Last time:
- RP amplification
- ZPP, $ZPP = RP \cap co\text{-}RP$
- BPP, BPP amplification
- PP, $NP \subseteq PP$
- relations among the above

Pap 11.2, AB 7.5, Ca: 5.5

Today:
- $BPP \subseteq P/poly$ (nonuniformity is at least as powerful as randomness)
- $BPP \subseteq PH$ (in fact, $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$)
- start unit on complexity of counting problems

Papad. 18.1, AB 17.1–17.3

PS 3 out today.

Questions? (Next Mon: video; Rocco's OH this week: by appt.)

1st result today: Theorem (Adleman):
$ZPP \subseteq BPP \subseteq P/poly$, i.e.
any $L \in BPP$ has poly-size circuits.

Pf: Let $L \in BPP$. Can assume (amplif.) that M, a p.p.t. TM for L, has error prob. $\leq \frac{1}{2^{n+1}}$ on each $|x| = n$. Can view M as det alg. taking x, r (r ← string of rand bits) as input. So

$\forall x$,

$$\Pr_r[M(x,r) \text{ is wrong}] \leq \frac{1}{2^{n+1}}.$$

But there are only 2^n x's w/ $|x|=n$. So (u.b.)

$$\Pr_r[M(x,r) \text{ is wrong on } \underline{\text{any}} \text{ on } |x|=n] \leq 2^n \cdot \frac{1}{2^{n+1}} < 1.$$

i.e. $\Pr_r[M(\cdot,r) \text{ is perfect}] > 0$. $M_r(x) = M(x,r)$

So there is an r^* s.t. M_r is perfect on all length-n inputs.

((Can view this in ckt terms: hardwire r^* into ckt corr. to $M(\cdot,\cdot)$ a la Cook-Levin.) ∎

2nd (last) rand. result:

Thm (Sipser; Gacs; Lautemann) $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$.

Pf: Enough to show $BPP \subseteq \Sigma_2^P$ (& recall BPP closed under complem.)

($L \in \Sigma_2^P$: $x \in L \Leftrightarrow \exists^P y \, \forall^P z \, [O(x,y,z) = 1]$) ← O: det poly-time

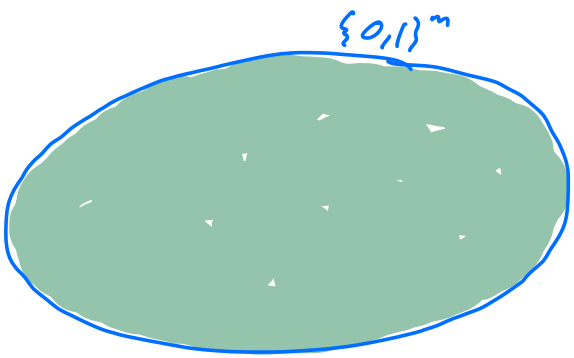
Fix $L \in BPP$. Ampl. $\Rightarrow \exists$ DTM $M(\cdot,\cdot)$ s.t. $\forall n$, $\forall |x| = n$, ($\exists$ poly $p(n)$)

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

$$x \notin L \Leftrightarrow \Pr_{r \in \{0,1\}^{p(n)}} [M(x,r) \text{ acc}] \leq 2^{-n}$$

Write $m = \text{poly}(n)$ for $p(n)$. For any given $|x| = n$, define $A(x) \subseteq \{0,1\}^m$ to be set of outcomes of r that cause M to accept (x,r).

$x \in L$:



$|A(x)| \geq 2^m (1 - 2^{-n})$

$x \notin L$:

$|A(x)| \leq 2^m \cdot 2^{-n}$

We'll argue that • if $A(x)$ very large, then "some collection of a few shifts of $A(x)$ cover everything";
• if $A(x)$ very small, then "no collection of a few shifts of $A(x)$ cover everything".

This will do the job to put $L \in \Sigma_2^P$.

Shifting:

Def: For 2 strings $u, v \in \{0,1\}^m$ ($\mathbb{F}_2^m$), the string "$u \oplus v$" is bitwise XOR of u & v.

$u = 00101$ $\quad u \oplus v = 10011$.
$v = 10110$

Def: Given $S \subseteq \{0,1\}^m$, the set "$S \oplus v$" is $\{u \oplus v : u \in S\}$.

Note $|S \oplus v| = |S|$.

Easy claim: (small sets) Let $m = \text{poly}(n)$. Let $S \subseteq \{0,1\}^m$ have $|S| \leq 2^{-n} \cdot 2^m$.

