Last time: Randomized Complexity Classes

RP : one-sided error, randomized polytime

BPP : two-sided error, randomized polytime

Also,

$ZPP = RP \cap coRP$: zero error, random. polytime

- either outputs the correct answer, or "don't know",
- $Pr[\text{"don't know"}] < \frac{1}{3}$.

Example of a co-RP algorithm:

Polynomial Identity Testing

Input: An algorithm a computing a multi-variate polynomial $p(x_1, \dots, x_n)$ of total degree $\leq d$.

Decide: Is $p(x_1, \dots, x_n) \equiv 0$?

Ex: $\prod_{i>j} (x_i - x_j)$ is an algorithm

$\prod_{\substack{i>j \\ i,j\in\{1,\dots,n\}}} (x_i - x_j)$ is an algorithm for a polynomial $p(x_1,\dots,x_n)$ of total degree $\le n$.

The degree of a polynomial:

$$p(x,y,z) = 10\cdot \underbrace{xyz^3}_{\deg 5} - 7\cdot \underbrace{y^5}_{\deg 5} + 13\cdot \underbrace{x^5y^6z^8}_{\deg 19}$$

total deg = max deg over all monomials

= 19

Schwartz-Zippel Lemma:

$\forall$ $p(x_1,\dots,x_n) \not\equiv 0$ of total degree $\le d$,

$\forall$ finite set $S \subseteq \mathbb{Z}$,

$$\Pr_{r_1,r_2,\dots,r_n\in S}\left[p(r_1,r_2,\dots,r_n)=0\right] \le \frac{d}{|S|}.$$

Proof (by induction on n):

Base case: $n=1$. $p(x)\not\equiv 0$ of deg $\le d$ can have $\le d$ roots.

can have $\leq d$ root's.

So, $\Pr_{r \in S}[p(r)=0] \leq \frac{d}{|S|}$.

Induction Step: Assume the statement is true for $\leq n$ variables. Prove for $n+1$ variables.

Idea: $p(x_1, \ldots, x_n, x_{n+1}) =$

$$\underbrace{q_0(x_1,\ldots,x_n)} + \underbrace{q_1(x_1,\ldots,x_n)} \cdot x_{n+1} + \underbrace{q_2(x_1,\ldots,x_n)} \cdot x_{n+1}^2 + \ldots + \underbrace{q_k(x_1,\ldots,x_n)} \cdot x_{n+1}^k$$

a polynomial in x_{n+1}, whose coefficients are polynomials $q_0, q_1, \ldots, q_k$ in $x_1, \ldots, x_n$.

Ex: $p(x_1, x_2, x_3) = 3 \cdot x_1 x_2^2 + 7 \cdot x_2^3 x_3^2 - 2 \cdot x_3^7$

$$= \underbrace{(3 x_1 x_2^2)}_{q_0} \cdot x_3^0 + 0 \cdot x_3^1 + \underbrace{(7 x_2^3)}_{q_2} \cdot x_3^2 + 0 \cdot x_3^3 + 0 \cdot x_3^4 + 0 \cdot x_3^5 + 0 \cdot x_3^6 - \underbrace{(2)}_{q_7} \cdot x_3^7$$

$$p(x_1, \ldots, x_n, x_{n+1}) = \sum_{i=1}^{k} q_i(x_1, \ldots, x_n) \cdot x_{n+1}^i$$

$$\Pr_{r_1, \ldots, r_{n+1} \in S}[p(r_1, \ldots, r_n, r_{n+1}) = 0] =$$

$$\Pr_{r_1,\dots,r_{n+1}\in S}[p(r_1,\dots,r_n,r_{n+1})=0] =$$

$$\Pr[\,p(r_1,\dots,r_{n+1})=0 \mid q_K(r_1,\dots,r_n)=0\,]\cdot \Pr[\,q_K(r_1,\dots,r_n)=0\,]$$

$$+$$

$$\Pr[\,p(r_1,\dots,r_{n+1})=0 \mid q_K(r_1,\dots,r_n)\neq 0\,]\cdot \Pr[\,q_K(r_1,\dots,r_n)\neq 0\,]$$

$$\leq \Pr[\,q_K(r_1,\dots,r_n)=0\,]$$

$$+ \Pr_{\substack{r_1,\dots,r_n\in S\\ r_{n+1}\in S}}[\,p(r_1,\dots,r_{n+1})=0 \mid q_K(r_1,\dots,r_n)\neq 0\,]$$

$$\leq \frac{\deg(q_K)}{|S|} + \frac{K}{|S|} = \frac{\deg(q_K)+K}{|S|} \leq \frac{d}{|S|}.$$

QED

Rand. algo for PIT

Given $\mathcal{C}$ for $p(x_1,\dots,x_n)$ of $\deg \leq d$.

Define $S = \{1,2,3,4,\dots,10\cdot d\}$

Pick ...

Define $S = \{1, 2, 3, 4, \ldots, 10 \cdot d\}$

Pick $r_1, r_2, \ldots, r_n \in S$ at random.

Output "Zero" iff $a(r_1, \ldots, r_n) = 0$.

<u>Open Problem</u>: Is there a <u>deterministic</u> polytime (or, even, sub-exponential-time) algo. for Poly Identity Testing?

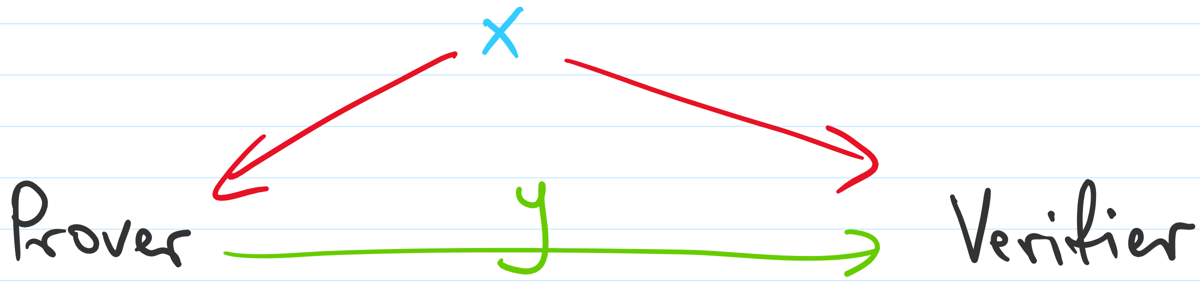
<u>Thm</u> [K., Impagliazzo]: If Poly Id. Test. is in P, then we get STRONG circuit lower bounds ($\approx NP \neq P$).

<u>Message</u>: Derandomizing BPP algorithms is impossible without, at the same time, proving new, strong complexity lower bounds.

$$\begin{tikzcd} \text{Complexity} \arrow[rr, bend left] & & \text{Algorithms} \arrow[ll, bend left] \end{tikzcd}$$

Randomness + Interaction : Interactive Proofs (IP)

NP :



