Last time:

- finish fast rand alg for polynomial identity testing: Schwarz–Zippel (lemma)
- rand. alg. #2: $poly(n) \cdot (3/2)^n$-time alg for 3CNF-SAT
- start rand. complexity classes — Pap. 11.2, AB 7.3, Ca: 5.4 — RP, co-RP

Today:

- RP amplification
- ZPP, $ZPP = RP \cap co\text{-}RP$ — Pap 11.2, AB 7.5, Ca: 5.5
- BPP, BPP amplification
- PP, $NP \subseteq PP$
- relations among the above
- $BPP \subseteq P/poly$ (nonuniformity is at least as powerful as randomness)
- $BPP \subseteq PH$ (in fact, $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$)

Questions?

Recall: 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 $x \notin L$, $Pr[M \text{ acc } x] = 0$.

RP Amplif.: Can replace "$\frac{1}{2}$" in def. of RP w/ "$1 - 2^{-p(n)}$" for any poly $p(n)$, & doesn't change class of lang. in RP.

(co-RP: similar.)

Pf: Consider M': run orig. RP machine M $p(n)$ times on input $|x| = n$; M' accepts if any of the $p(n)$ runs of M accept.

$x \notin L \Rightarrow Pr[M' \text{acc}] = 0$ "

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

RP, co-RP: " always poly-time;
" can make mistakes.

ZPP: flips this.

Def: The class ZPP cont. those lang. L s.t. there is a prob. TM M for L, + a poly $p(n)$, s.t.

(1) $\forall x$, M never errs w.r.t. L ; +
$(M_{acc}\, x \overset{\text{w. prob.} > 0}{\Rightarrow} x \in L$;
$M_{rej}\, x \overset{\text{w. prob.} > 0}{\Rightarrow} x \notin L)$

(2) $\forall |x| = n$,
$E[T(M(x))] \leq p(n)$, where
$T(M(x))$ = time M runs for on x before acc. or rej.
random variable.

Note: poss that on some runs M may go for

$n^{\log n}$, or 2^n, or 2^{2^n}, ... time.

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

Pf: $RP \cap coRP \subseteq ZPP$: Fix $L \in RP \cap co\text{-}RP$.

Let M_1 = RP machine for L

M_2 = co-RP " " " . one "trial"

We construct ZPP M for L:

M runs M_1 & M_2 on x.

M: accepts if M_1 accepts;

rejects if M_2 rejects;

& if M_1 rej & M_2 accepts, M tries again (with fresh coin tosses).

Does this work? Yes:

- if M accepts x on any execution, must have M_1 acc x on some exec, so $x \in L$;
- if M rejects x on any execution, must have M_2 rej x on some exec, so $x \notin L$.

So (1) of ZPP def. holds.

(2): E[runtime of M]?

Whether $x \in L$ or $x \notin L$,

Pr[1st trial succeeds] $\geq \frac{1}{2}$

So E[# trials needed] $\leq$

$$\mathbb{E}[\#\text{ times need to toss fair coin before get } H]$$
$$= 1\cdot\tfrac{1}{2} + 2\cdot\tfrac{1}{4} + 3\cdot\tfrac{1}{8} + \cdots$$
$$\tfrac{1}{2} + \tfrac{1}{4} + \tfrac{1}{8} + \cdots = 1$$
$$+\ \tfrac{1}{4} + \tfrac{1}{8} + \cdots = \tfrac{1}{2}$$
$$+\ \tfrac{1}{8} + \cdots \quad \vdots \quad \Rightarrow 2$$

So $\mathbb{E}[\#\text{trials}] \le 2$, + $\mathbb{E}[\text{time}] \le 2 \cdot \max(\text{RP runtime} + \text{coRP runtime})$.

Now $ZPP \subseteq RP \cap coRP$.

Fix $L \in ZPP$, let M be ZPP machine w/ $p(n) = \mathbb{E}[\text{runtime}]$. We'll show $L \in RP$.

Let M' be the prob. TM that runs M on x for $\le 2p(n)$ steps, acc./rej. as M does; if M still running after $2p(n)$ steps, M' halts & rej. ($|x|=n$)

- $x \notin L$: M either rej in $\le 2p(n)$ steps or is still running; so M' rej. for sure.
- $x \in L$: since $\mathbb{E}[\text{runtime}] = p(n)$, by Markov know $\Pr[\text{runtime} > 2p(n)] < \frac{1}{2}$.

