

AGENDA

0. Cook-Levin Revisited.
1. Example: PIT
2. $BPP \subseteq \Sigma_2$ (Sipser-Gacs - Lautemann)
3. Valiant Vazirani thm.

Recall: Last time, we introduced BPP, the class of languages we can PROBABLY efficiently decide, given randomness.

Big question: $P = BPP$?

Example: Polynomial identity testing.

Problem (PIT): Given a (description of) a polynomial $p(x_1, \dots, x_n)$ over a field $\mathbb{F}$, decide if p is identically 0.

Note: We can assume that the degree d of the p has $3d < |\mathbb{F}|$. Otherwise, embed p in a bigger field and the problem is unchanged.

LEMMA (Schwartz-Zippel)

Let $p(x_1, \dots, x_n)$ be a polynomial of total degree d over $\mathbb{F}$. For any $S \subseteq \mathbb{F}$, if $y_1, \dots, y_n$ are chosen unif. at random from S ,

$$\Pr\{p(y_1, \dots, y_n) = 0\} \leq d/|S|.$$

pf. HW.

Given SZ lemma, randomized alg for PIT:

- Choose $S \subseteq \mathbb{F}$ w/ $3d < |S| \leq \text{poly}(d)$
- Choose $y_1, \dots, y_n \in S$ randomly.
- If $p(y_1, \dots, y_n) = 0$, say "ZERO", else "NOT ZERO"

$$\Pr\{\text{incorrectly say ZERO}\} \leq d/|S| \leq 1/3$$

$$\Pr\{\text{incorrectly say NONZERO}\} = 0.$$

BIG QUESTION: Can you do this deterministically?

①

② $BPP \subseteq \Sigma_2$.

In addition to not knowing if $BPP = P$, there are tons of things we don't know about BPP. For example, the relationship of BPP w/ NP.

$$BPP \stackrel{?}{\subseteq} NP$$

$$NP \stackrel{?}{\subseteq} BPP$$

← on HW, show that $NP \subseteq BPP \Rightarrow NP = RP$

Last time we showed $BPP \subseteq P/\text{poly}$. But P/poly is HUGE.

Today, we won't quite show $BPP \subseteq NP$, but show something only a little worse.

And, it will imply $P = NP \Rightarrow P = BPP$.

L is in NP means $\exists$ polytime M ,

$$x \in L \Leftrightarrow \exists y, M(x, y) = 1$$

We need something a little more refined. Try

$$x \in L \Leftrightarrow \exists y \text{ s.t. } \forall z, M(x, y, z) = 1$$

DEF Σ_2 is the class of L s.t. $\exists$ polytime M , and poly $q(n)$ s.t.

$$\forall n, \forall x \in \Sigma^n$$

$$x \in L \Leftrightarrow \exists y \in \Sigma^{q(n)} \forall z \in \Sigma^{q(n)} M(x, y, z) = 1$$

Remark. Σ_2 is the second level of the POLYNOMIAL HIERARCHY. More on that later.

Fact: $NP \subseteq \Sigma_2$ (just have M ignore the string z)

LEMMA: If $P = NP$, then $\Sigma_2 = P$ also.

Proof Say $P = NP$. Say M is the TM for $L \in \Sigma_2$.

Then L_0 given by

$$(x, y) \in L_0 \Leftrightarrow \exists z \in \Sigma^{q(n)} M(x, y, z) = 0 \text{ is in } NP = P, \text{ so}$$

there's a polytime machine M_0 for L_0 . But then

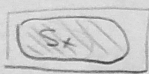
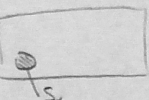
$$x \in L \Leftrightarrow \exists y \in \Sigma^{q(n)} (M_0(x, y) = 0)$$

so $L \in NP = P$. ✓

②

Thm (Sipser-Gacs-Lautemann) $BPP \subseteq \Sigma_2$. ③

Let $S_x = \{r : M(x, r) = 1\}$. Fix n , let $m = \text{poly}(n)$ be # random bits used.

If $x \in L$,  $|S_x| \geq (1 - 1/2^n) \cdot 2^m$
 If $x \notin L$,  $|S_x| \leq \frac{1}{2^n} \cdot 2^m$

Idea: find a bunch of "shifts" $\varphi_1, \dots, \varphi_k$ of these sets,
 many

If $x \in L$, $\exists \varphi_1, \dots, \varphi_k$ so that $\varphi_i(S_x)$ cover the whole thing.
 If $x \notin L$, $\nexists$ such.
 aka, $\forall r \in \{0, 1\}^m$ ()

This is exactly what we want:
 $x \in L \iff \exists y \forall z$ (polytime stuff of x, y, z)

Slightly more rigorously.

