_i \mathbb{E}[e^{tX_i}]$$

- We will prove $\prod_i \mathbb{E}[e^{tX_i}] \leq e^{(e^t-1)\mu}$ in the next slide.
- For $t = \ln(1 + \delta)$:

$$\mathbb{E}[e^{tX}] / e^{t(1+\delta)\mu} \leq e^{(e^t-1)\mu} / e^{t(1+\delta)\mu} = \left[\frac{e^\delta}{(1 + \delta)^{1+\delta}}\right]^\mu$$
**Lemma**

\[ \prod_i \mathbb{E}[e^{tX_i}] \leq e^{(e^t - 1)\mu} \]

**Proof.**

- Using \(1 + x \leq e^x\):

  \[
  \mathbb{E}[e^{tX_i}] = p_i e^t + (1 - p_i) = 1 + p_i (e^t - 1) \leq \exp(p_i (e^t - 1))
  \]

- Using \(\mu = \mathbb{E} \left[ \sum_i X_i \right] = \sum_i p_i\):

  \[
  \prod_i \exp(p_i (e^t - 1)) = \exp(\sum_i p_i (e^t - 1)) = \exp((e^t - 1)\mu)
  \]

\[\square\]
Example 1

- Your sports team wins each game (independently) with prob. 1/4.
- What’s probability that they win at least half of their $n$ games.
Outline

Chernoff Bounds

Schwartz-Zippel
Checking Polynomial Multiplication via Schwartz-Zippel

Problem
Given three \( n \) variable polynomials \( P_1, P_2, P_3 \). Can you test if

\[
P_1(x_1, \ldots, x_n) \times P_2(x_1, \ldots, x_n) = P_3(x_1, \ldots, x_n)
\]

faster than multiplying the polynomials? Equivalently, is

\[
Q(x_1, \ldots, x_n) = P_1(x_1, \ldots, x_n) \times P_2(x_1, \ldots, x_n) - P_3(x_1, \ldots, x_n)
\]

zero for all \( x_1, \ldots, x_n \)?

Theorem (Schwartz-Zippel)
Let \( Q(x_1, \ldots, x_n) \) be a non-zero multivariate polynomial of total degree \( d \). Fix any finite set of values \( S \) and let \( r_1, \ldots, r_n \) be chosen independently and uniformly at random from \( S \). Then,

\[
\mathbb{P}[Q(r_1, \ldots, r_n) = 0] \leq \frac{d}{|S|}
\]
Schwartz-Zippel Proof

- Induction on $n$: For $n = 1$, because $Q$ has at most $d$ roots,
  \[ \mathbb{P}[Q(r_1) = 0] \leq d/|S| \]

- For induction step define $Q_i$ for $0 \leq i \leq k$:
  \[ Q(x_1, \ldots, x_n) = \sum_{i=0}^{k} x_1^i Q_i(x_2, \ldots, x_n) \]
  where $k$ is maximum such that $Q_k(x_2, \ldots, x_n) \neq 0$

- Since total degree of $Q_k$ is at most $d - k$,
  \[ \mathbb{P}[Q_k(r_2, \ldots, r_n) = 0] \leq (d - k)/|S| \]

- Consider $q(x) = Q(x, r_2, \ldots, r_n)$,
  \[ \mathbb{P}[q(r_1) = 0 | Q_k(r_2, \ldots, r_n) \neq 0] \leq k/|S| \]

- Putting together gives $\mathbb{P}[Q(r_1, \ldots, r_n) = 0]$ at most
  \[ \mathbb{P}[Q_k(r_2, \ldots, r_n) = 0] + \mathbb{P}[q(r_1) = 0 | Q_k(r_2, \ldots, r_n) \neq 0] \leq d/|S| \]
  where we used $\mathbb{P}[A] = \mathbb{P}[A \cap B] + \mathbb{P}[A \cap B^c] \leq \mathbb{P}[B] + \mathbb{P}[A | B^c]$