BPP, RP, ZPP = RP $\cap$ coRP

Thm: If P = NP then P = BPP $BPP \subseteq NP^{SAT}$

Pf: Suppose $f \in BPP$.

$\exists\ M(x, r)$ $r \in \{0,1\}^m$

$\forall x \quad \Pr_r[M(x,r) = f(x)] \geq 1 - 2^{-2n}$.

Let $k = \lceil m/n \rceil \quad u_1, u_2, \ldots, u_k \in \{0,1\}^m$

Claim: $f(x) = 1 \iff$

$$\exists u_1, u_2, \ldots, u_k\ \forall r\ \ M(x, r \oplus u_1) = 1 \ \vee\ M(x, r \oplus u_2) = 1 \ \vee \cdots \vee\ M(x, r \oplus u_k) = 1$$

Pf: If $f(x) = 1$.

Fix r. Pick $u_1, \ldots, u_k$ uniformly.

$$\Pr[M(x, r \oplus u_1) = M(x, r \oplus u_2) = \cdots = M(x, r \oplus u_k) = 0] \leq 2^{-2nk} < 2^{-m}.$$

$\Rightarrow \exists u_1, \ldots, u_k\ \forall r\ \exists_i\ M(x, r \oplus u_i) = 1$

$f(x) = 0 \iff$

$$\forall u_1, \ldots, u_k\ \exists r\ \ M(x, r \oplus u_1) = 0 \ \wedge\ M(x, r \oplus u_2) = 0 \ \wedge \cdots \wedge\ M(x, r \oplus u_k) = 0$$

$\exists z\ C(y, z) \iff C'(y)$

$\exists u_1, \ldots, u_k\ C'(x, u_1, \ldots, u_k)$

$\downarrow$

$C''(x)$

If $f(x) = 0$.

Fix $u_1, \ldots, u_k$. Pick r uniformly.

$$\Pr[M(x, r \oplus u_1) = 1 \vee \cdots \vee M(x, r \oplus u_k) = 1] \leq k\, 2^{-n} < 1.$$

Eventually: IP = PSPACE.

Polynomial: $3x_1x_2^2 + 5x_2^2x_1 + x_2x_4$) degree 3 $\rightarrow$ poly over $\mathbb{F}_{13}$

Finite fields: finite set where you can add, multiply, divide.

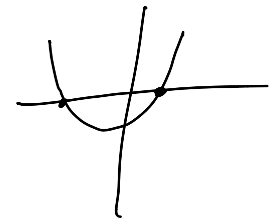
$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$

$xy \bmod p$

$x + y \bmod p$.

$\forall x,\ \exists x^{-1} \in \mathbb{F}_p$ s.t. $x \cdot x^{-1} = 1$.

FACT: If $p(x) \neq 0$ is a univariate poly of deg d then $p(x)$ has at most d roots.



$\Rightarrow \exists$ at most d points $a_1, \ldots, a_d$ s.t $p(a_i) = 0$.

$p(a) = 0 \Rightarrow X - a$ divides $p(x)$

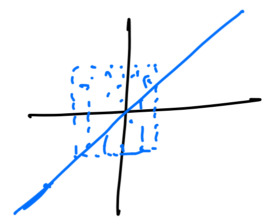
$p(a_1) = p(a_2) = \cdots = p(a_r) = 0 \iff (X - a_1)(X - a_2) \cdots (X - a_r)$ divides $p(x)$.

FACT: (Schwartz-Zippel)

If $p(x_1, \ldots, x_n)$ is deg d, S is any finite set
$\neq 0$

let $a_1, \ldots, a_n \in_R S$ $\quad \Pr[p(a_1, \ldots, a_n) = 0] \leq \frac{d}{|S|}$.

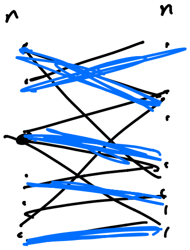
$p(x,y) = x - y$



$$\underset{n \times n \text{ matrix}}{\det(M)} = \sum_{\substack{\text{permutations} \\ \pi \text{ of } \{1,\ldots,n\}}} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i,\pi(i)}$$

FACT: $\det(M)$ can be computed by a circuit of size $\operatorname{poly}(n)$ and depth $O(\log^2 n)$.

Bipartite graph



Perfect matching: n disjoint edges.

Given G: does G have a p.m.?

Let M be the matrix where

$$M_{ij} = \begin{cases} x_{ij} & \text{if } (i,j) \in G \\ 0 & \text{o.w} \end{cases}$$

deg $n \to$ [$\det(M) = 0$ iff no p.m.

Let S be any set of $3n$ numbers

Sample $x_{ij} \in_R S$ compute $\det(M)$.

If no p.m $\Pr[\det = 0] = 1$.

If p.m $\Pr[\det = 0] \leq 1/3$.

Thm: Any arithmetic circuit of size s, deg r

$\Rightarrow$ circuit of size poly(s,r)

depth $O(\log r \cdot (\log r + \log s))$.