Last time: end of space unit:

Immerman-Szelepcsényi thm: AB 4.3.2, Sipser 8.6, Papad. 7.3 Cai 3.3

nondet space is closed under complement

↳ NL = co-NL

- Start randomized computation unit: Ca: 5.1

probability basics:

- Sample space S, probabilistic experiment
- dist $\mathcal{D}$ over S. $Pr[s]$ $Pr_{\mathcal{D}}[s]$
- Events. $A \subseteq S$ $\bar{A}$ = complem. of A
- Compound events: $A \wedge B$
- $Pr[A \wedge B] = Pr[A] \cdot \underbrace{Pr[B|A]}_{\text{condit. prob.}}$
- $Pr[A] \leq Pr[B] + Pr[A|\bar{B}]$
- Independence:
  $Pr[A \wedge B] = Pr[A] \cdot Pr[B]$
- Random variables $X: S \to \mathbb{R}$
- Expectation $\mathbb{E}[X] = \sum_{s \in S} X(s)\, \mathcal{D}(s)$
  $= \sum_a a \cdot Pr[X=a]$
- Linearity of expectation:
  for any random vars X_1, X_2 (not necc. indep.!),
  $\mathbb{E}[X_1 + X_2] = \mathbb{E}[X_1] + \mathbb{E}[X_2]$.

Ca: 5.1, course webpage

Today: • Tail bounds (Markov, Chebyshev, Chernoff, Hoeffding)

- Rand. alg. #1: fast rand alg for polynomial identity testing
- (start) rand. alg. #2: faster-than-2^n alg for 3CNF-SAT

→ Pap. 11.1, AB 7.2.3 (see also Sipser 10.2) Schöning '99 paper

No OH this week; use Ed Disc. for q's.

Questions?

Tail bounds:

"some $\overbrace{\text{event}}^{\text{r.v. } X \text{ is large/small}}$ has low prob."

Most basic: Markov's inequality.

Markov's ineq: Let X be a non-neg. r.v.

For any $k \geq 1$, have $\Pr\{X \geq \underbrace{k \cdot \mathbb{E}[X]}_{a}\} \leq \frac{1}{k}$.

Ex: let X = # children in a unif. random U.S. household.

Sps $\mathbb{E}[X] = 1.8$. Means must have $\Pr[X \leq 10] \leq .18$,

o/w $\mathbb{E}[X]$ couldn't be only 1.8.

Pf: equiv. to: $\Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}$.

Have

$$\mathbb{E}[X] = \sum_b b \cdot \Pr[X=b]$$

$$= \underbrace{\sum_{b:\, b<a} b \cdot \Pr[X=b]}_{\geq\, 0} + \sum_{b:\, b\geq a} b \cdot \Pr[X=b]$$

$$\geq 0 + \sum_{b:\, b \geq a} a \cdot \Pr[X=b]$$

$$= a \cdot \Pr[X \geq a]$$

What about r.v. that take neg. values

Recall: Variance of a r.v. X is

$$\mathrm{Var}[X] = \mathbb{E}[(X-\mu)^2], \text{ where}$$

$$\mu = \mathbb{E}[X]$$

(measures "spread")

Std dev of X: $\sigma(X) = \sqrt{\mathrm{Var}[X]} = \text{std-dev}(X)$

Chebyshev's inequality: For any r.v. X, have

$$\Pr[|X-\mu| \geq a] \leq \frac{\mathrm{Var}[X]}{a^2}.$$

Pf: $\Pr[|X-\mu| \geq a] = \Pr[(X-\mu)^2 \geq a^2]$

$\leq \frac{\mathrm{Var}[X]}{a^2}$ by Markov on $(X-\mu)^2$.

Intuitive statement of Cheby: every r.v. X deviates from its mean by $\geq t$ std dev's w.p. $\leq 1/t^2$.

Above bds: very general, not very strong.

For rv's X that are sums of many indep. RVs, much stronger tail bounds hold. Here's one:

"multiplicative"

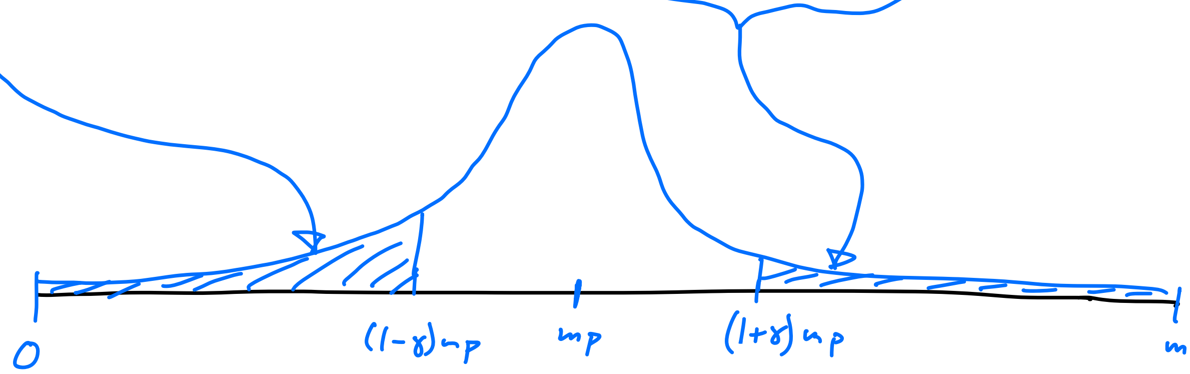
"Chernoff bound": Let $X_1, \dots, X_m$ be $\overbrace{\text{i.i.d.}}^{\text{independent, identically distributed}}$ $\underbrace{\text{Bernoulli}}_{0/1}$ r.v.'s with $\Pr[X_i = 1] = p$ for all i.