Then for any fixed coll. $u^{(1)}, \dots, u^{(m)}$ of m vectors in $\{0,1\}^m$, have

$$\bigcup_{i=1}^{m} (S \oplus u^{(i)}) \neq \{0,1\}^m.$$

($x \oplus x = 0^m \ \forall x \in \{0,1\}^m$)

Can't cover everything.

Pf: For each $i \in [m]$, have $|S \oplus u^{(i)}| \leq 2^{-n} \cdot 2^m$.

So

$$\left| \bigcup_{i=1}^{m} (S \oplus u^{(i)}) \right| \leq m \cdot 2^{-n} \cdot 2^m \ll 2^m.$$

b/c $m = \text{poly}(n)$

Claim abt large sets:

Claim: Let $S \subseteq \{0,1\}^m$ have $|S| \geq (1-2^{-n}) \cdot 2^m$.

Then there exist $u^{(1)}, \dots, u^{(m)} \in \{0,1\}^m$ s.t.

Can cover everything.

$$\bigcup_{i=1}^{m} (S \oplus u^{(i)}) = \{0,1\}^m.$$

Pf: Prob. method: argue that picking unif. rand. $u^{(1)}, \dots, u^{(m)}$ has excellent chance of working.

Rand. experiment: .

Fix any $z \in \{0,1\}^m$.

Let B_z = "bad" event that $z \notin \bigcup_{i=1}^{m} (S \oplus u^{(i)})$.

Fix $i \in [m]$: $z \notin S \oplus u^{(i)}$ iff $z \oplus u^{(i)} \notin S$. ($S \oplus u^{(i)} \oplus u^{(i)} = S$)

For unif rand $u^{(i)} \sim \{0,1\}^n$,

have that $z \oplus u^{(i)}$ is unif. random.

So $\Pr[z \oplus u^{(i)} \notin S] = \Pr[z \notin S \oplus u^{(i)}]$

$\leq 2^{-n}$. (by [redacted]).

for any fixed z,

So $\Pr[z \notin \bigcup_{i=1}^{m} (S \oplus u^{(i)})] \leq (2^{-n})^m$ (indep.)

↳ Really tiny!

So (u.b. over all z)

$\Pr[$any elt z of $\{0,1\}^n$ is not in $\bigcup_{i=1}^{m} S \oplus u^{(i)}]$

$\leq 2^n \cdot 2^{-nm} = 2^{-(n-1)m} < 1$.

So there exists an outcome $u^{(1)}, \ldots, u^{(m)}$ s.t.

$$\bigcup_{i=1}^{m} S \oplus u^{(i)} = \{0,1\}^n.$$ ∎

Let's apply these claims to $A(x)$.

- If $x \in L$, there is a set $u^{(1)}, \ldots, u^{(m)}$ s.t.

$$\bigcup_{i=1}^{m} (S \oplus u^{(i)}) = \{0,1\}^n ;$$

- If $x \notin L$, there is no set $u^{(1)}, \ldots, u^{(m)}$ s.t.

$$\bigcup_{i=1}^{m} (S \oplus u^{(i)}) = \{0,1\}^m .$$

So $\forall x$, have

$$x \in L \Leftrightarrow \exists u^{(1)}, \ldots, u^{(m)} \; \forall z \in \{0,1\}^m, \left[\bigvee_{i=1}^{m} M(x, z \oplus u^{(i)}) \text{ accepts} \right]$$

(this is our $D(x, u^{(i)}, z)$)

So $L \in \Sigma_2^P$. ∎

Note: if $P = NP$, then $\Sigma_2^P = P$ so $P \subseteq BPP \subseteq \Sigma_2^P = P$. ($P = NP \Rightarrow P = BPP$.)

Next unit: COUNTING

Problems where output is a #, not just Y/N.

Examples:

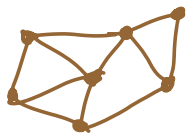
#SAT: input is a Bool form. $\varphi(x_1, \ldots, x_n)$

q: how many $x \in \{0,1\}^n$ have

$\varphi(x_1, \ldots, x_n) = 1$?

#CYCLES: input : undir. $G = (V, E)$

q: how many distinct cycles does G contain?



#PATHS: input G, s, t (dir.) ; q: how many distinct $s \rightsquigarrow t$ paths?

Motivations:

- network reliability
- combinatorial enum.
- statistical physics (config. of phys. systems)
- decision-making under uncertainty

Next time: #P, completeness, reductions, permanent.