Fix $k = 1/m$ (still $\text{poly}(n)$). For $u \in \{0, 1\}^m$, define $\varphi_u(r) = r \oplus u$.

CLAIM: $\forall S \subseteq \{0, 1\}^m$ w/ $|S| \geq (1 - 1/2^n) \cdot 2^m$, $\exists$ k vectors $u_1, \dots, u_k$ s.t. $\bigcup_{i=1, \dots, k} \varphi_{u_i}(S) = \{0, 1\}^m$

PF Pick u_i at random.

$$\mathbb{P}(r \in \{0, 1\}^m \text{ doesn't get hit}) = \mathbb{P}(r \notin \varphi_{u_i}(S) \forall i) = \left(\frac{1}{2^n}\right)^k$$

$$\mathbb{P}(\exists r \text{ that doesn't get hit}) \leq \left(\frac{1}{2^n}\right)^k \cdot 2^m = 2^{m-kn} < 1$$

So there's some choice of u so that all r get hit.

CLAIM: $\forall S$ w/ $|S| \leq \frac{2^m}{2^n}$, $\forall k$ vectors $u_1, \dots, u_k$, $\bigcup_{i=1, \dots, k} \varphi_{u_i}(S) \neq \{0, 1\}^m$

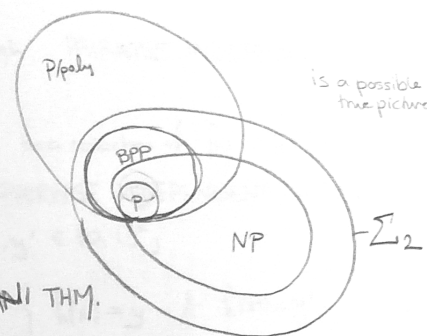
$$\text{PF } \left(\frac{2^m}{2^n}\right) \cdot k < 2^m \quad \checkmark$$

So then $\exists u_1, \dots, u_k \in \{0, 1\}^m$, $\forall r \in \{0, 1\}^m$, $r = \bigcup_{i=1, \dots, k} \varphi_{u_i}(S) \iff x \in L$

So $L \in \Sigma_2$.

COR $P = NP \implies BPP = P$

So now?



③ VALIANT-VAZIRANI THM.

Here's an example of how randomized complexity can teach us something about the deterministic world, via RANDOMIZED REDUCTIONS.

Recall $SAT = \{\varphi : \exists y. \varphi(y) = 1\}$ is NP-complete.

Consider

$$USAT = \{\varphi : \exists \text{ EXACTLY ONE } y \text{ s.t. } \varphi(y) = 1\}$$

Suppose someone promises me:

either $\varphi \in USAT$ or $\varphi \notin SAT$.

Then can I decide which?

On the surface, this seems easier, but...

THM Suppose there's a polytime M s.t.

$$M(\varphi) = \begin{cases} 1 & \varphi \in USAT \\ 0 & \varphi \notin SAT \\ \text{anything} & \text{else} \end{cases}$$

Then $NP = RP$.

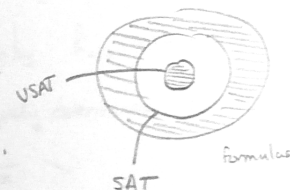
We think this is pretty unlikely, so it's unlikely that this problem is any easier! We'll actually show:

THM $\exists$ probabilistic polytime-computable f s.t. $\forall n, \forall$ nonvariable φ ,

$$\varphi \in SAT \implies \mathbb{P}\{f(\varphi) \in USAT\} \geq 1/8n$$

$$\varphi \notin SAT \implies \mathbb{P}\{f(\varphi) \in SAT\} = 0$$

This is a randomized reduction from SAT to "promise-USAT". Last week, if we wanted to say USAT was hard, we'd have to find a deterministic reduction. We don't know how to do that! But we can give this randomized reduction.



The proof goes through PAIRWISE INDEPENDENT HASH fns.

(5)

Def Let $H_{n,k}$ be a collection of fns $h: \{0,1\}^n \rightarrow \{0,1\}^k$.
 $H_{n,k}$ is PAIRWISE INDEPENDENT if $\forall x, x' \in \{0,1\}^n, x \neq x'$,
 and $\forall y, y' \in \{0,1\}^k$,

$$\prod_{h \in H_{n,k}} \{h(x)=y \wedge h(x')=y'\} = 2^{-2k}$$

h drawn uniformly

NOTICE. If $h(x), h(x')$ were independent, uniform random variables,
 then this probability would also be $(\frac{1}{2^k})^2 = 2^{-2k}$.
 So this says that $h(x), h(x')$ behave like independent random variables.