Let $X = X_1 + \dots + X_m$ (so $\mathbb{E}[X] = pm$)

Then for all $0 \le \gamma \le 1$

$$\Pr[X \le \underline{(1-\gamma)}mp] \le \exp\left(-\tfrac{1}{2}\cdot\gamma^2\cdot mp\right),$$

$$\Pr[X \ge \underline{(1+\gamma)}mp] \le \exp\left(-\tfrac{1}{3}\cdot\gamma^2\cdot mp\right)$$



---

additive

<u>Hoeffding bound</u>: Let $X_1, \dots, X_m$ as above.

Let $\hat{p} = \frac{1}{m}(X_1 + \dots + X_m)$. Then

$$\Pr[\hat{p} - p \ge \varepsilon] \le \exp(-2m\varepsilon^2)$$

$$\Pr[p - \hat{p} \geq \varepsilon] \leq \exp(-2m\varepsilon^2).$$

Rand. alg. for identity testing

ID-TEST: input is $\overset{p,\,q}{2}$ $\overbrace{\text{multivariate algebraic expressions}}^{\text{algebraic formulas}}$ formed with $+, -, \times$: e.g. (coeff in $\mathbb{N}$)

$$p(x_1, \ldots, x_\ell) = ((x_1 + x_2) \cdot (3x_1 - 2x_4) + (5(x_1 + 6 \cdot (x_3 \cdot (x_4 - x_2))) - 7x_5) \cdot (x_4 - x_8))$$

$$q(x_1, \ldots, x_\ell) = (x_1 - x_2) \cdot (x_3 - x_4) \cdot (x_5 - x_6)$$

(Think of domain as $\mathbb{R}$)

Question: is $p \equiv q$? (if we were to expand them out into "canonical form"

$$\sum_{a_1, \ldots, a_\ell \in \mathbb{N}} c_{a_1, \ldots, a_\ell} \, x_1^{a_1} x_2^{a_2} \cdots x_\ell^{a_\ell},$$

they'd be the same)

<u>Ex:</u> $p = x \cdot x - y \cdot y$
$q = (x-2y)\cdot(x+2y) + 3y^2$ } YES

How to solve?

<u>1st try:</u> expand out p, q.
Too Inefficient:
$p = (x_1+x_2)(x_3+x_4)\ldots(x_{\ell-1}+x_\ell)$, expanded out, has $2^{\ell/2}$ monomials

<u>2nd try:</u> plug in values $\bar{\alpha} = (\alpha_1, \ldots, \alpha_\ell)$ for $x_1, \ldots, x_\ell$.
If $p(\alpha) \neq q(\alpha)$: ☺ know answer is NO.
If $p(\alpha) = q(\alpha)$: not sure.

Doing this deterministically won't work: for any fixed α, there's a p, q pair that it "fools."
e.g. $\alpha = (1,2,3)$

$p = x_1 + x_2 + x_3$ $\quad$ $q = x_1 \cdot x_2 \cdot x_3$
$\quad 6 \quad\quad\quad\quad 6$

Right approach: tweak by picking α randomly.

The alg:

$p = x_1 + x_2 + x_3$ $\quad$ $\alpha_1 = 4$, $\alpha_2 = 2$, $\alpha_3 = 6$

$p(\bar{\alpha}) = 4 + 2 + 6$

Input: $p(x_1, \dots, x_\ell)$ & $q(x_1, \dots, x_\ell)$

- Let $m = \underset{\text{length of } p}{|p|} + |q|$, $M = 2^m$
- Choose $\underline{\alpha_1, \dots, \alpha_\ell}$ indep. & unif. from $\underline{S = \{1, \dots, M\}}$
- Evaluate $\underset{= p(\alpha_1, \dots, \alpha_\ell)}{p(\bar{\alpha})}$, $q(\alpha)$
- output "SAME" if $p(\alpha) = q(\alpha)$,
  "DIFFERENT" if $p(\alpha) \neq q(\alpha)$.

Claim 1: If $p \equiv q$, alg says SAME w.p. 1.

Claim 2: If $p \not\equiv q$, then $\Pr[\text{alg says SAME}] \le \frac{m}{M} = \frac{m}{2^m}$.

Note: this holds for all $p \not\equiv q$;
Rand. is over coin tosses of the alg.

To do: Claim 2 pf. Idea:

- deg of p, q can't be too high; so $r = p - q$ can't have too high degree
- "low" deg r can't have many roots, so prob. α <u>is</u> a root (i.e. $p(\alpha) = q(\alpha)$) is low.

<u>Degree</u> of a multivariable polynomial: max deg of any monom. in canonical form of the poly.

(deg of multivariate monom: sum of indiv. var. deg's).

$$p = x^4 y^3 + 4x^6 - x^3 yz \quad : \quad \deg(p) = 7$$

<u>Lemma</u>: If r is an alg. formula, $\deg(r) \le |r|$.

<u>Pf</u>: easy induction ($x \cdot x \cdot x \cdot x \cdot x$ length 5, degree 5).

Key: <u>Schwarz-Zippel lemma</u>:

<u>S-Z lemma</u>: Let S be any finite set of #s. Let $r(x_1, \dots, x_n)$ be a not identically 0 poly.

Then

$$\Pr_{\alpha_1,\dots,\alpha_n \sim S}\left[r(\alpha_1,\dots,\alpha_n)=0\right] \le \frac{\deg(r)}{|S|}.$$

Pf: next time: