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

$\cup I$

$RP \subseteq NP$

$\cup I$

ZPP

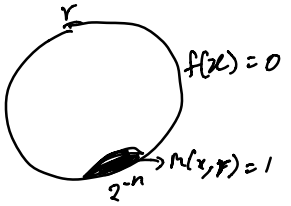
BPP has poly sized circuits.

Thm: $BPP \subseteq NP^{3SAT}$.

Pf: $f \in BPP$ via $M(x,r)$.

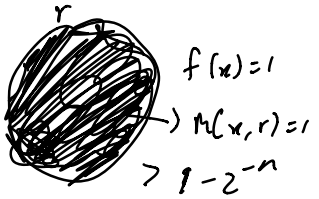
wlog $\Pr_r[M(x,r) = f(x)] > 1 - 2^{-n}$.

(r: m random bits)



$k \sim m/n$.

$u_1, \ldots, u_k \in \{0,1\}^m$



Claim 1: If $f(x) = 0$ $\forall$ choice of $u_1, \ldots, u_k$ $\exists$ r s.t. $M(x, r \oplus u_1), \ldots, M(x, r \oplus u_k) = 0$.

Pf: Pick r at random.

$$\Pr_r[M(x, r \oplus u_i) = 1] < 2^{-n}$$

$$\Rightarrow \Pr_r[M(x, r \oplus u_i) = 1 \text{ for some } i] < k \cdot 2^{-n} < 1$$

Claim 2: If $f(x) = 1$ there is a choice of $u_1, \ldots, u_k$ s.t. for every r $\exists i$ with $M(x, r \oplus u_i) = 1$.

Pf: Pick $u_1, \ldots, u_k$ uniformly at random.

$\forall$ r $\Pr[M(x, r \oplus u_1) = M(x, r \oplus u_2) = \cdots = M(x, r \oplus u_k) = 0]$

$$< (2^{-n})^k = 2^{-nk}.$$

$$\Pr_{u_1, \ldots, u_k}[\exists r \text{ s.t. } M(x, r \oplus u_1) = \cdots = M(x, r \oplus u_k) = 0] < 2^m \cdot 2^{-nk}.$$

$$= 2^{m - nk}.$$

$$< 1.$$

Choose $nk > m$.

NP 3SAT algorithm

- Guess $u_1, \ldots, u_k$.
- Using 3SAT call check

$$\forall r \bigvee_{i=1}^{k} M(x, r \oplus u_i) = 1$$

$$\Leftrightarrow \neg \exists r \bigvee_{i=1}^{k} M(x, r \oplus a_i) = 0$$

X ——— X

$IP = PSPACE$

$$P \subseteq NP \subseteq IP = PSPACE$$

X ——— X

Finite Field

$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ → p is prime number

$a, b \in \mathbb{F}_p$ $\quad a \cdot b = ab \bmod p$.

$a + b = a + b \bmod p$

$gcd(a, b) = ca + db$ → all 4 are integers.

$a \neq 0$, $a \in \mathbb{F}_p$ $\quad gcd(a, p) = 1 = ca + dp$

$\Rightarrow ca = 1 \bmod p$.

$b/a = bc$

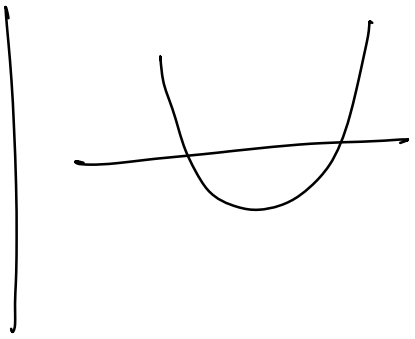
$\mathbb{F}_3$

$x^2 + 2x + 1$ ← deg 2.

FACT: deg d polynomial has at most d roots.

$f(x)$ deg d

⇒ are at most d inputs $r_1, \ldots, r_d$ s.t $f(r_i) = 0$.



pf: $f(a) = 0$

$\Rightarrow (x - a)$ divides $f(x)$.

$(x - r_1)(x - r_2) \cdots (x - r_d)$ divide $f(x)$.

$\rightarrow$ $f(x) = q(x) \cdot h(x) + r(x)$

$\downarrow$

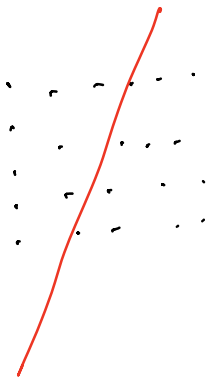
deg r < deg h.

Schwartz-Zippel lemma

$14x^{10}y^5z^8 - 3x^3y$ deg = 15.

$(x - y)$

$x^{10}(14y^5z^8) - x^3(3y)$



Lemma: Let $f(x_1, \ldots, x_n)$ be a poly of deg d, non-zero. Let S be any set of numbers. Let $a_1, \ldots, a_n \in S$ be uniformly random. Then $\Pr[f(a_1, \ldots, a_n) = 0] \leq \frac{d}{|S|}$.

Pf: When $n = 1$,

$$\Pr[f(a_1) = 0] \leq \frac{d}{|S|}.$$

In general

$$f(x_1, \ldots, x_n) = x_n^{\ell} \cdot q_{\ell}(x_1, \ldots, x_{n-1}) + x_n^{\ell-1} q_{\ell-1}(x_1, \ldots, x_{n-1}) + \cdots + x_n^0 q_0(x_1, \ldots, x_{n-1})$$

(q_{ℓ}: deg $\leq d - \ell$)

If $f(a_1, \ldots, a_n) = 0$

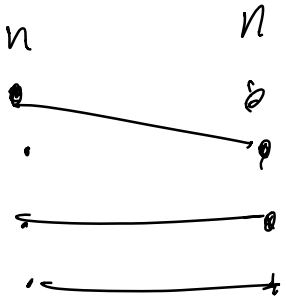
$\Rightarrow$ $q_{\ell}(a_1, \ldots, a_{n-1}) = 0 \rightarrow \Pr[\,] \leq \frac{d-\ell}{|S|}$

or $f(a_1, \ldots, a_n) = 0$ and $q_{\ell}(a_1, \ldots, a_{n-1}) \neq 0$

$$\Pr[\,] \leq \frac{\ell}{|S|}.$$

So $\Pr[f(a_1, \ldots, a_n) = 0] \leq \frac{d-\ell}{|S|} + \frac{\ell}{|S|} = \frac{d}{|S|}$.

Bipartite matching



Goal: Is there a perfect matching? (matching of size n.)

Given a matrix M

$$\det(M) = \sum_{\pi \in S_n} \text{sign}(\pi) \prod_{i=1}^{n} M_{i,\pi(i)}$$

$$M_{i,j} = \begin{cases} x_{i,j} & \text{if } i-j \text{ in graph} \\ 0 & \text{o.w.} \end{cases}$$

$\det(M) \neq 0$ iff $\exists$ perfect matching.

FACT: Can compute $\det(M)$ in $O(n^3)$ time, also $O(\log^2 n)$ depth circuit.

Algorithm Let $S = \{1, 2, 3, \ldots, 100n\}$

Pick $x_{i,j} \in S$.

Compute $\det(M)$.

$$\det\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = x_{11}x_{22} - x_{21}x_{12}$$

$$\det\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & 0 \end{pmatrix} = -x_{21}x_{12}$$