Last time: 1) Finish randomized P/poly alg. analysis (Schwartz-Zippel lemma)
2) Rand. poly-time alg; no known det. poly-time alg.
3) Randomized alg. to solve 3CNF satisfiability in \( \tilde{O}\left(\frac{3^k}{2k}\right) \) time (better than trivial \( 2^k \) time!)

Today: • Finish \( \tilde{O}\left(\frac{3^k}{2k}\right) \) time rand. alg. for 3CNF sat.

• Basics of randomized complexity classes:
  \textbf{RP, coRP, ZPP, BPP, (PP)}

Readings: Pap. 11.2, AB 7.3, Cai 5.4

Reminder: midterm due 11:59 pm Fri (no late days)

Questions?

Recall our TRY alg:

\textbf{TRY: Input: 3CNF } \Phi = C_1, \ldots, C_m \text{ on } n \text{ vars.}
1) Choose } \bar{x} \text{ at random}
2) Repeat } 1/4 \text{ times:
   • if } \Phi(\bar{x}) = 1 \text{, stop and output } \bar{x}
   • if } \Phi(\bar{x}) = 0 \text{, choose any clause } C_i \text{, let } \bar{x}_i \text{ be sat. by } \bar{x}
   Pick a random literal in } C_i \text{ and flip that bit of } \bar{x}
3) If did not succeed in } 8 \text{ repetitions, output } \bar{x}

We'll show:

\underline{Claim 2:} Sps } \Phi \text{ is satisfiable. Then }
\Pr[\text{TRY outputs a sat. } \bar{x} \text{ st } ] > \frac{1}{N},
\text{ where } N \leq \text{poly}(n) \cdot \left(\frac{3^k}{2k}\right)^k.

\underline{Pf:}
• Sps } \Phi \text{ is satisfiable. Fix } \bar{x}^* \text{ to be a part. s.t.}
  \text{ Let } \bar{z} \in \{0,1\}^n \text{ be osst. from Step 2.}
  \text{ If } \bar{z} \text{ sat } \Phi: \;
  \text{ Assume } \bar{z} \text{ doesn't sat. } \Phi.
  \text{ So } \bar{z} \text{ differs from } \bar{x}^* \text{ in some } i \text{ s.t. } \Phi(\bar{x}^*) \neq \Phi(\bar{z})
bit positions. In step 2, when we choose a $C_i$ that $z$ doesn’t satisfy, at least one of $C_i$’s 3 bits must be set different in $z^*$ vs $z$. So choosing a bit in $C_i$ randomly, we have $\frac{1}{3}$ chance of “fixing” a bit in $z$ to agree with $z^*$.

* Suppose $k = \frac{3}{4}$. ($z$ diff from $z^*$ in $\frac{3}{4}$ pos.) ($\frac{3}{4}$, but possible.)

In each of the $\frac{3}{4}$ repetitions, $\text{TRY}$ performs, either win $\square$ or have $\geq \frac{1}{3}$ chance of fixing a pos. ($k$ decr. by 1). So assuming $P_C$ after $\frac{3}{4}$ steps, fixed all $\frac{3}{4}$ pos. (one at $z^* = (\frac{1}{3})^{\frac{3}{4}}$.

Let $p = Pr[k = \frac{3}{4}]$. Have

$Pr[\text{TRY} \text{ } \text{finds } \text{ a set } \text{ at } \text{ st } ] \geq p \cdot \left(\frac{1}{3}\right)^{\frac{3}{4}}.$

What’s $p$? $p = Pr[\text{r fair } \mathbb{S} \text{ } \text{yield exactly } \frac{3}{4}]$.

$p = \left(\frac{n}{\frac{3}{4}}\right)^{\frac{3}{4}}.$ So $2^{-\frac{3}{4}} = \frac{n^{\frac{3}{4}}}{(\frac{3}{4})!} \cdot \frac{1}{2^{\frac{3}{4}}}$.

We use a useful fact about binomial coeff (follows from Stirling’s approx for $n!$, which says

$n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n.$

We use a useful fact about binomial coeff (follows from Stirling’s approx for $n!$, which says

$$n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n.$$
\[ H(\alpha) = \text{binary entropy} \]

\[ H(\alpha) = \alpha \cdot \log_2 \frac{1}{\alpha} + (1-\alpha) \log_2 \frac{1}{1-\alpha}. \]

So we have (ignoring the poly(\(n\)) mult. factor)

\[ P \cdot \frac{1}{3^{\frac{1}{14}}} = \frac{(\frac{4}{3})}{2^{\frac{1}{2}}} \cdot \frac{1}{3^{\frac{1}{14}}} \cdot \frac{1}{2^n} = \frac{H(\frac{4}{3})}{2^n} \cdot \frac{1}{3^{\frac{1}{14}}} \]

\[ = \frac{1}{2^n} \cdot \left(\frac{4}{3}\right)^{\frac{3}{4}} \cdot \frac{1}{3^{\frac{1}{14}}} \]

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

\[ = \left(\frac{4^{\frac{1}{2}}}{3}\right)^n = \left(\frac{2}{3}\right)^n. \]

So \( Pr \left[ \text{TRY \(s_{\text{eq}}\)} \right] \geq \frac{1}{N} \quad \text{where} \]

\[ N \leq \text{poly}(n) \cdot \left(\frac{3}{2}\right)^n. \]
Can do a tighter analysis: replace the \( \frac{n}{4} \) steps that you allow the \( \frac{c}{2} \) by \( 3n \) steps.

