Last time:

Cai: 5.1, course webpage

- Tail bounds (Markov, Chebyshev, Chernoff, Hoeffding)
- Rand. alg. #1: fast rand alg for polynomial identity testing

Pap. 11.1, AB 7.2.3 (see also Sipser 10.2)

Today:

- finish
- rand. alg. #2: faster-than-2^n alg for 3CNF-SAT

1.5"

Schöning '99 paper

- start rand. complexity classes

Pap. 11.2, AB 7.3, Cai 5.4

Questions?

Recall:

Schwarz-Zippel lemma: Let S be any finite set of #s. Let $r(x_1, \dots, x_n)$ be a not identically 0 poly. Then

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

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

(Given S-Z lemma, Claim 2 is immediate: apply SZ to $r = p - q$. Have $\deg(r) = \deg(p-q) \le |p| + |q| \le m$, $|S| = M = 2^m$.)

Proof of SZ:

induc. on n.

$n=1$: SZ says for poly $r(x)$: have $\Pr_{\alpha\sim S}[r(\alpha)=0] \le \frac{\deg(r)}{|S|}$

True from standard fact that a deg-d univ. real poly. has $\le d$ root.

Suppose (induc.) SZ true for $(n-1)$-var polys

Have $r(x_1,\dots,x_n)$. Factor out x_n from each monom:

write $r(x_1,\dots,x_n)$ as

$$\sum_{i=0}^{K} r_i(x_1,\dots,x_{n-1})\cdot(x_n)^i,$$ where

$K \le \deg(r)$ is max deg of x_n in any monom.

Note

- $r_K(x_1,\dots,x_{n-1}) \not\equiv 0$ (not id-0).
- $\deg(r_K) + K \le \deg(r)$

Recall

$$\Pr[\overset{r(\alpha_1,\dots,\alpha_n=0)}{A}] \le \Pr[\overset{r_K(\alpha_1,\dots,\alpha_{n-1})=0}{B}] + \Pr[A \mid \bar{B}]$$

So

$$\Pr[r(\alpha_1,\dots,\alpha_n)=0] \le \Pr[r_K(\alpha_1,\dots,\alpha_{n-1})=0] + \Pr[r(\alpha_1,\dots,\alpha_n)=0 \mid r_K(\alpha_1,\dots,\alpha_{n-1})\neq 0]$$

$\le \frac{\deg(r_K)}{|S|}$, by IH $\qquad\qquad \le \frac{K}{|S|}$, by base case:

for each fixed outcome of $(\alpha_1, \dots, \alpha_{n-1})$ s.t. $r_k(\alpha_1, \dots, \alpha_{n-1}) \neq 0$,

$\sum_{i=0}^{k} r_i(\underset{\alpha_1}{x_1}, \dots, \underset{\alpha_{n-1}}{x_{n-1}}) \cdot (x_n)^i$ is a not-ident.-0 deg-k poly in one var, x_n

So $\Pr[r(\alpha_1, \dots, \alpha_n) = 0] \leq \dfrac{\deg(r_k) + k}{|S|} \leq \dfrac{\deg(r)}{|S|}$. ■

Fact: Known that to give <u>det</u> algs for ID-TEST, will require proving ckt lower bounds.

Second rand. alg.: faster than brute force rand alg for 3CNF SAT.

3CNF: $\{\phi : \phi \text{ is a satisfiable 3CNF}\}$

$\phi = (x_1 \vee x_4 \vee \bar{x}_6) \wedge (x_2 \vee \bar{x}_3 \vee \bar{x}_5) \wedge (\bar{x}_2 \vee \bar{x}_4 \vee x_5) \wedge (x_1 \vee x_2 \vee x_3)$.

NPC; don't expect poly(n) time alg (even rand.)

Search problem: given ϕ, say "unsat" or (correctly) output sat asst.

/

Here's a rand alg: C_i = clause

TRY: Input: $\phi = C_1 \wedge \ldots \wedge C_m$ on n vars

1) Rand. pick uniform initial asst $z \in \{0,1\}^n$
2) Repeat $n/4$ times:
   - if $\phi(z) = 1$, :) stop & output z
   - if $\phi(z) = 0$, some $C_i(z) = 0$; let C be any such clause. Pick a unif. rand. one of the 3 literals in C, & flip that bit of z.

Ex: sps ϕ as above, $z = 0\underline{0}0111$, pick $C = C_4$
$C_4 = x_1 \vee x_2 \vee x_3$. Rand pick z_3 to flip; new z becomes $00\underline{1}111$

Claim 1: if ϕ unsat, TRY surely does not output a s.a.

Claim 2: if ϕ is satisfiable,

$\Pr[\text{TRY outputs a s.a.}] \geq \frac{1}{N}$, $N \leq \text{poly}(n) \cdot \left(\frac{3}{2}\right)^n$.

Given C2, our overall alg: do $\ell \cdot N$ indep. rep. of TRY.

If no s.a., we'll be correct;

if $\exists$ s.a.,

$$\Pr[\ell \cdot N \text{ rep. of TRY all don't find a s.a.}] \le \left(1-\frac{1}{N}\right)^{\ell \cdot N} \le e^{-\ell}.$$

$x \geq 1$: $\left(1-\frac{1}{x}\right)^x \le \frac{1}{e}$

$\ell = n$

So this is $\text{poly}(n) \cdot N \le \text{poly}(n) \cdot \left(\frac{3}{2}\right)^n$ r. alg. for 3CNF SAT.