So M is RP machine for L.

Same arg gives L also in co-RP. 

ZPP is "stricter" than RP, co-RP.
A "looser" rand. C.C. :

Def $L \in BPP$ if $\exists$ p.p.t. TM M s.t.
$\forall x,$

$$x \in L \Rightarrow Pr[M(x) \text{ acc}] \geq 2/3$$
$$x \notin L \Rightarrow Pr[M(x) \text{ acc}] \leq 1/3.$$

} gap

Equiv. def. : $L \in BPP$ if $\exists$ det poly time TM M', poly $p(n)$ s.t. $\forall n$, $\forall |x|=n$,

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^{p(n)}}[M'(x,r) \text{ acc}] \geq 2/3$$

$$x \notin L \Rightarrow \Pr_{r \in \{0,1\}^{p(n)}}[M'(x,r) \text{ acc}] \leq \frac{1}{3}.$$

BPP is "feasible classical computation"

BPP amplif. : Can replace "$2/3$" in def "$\frac{1}{3}$"

with "$1-2^{-p(n)}$" " $2^{-p(n)}$ " ✝ doesn't change BPP.

Pf: Chernoff bd. Recall:

> "Chernoff bound" ("multiplicative"): Let $X_1, \dots, X_m$ be i.i.d. (independent, identically distributed) 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 $0 \le \gamma \le 1$
>
> $$\Pr[X \le (1-\gamma)mp] \le \exp(-\tfrac{1}{2}\cdot\gamma^2\cdot mp).$$

Run BPP alg $m = \Theta(p(n))$ times, acc iff # times it accepts $\ge \frac{m}{2}$.

Analysis: Sps. $x \in L$. (other case similar).

$\Pr[$ fewer than $m/2$ runs accept$]$ corr. to $\gamma = \frac{1}{4}$ (b/c $\frac{3}{4}\cdot\frac{2}{3} = \frac{1}{2}$), $p = 2/3$, so $\le e^{-\Omega(m)}$.

Other direc. (tiny gap) (last rand c.c.):

Def: $L \in PP$ if $\exists$ p.p.t. TM M s.t.

$$x \in L \Rightarrow \Pr[M(x) \text{ acc}] > \tfrac{1}{2};$$

$$x \notin L \Rightarrow \Pr[M(x) \text{ acc}] \leq \tfrac{1}{2}.$$

Not "feasible computation": if $L \in PP$ & have the ppt M, how do you eff. det. whether $x \in L$?

Obs: $NP \subseteq PP$.

Pf: Let $L \in NP$ with NTM M.
Here's a p.p.t. TM M':

- toss coin; accept if H. If T,
- run M, tossing coins for nondet choices.

M' puts $L \in PP$.

Relat. among these classes:

- $P \subseteq ZPP \subseteq \begin{matrix} RP \\ \cap \\ \text{co-RP} \end{matrix} \subseteq BPP$
- $RP \subseteq NP$
- $BPP \subseteq EXP$: enum. all seq. of coin tosses,

Keeping count of # acc/rej.

- $BPP \subseteq PSPACE$ (reuse space in)

- ? $BPP \subseteq NP$? don't know.

  ? $BPP = NEXP$? don't know.

  ($L \neq P$ or $P \neq PSPACE$.)

- Know: If $P = NP$, then $BPP = P$

  If $BPP = P$, then $BPP \neq EXP$.

  So either $P \neq NP$ or $BPP \neq EXP$.

- Most people think $P = BPP$... but hard to prove.

  Seems to often/sometimes happen that problems go from BPP to P...

'77: PRIMES $\in BPP$
'79: " $\in$ co-RP
'92: " $\in$ RP
'02: " $\in P$.

} so $\in ZPP$

Two results "upper bounding" BPP.

(1) $BPP \subseteq P/poly$ (2) $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

Thm: ; i.e. any $L \in BPP$ has poly-size circuits.

Pf idea: "Probabilistic method": existence proofs based on probability -- show that a rand object has nonzero prob. of having prop. P. This tells us an object w/ prop. P must exist, even though we don't know what it is!

Key idea: if an event has nonzero prob., the object it describes must exist.

Next time: use this to argue existence of poly-size ckts for any $L \in BPP$.

Also nexttime: counting problems.