Take adv. of fact that \( 3n \) step RW can

\[
\frac{\epsilon}{3} \to \frac{\epsilon}{3}
\]

start a little further than \( \frac{\epsilon}{4} \) from 0 \& have a decent chance of reaching 0.

Turns out \( P_r[\text{modified TRY outputs s.a.}] \geq \frac{1}{N}, N \leq \text{poly}(n) \cdot \left(\frac{4}{5}\right)^n \).

---

**Rand Cxity Classes**

- **Def**: A probabilistic TM is a TM with a special "coin flip" state \( q_{flip} \), coin toss tape: when Mentors the coin flip state \( q_{flip} \), the cell on is replaced w/ a uniform rand. 0/1.
  
  Alt. def: prob. TM \( M \) has an extra read-only, move-R only tape filled w/ uniform rand. bits.

\( \Rightarrow \) can think of prob. TM as like an NTM but where NTM has binary nondet., \( \& \) nondet. choices made randomly.
A \text{prob. poly-time TM} (\text{p.p.t. TM}) is a prob TM s.t. \exists \text{ poly p(h)} s.t. M always halts in p(h) time (no matter how coins land).

\textbf{Def: } RP (randomized poly time):
A lang. \( L \) is \( \in \text{RP} \) means: there's a p.p.t. TM \( M \) s.t. \( \forall x \),
\[ M_{\text{acc}} x: \text{ know } x \notin L \quad \Rightarrow \quad \Pr [M_{\text{acc}} x] \geq \frac{1}{2} \]
\[ M_{\text{rej}} x: \text{ not sure } \quad x \notin L \quad \Rightarrow \quad \Pr [M_{\text{acc}} x] = 0. \]

\( \blacklozenge \) Holds \( \forall x \); rand. over \( \$ \)
\( \blacklozenge \) Like NP: NP machine said to acc. if any acc path exist. RP machine acc. if \( \geq \frac{1}{2} \) all comp. paths are acc paths.

\textbf{Def: } \( L \subseteq \text{coRP} \) if \( \overline{L} \in \text{RP} \), i.e. \( \exists \text{ p.p.t TM M} \)
\[ M_{\text{acc}} x: \text{ not sure } \quad x \in L \quad \Rightarrow \quad \Pr [M_{\text{acc}} x] = 1 \]
\[ M_{\text{rej}} x: \text{ know } \quad x \notin L \quad \Rightarrow \quad \Pr [M_{\text{acc}} x] \leq \frac{1}{2}. \]

\( \text{IO-TEST} = \{ (p,q): p,q \text{ alg. formulas s.t. } p \equiv q \} \)
\[ \in \text{coRP: } \text{ if } p(x) \neq q(x), \text{ know } (p,q) \notin \text{IO-TEST} \]

```
"RP amplification": can replace \( \frac{1}{2} \) with \( \frac{2}{3} \)
or even \( 1 - \frac{1}{3} p(h) \) \( p(h) \) any fixed poly.
```
+ doesn't change class of languages in RP.

**Proof:** Given $M$ as in orig RP def, let $M'$ be alg that runs $M$ $p(n)$ times on input $x$; $M'$ accepts if $M$ accepts on any of the $p(n)$ runs.

$x \notin \mathcal{L} \Rightarrow M$ rej on every run for sure, so

$\Pr \left[ M' \text{ acc } x \right] = 0 \checkmark$

$x \in \mathcal{L} \Rightarrow \Pr \left[ M \text{ rej every time} \right] \leq \frac{1}{2^p(n)}$.

---

**RP, co-RP:** always halt in poly time. *But may give errors.* In contrast with:

**ZPP:** **Def:** A lang $\mathcal{L}$ is in ZPP if there is a prob. TM $M$ & a fixed poly $p(n)$ s.t.

1. $\forall x, M$ never outputs wrong answer:

   $x \in \mathcal{L} \Rightarrow \Pr \left[ M \text{ rej } x \right] = 0$

   $x \notin \mathcal{L} \Rightarrow \Pr \left[ M \text{ acc } x \right] = 0$

2. $\forall x \in \Sigma^* \ni E \left[ \text{runtime of } M \text{ on } x \right] \leq p(n), \quad T(M, x)$

"zero-error prob. poly time."

---

**Thm:** $\text{RP} \cap \text{co-RP} = \text{ZPP.}$

**BPP, PP:** rel. between these classes, other classes.