To show:

$$\boxed{\begin{array}{l} \underline{\text{Claim 2}}: \text{if } \phi \text{ is satisfiable,} \\ \Pr[\text{TRY outputs a s.a.}] \geq \frac{1}{N}, \quad N \le \text{poly}(n) \cdot \left(\frac{3}{2}\right)^n. \end{array}}$$

<u>Pf</u>: Sps ϕ is satisfiable. Fix a specific s.a. z^*.

Consider rand z from Step 1.

If z sat. ϕ, great; assume $\phi(z)=0$.

Define $k :=$ # bit pos. where z + z^* disagree.

TRY : Input : $\phi = C_1 \wedge \ldots \wedge C_m$ on n vars
1) Rand. pick uniform initial asst $z \in \{0,1\}^n$
2) Repeat $n/4$ times:
• if $\phi(z)=1$, " stop + output z
• if $\phi(z)=0$, some $C_i(z)=0$; let C be any such clause. Pick a unif. rand. one of the 3 literals in C, + flip that bit of z.

In each of the $n/4$ indep. rep. of loop, have $\geq \frac{1}{3}$ chance of "fixing" a bit in z to agree w/ corr. bit of z^* (decr. k by 1)

(unlikely, but possible)

Suppose, at first, $k = \frac{n}{4}$. Let $p = \Pr[\text{init. } k \text{ is } \frac{n}{4}]$

Suppose further each of the $\frac{n}{4}$ rep. of loop decr. k by 1. Then at last step $z = z^*$:).

$\Pr[\quad]$

So $\Pr[\text{TRY finds s.a.}] \geq p \cdot q$

Let's analyze:

what is q? It's $\geq \left(\frac{1}{3}\right)^{n/4}$ $\qquad n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n$

what is p? It's $\dfrac{\binom{n}{n/4}}{2^n}$.

follows from Stirling's approx. for $n!$:

Recall useful binom. coeff. fact:

$$\boxed{\begin{array}{l} \underline{\text{Fact:}} \text{ For any const } 0<\alpha<1, \binom{n}{\alpha n} \text{ is } = \text{to} \\ \quad n^{\pm\Theta(1)} \cdot 2^{H(\alpha)\cdot n}, \quad H(\alpha) = \alpha \log\frac{1}{\alpha} + (1-\alpha)\log\frac{1}{1-\alpha} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{"}\log\text{"} = \log_2 \\ \quad \text{"binary entropy function".} \end{array}}$$

So, ignoring $n^{\pm\Theta(1)}$,

$$p \cdot q \geq \frac{\binom{n}{n/4}}{2^n} \cdot \frac{1}{3^{n/4}}$$

$\log 4 = 2$, so
$\frac{1}{4}\log 4 = \frac{1}{2}$, so

$$\approx \frac{2^{\left(\frac{1}{4}\cdot\log 4 + \frac{3}{4}\cdot\log\frac{4}{3}\right)n}}{2^n} \cdot \frac{1}{3^{n/4}}$$

$$= \frac{2^{\frac{n}{2}}}{2^n} \cdot \left(\frac{4}{3}\right)^{\frac{3}{4}n} \cdot \frac{1}{3^{n/4}}$$

$$= \frac{1}{2^{n/2}} \cdot \frac{\left(4^{3/4}\right)^n}{3^n} = \frac{1}{(4)^{\frac{n}{4}}} \cdot \frac{(4)^{\frac{3}{4}\cdot n}}{3^n}$$

$$= \left(\frac{4^{\frac{1}{2}}}{3}\right)^n = \left(\frac{2}{3}\right)^n,$$ as claimed.

Can tweak alg, + go for $3n$ steps rather than $n/4$: more detailed analysis gives $(4/3)^n$ in place of $(3/2)^n$.

Randomized Complexity Classes

Def: A probabilistic TM is a TM M with a special "coin flip" state q_{flip} s.t. when M enters q_{flip}, in next time step tape cell is rand. replaced w/ unif 0/1.

Alt. def: M gets extra read-only, move-right-only "random tape" filled w/ rand. bits.

· Can view as like NTM (binary-choice) but now \$ for nondet. choices.

A probabilistic poly-time (p.p.t.) TM: $\exists$ poly $p(n)$ s.t. M always halts in $p(n)$ steps (no matter how coin tosses came out).

Def Lang L is in RP (randomized P) if there's a p.p.t. TM M s.t. $\forall$ input x,

- if $x \in L$, $\Pr[M \text{ accepts } x] \geq \frac{1}{2}$
- if $x \notin L$, $\Pr[M \text{ acc } x] = 0$.

If RP machine for L accepts x: know $x \in L$.

· Rand over coin tosses; hold $\forall x$.

· Anal. to NP where "$\geq \frac{1}{2}$" $\Longleftrightarrow$ "> 0".

<u>Def</u> Lang L is in coRP if there's a p.p.t. TM M s.t. $\forall$ input x,

- if $x \in L$, $\Pr[M \text{ accepts } x] = 1$
- if $x \notin L$, $\Pr[M \text{ acc } x] \leq \frac{1}{2}$.

If coRP machine for L <u>rejects</u> x: <u>know</u> $x \notin L$.

IO-TEST in co-RP: only errs on inputs not in L.

Next time: RP, co-RP amplif.

ZPP

BPP

nonuniformity

poly-time hierarchy