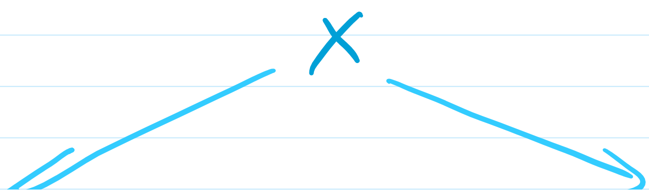
check that y is a valid witness for x

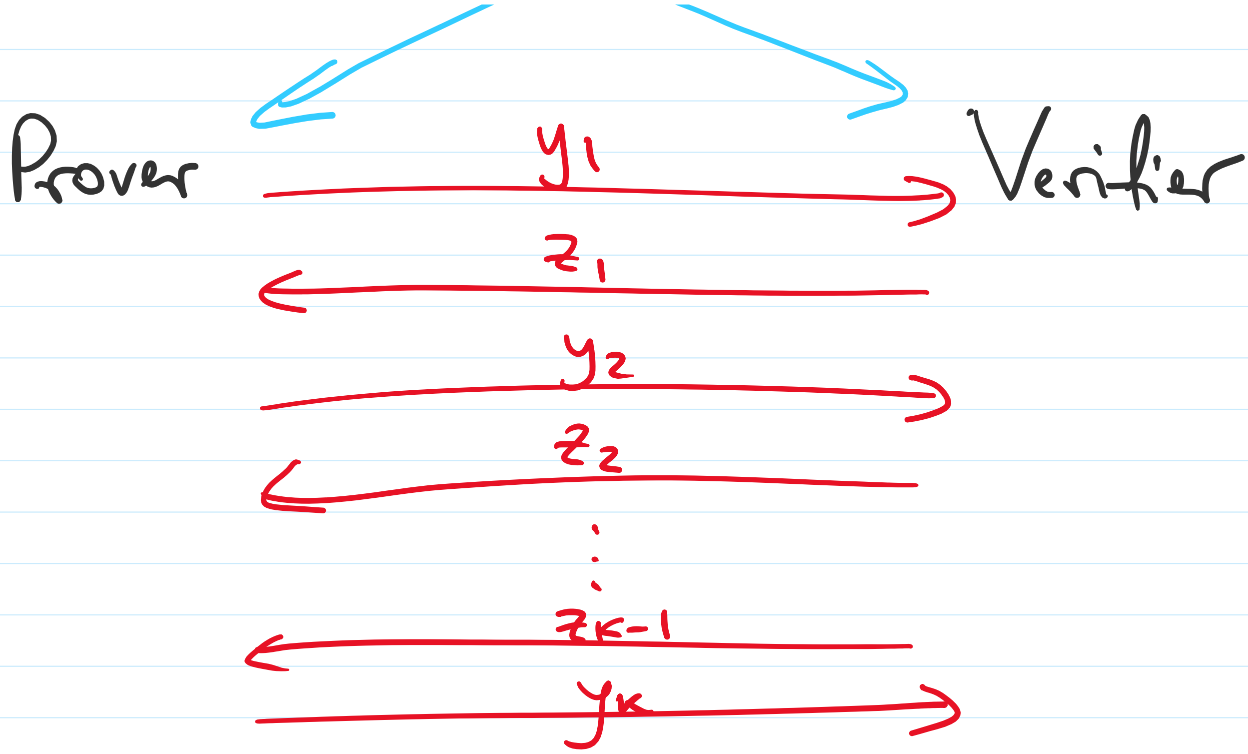
<u>Generalize in two ways :</u>

(1) allow Verifier to be a <u>randomized</u> poly time algorithm.

(2) allow many (polynomial number) of rounds of communication.

IP:



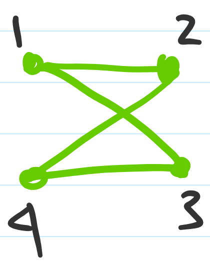


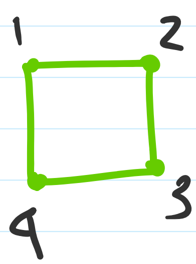
Example: Graph Non-Isomorphism

Given: $G_0 = (V_0, E_0)$

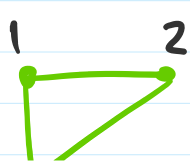
$G_1 = (V_1, E_1)$

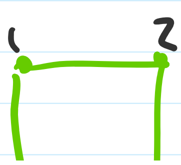
Decide: $G_0 \not\cong G_1$?



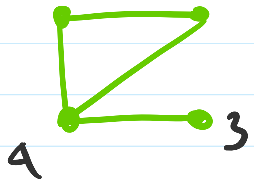


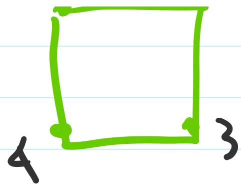
are isomorphic





are non-isomorphic.





are non-isomorphic.

IP-protocol for Graph Non Isomorphism

(G_0, G_1) both graph on n nodes $(1, 2, \dots, n)$

P $\qquad\qquad$ V

random $i \in \{0,1\}$
random permutation
$\pi : [n] \to [n]$

$\xleftarrow{\pi(G_i)}$

$\xrightarrow{j \in \{0,1\}}$

accept iff $j = i$

Correctness Analysis:

(1) $G_0 \not\cong G_1 \Rightarrow$

the prover can determine which of G_0 or G_1 is isomorphic to $\pi(G_i)$ & so can send $j = i$.

& so can send $j=i$.

(2) $G_0 \simeq G_1 \Rightarrow$

$\pi(G_0)$ is distributed the same as $\pi(G_1)$

So, Prover has no way to pick the correct $j=i$, except by randomly guessing $j \in \{0,1\}$. Hence, $\Pr[j=i] \leq \frac{1}{2}$.