Example. Identify $\{0,1\}^n$ with $GF(2^n)$. (check if $GF(2^n)$ is OK)
 $H_{n,n} = \{h_{a,b} : a, b \in GF(2^n)\}$ given by $h_{a,b}(x) = ax + b$.

Indeed, if $ax' + b = y'$
 $ax + b = y$ then that uniquely determines a, b .

$$\text{so } \prod_h \{h(x)=y, h(x')=y'\} = \frac{1}{\#h's} = \frac{1}{2^{2n}}$$

And we can get these families for all n, k .

LEMMA. Let $H_{n,k}$ be pairwise indep hash family.

Choose $S = \{0,1\}^n$, and suppose $2^{k-2} \leq |S| \leq 2^{k-1}$.

Then $0 = \vec{0} = (0, \dots, 0)$

$$\mathbb{P}\{\exists \text{ unique } x \in S, h(x) = \vec{0}\} \geq 1/8$$

Proof Note $\mathbb{P}_h\{h(x)=h(x')=\vec{0}\} = \frac{1}{2^{2k}}$ and $\mathbb{P}_h\{h(x)=\vec{0}\} = \frac{1}{2^k}$

Let $N = |\{x : h(x) = \vec{0}\}|$

$$\sum_y \mathbb{P}\{h(x)=\vec{0} \wedge h(x')=y\}$$

By inclusion/exclusion

$$\begin{aligned} \mathbb{P}_h\{N \geq 1\} &\geq \sum_{x \in S} \mathbb{P}_h\{h(x)=\vec{0}\} - \sum_{\substack{x \neq x' \\ x, x' \in S}} \mathbb{P}_h\{h(x)=\vec{0} \wedge h(x')=\vec{0}\} \\ &= \frac{|S|}{2^k} - \binom{|S|}{2} \frac{1}{2^{2k}} \end{aligned}$$

aka, for each h ,
 $\mathbb{1}(\exists x, h(x)=\vec{0})$
 $\geq \sum_x \mathbb{1}_{h(x)=\vec{0}} - \sum_{x \neq x'} \mathbb{1}_{h(x)=\vec{0} \wedge h(x')=\vec{0}}$

$$\mathbb{P}(VA_1) = \sum_{i=1}^n (-1)^{i+1} \sum_{|A|=i} \mathbb{P}(A)$$

+ Bonferroni inequalities

and $\mathbb{P}_h\{N \geq 2\} \leq \binom{|S|}{2} \left(\frac{1}{2^{2k}}\right)$ by the union bd.

$$\text{So, } \mathbb{P}\{N=1\} = \mathbb{P}\{N \geq 1\} - \mathbb{P}\{N \geq 2\} \geq \frac{|S|}{2^k} - 2 \binom{|S|}{2} \frac{1}{2^{2k}} \geq \frac{|S|}{2^k} - \left(\frac{|S|}{2^k}\right)^2$$

Since $\frac{|S|}{2^k} \in [\frac{1}{4}, \frac{1}{2}]$, this is $\geq 1/8$.

Now we can prove the Valiant-Vazirani Thm.

Given φ on n vars, we want to map this to ψ , st $\varphi \in \text{SAT} \Rightarrow \psi$ maybe in SAT
 $\varphi \notin \text{SAT} \Rightarrow \psi \notin \text{SAT}$

Choose $k \in \{2, \dots, n+1\}$ randomly.

Fix a pairwise indep hash family $H_{n,k}$, choose $h \in H_{n,k}$.

Consider

$$\psi(x) = \varphi(x) \wedge (h(x)=\vec{0})$$

Notice, we do need a formula for $h(x)=\vec{0}$. We showed how to make one on Tuesday

If $\varphi \notin \text{SAT}$, $\psi \notin \text{SAT}$

If $\varphi \in \text{SAT}$, let $S = \{x : \varphi(x)=1\}$. Then $\mathbb{P}_k\{2^{k-2} \leq |S| \leq 2^{k-1}\} = 1/n$,
 and (by LEMMA)

$$\mathbb{P}_h(\exists \text{ unique } x \in S \text{ s.t. } h(x)=\vec{0} \mid 2^{k-2} \leq |S| \leq 2^{k-1}) \geq 1/8$$

so $\mathbb{P}_{h,k}(\exists \text{ unique } x \text{ s.t. } \psi(x)=0) \geq 1/8n$, and that's what we wanted.

(6)