- Schwartz-Zippel Lemma.

If $p(x_1,\cdots,x_n)\in \mathbb{F}[x_1,\cdots,x_n]$ is a non-zero polynomial of degree d, then $\forall S\subseteq \mathbb{F}$, $\Pr_{a_i\in_R S}[p(a_1,\cdots,a_n)=0]\le \frac{d}{|S|}$.

Proof. Induction on n. $n=1$: # roots $\le$ deg for univariate polynomials.

Assume $\le n-1$ cases. For n: Rewrite $p(x_1,\cdots,x_n)=\sum_{i=0}^{d} x_1^i\, p_i(x_2,\cdots,x_n)$.

Take the largest i s.t. $p_i\not\equiv 0$. (Such i exists, o.w. $p\equiv 0$.)

Since $\deg(p)=d$, we know $\deg(p_i)=d-i$. Now

$$\Pr_{a_i\in_R S}[p(a_1,\cdots,a_n)=0]=\Pr[p(a_1,\cdots,a_n)=0,\ p_i(a_2,\cdots,a_n)=0] + \Pr[p(a_1,\cdots,a_n)=0,\ p_i(a_2,\cdots,a_n)\neq 0]$$

$$\le \underbrace{\Pr[p_i(a_2,\cdots,a_n)=0]}_{\le \frac{d-i}{|S|} \text{ by induction}} + \underbrace{\Pr[p(a_1,\cdots,a_n)=0 \mid p_i(a_2,\cdots,a_n)\neq 0]}_{\le \frac{i}{|S|} \text{ by induction } (p(x_1,a_2,\cdots,a_n) \text{ has deg } i)}$$

$$=\frac{d}{|S|}.\qquad \square$$

- Application to perfect matching detection.

Consider a bipartite graph $G=(L,R,E)$. A perfect matching is a collection of n edges s.t. each vertex in L or R occurs exactly once.

Associate a variable x_{ij} with each edge $(i,j)\in E$. Define the matrix A by $A_{ij}=\begin{cases} x_{ij} & (i,j)\in E\\ 0 & \text{o.w.}\end{cases}$. Consider $\det(A)$ as a polynomial of x_{ij}'s.

Thm. $\det(A)\not\equiv 0 \iff G$ has a perfect matching.

Pf. Recall $\det(A)=\sum_{\pi\in S_n}\mathrm{sign}(\pi)A_{1\pi(1)}A_{2\pi(2)}\cdots A_{n\pi(n)}$, and observe that there is no cancellation of summands (since π is a permutation). $\square$

So to detect whether G has a perfect matching, it suffices to pick a field $\mathbb{F}$ of size $|\mathbb{F}|\ge \frac{n}{\varepsilon}$, and to evaluate the polynomial $\det(A)$ on a random input $x_{ij}\in_R \mathbb{F}$, output "$\exists$ perfect matching" iff answer $\neq 0$.

This randomized algorithm has one-sided error ε.

- Random self-reducibility of Permanent.

Recall that the permanent of a matrix A is defined as

$$\mathrm{perm}(A) = \sum_{\pi \in S_n} a_{1\pi(1)} \cdots a_{n\pi(n)}.$$

Consider the following problem. Suppose that we're given an algorithm that can compute the permanent of $(1-\frac{1}{3n})$-fraction of $n\times n$ matrices over some finite field $\mathbb{F}$. Can we design an algorithm w/ worst-case error prob. $\le \frac{1}{3}$?

Here is how: Suppose A is the input matrix. Pick a random $R \in \mathbb{F}^{n\times n}$, and let $B(x) = A + x\cdot R$. Then $B(x)$ is a deg-n polynomial in x. Note that for any fixed $\underset{(a\neq 0)}{a \in \mathbb{F}}$, $B(a) = A + a\cdot R$ is a random matrix over $\mathbb{F}$, on which the given algorithm computes the permanent correctly w.p. $1-\frac{1}{3n}$. Let's do this for $(n+1)$ times, namely pick $(n+1)$ distinct nonzero numbers $a_1, \dots, a_{n+1} \in \mathbb{F}$, and evaluate $\mathrm{perm}(B(a_i))$ for all a_i. W.p. $\ge \frac{2}{3}$, we get all the answers correctly. — At this point, we can compute the entire polynomial $B(x)$ since $n+1$ points uniquely determines a deg-n polynomial. Finally $\mathrm{perm}(A) = \mathrm{perm}(B(0))$. $\square$

- Expanders.

  - (Bipartite expander). A bipartite graph $G=(L,R,E)$ is an (n,m,d)-expander if $|L|=n$, $|R|=m$, G is d-left regular, and $\forall S \subseteq L$,

$$|\Gamma(S)| \ge \begin{cases} \frac{5d}{8}|S| & \text{if } |S| \le \frac{n}{10d} \\ |S| & \text{if } \frac{n}{10d} \le |S| \le \frac{n}{2}. \end{cases}$$

<u>Fact</u>. $\forall$ large d, n, $m > \frac{3n}{4}$, $\exists$ (n,m,d)-expander.

<u>Pf</u>. Random d-left regular graphs suffice whp.

$\forall S$ w/ $|S| \le \frac{n}{10d}$, $\forall T$ w/ $|T| < \frac{5d}{8}|S|$, $\Pr[\Gamma(S) \subseteq T] \le \left(\frac{|T|}{m}\right)^{|S|\cdot d} < \frac{1}{10} \cdot \frac{1}{\binom{n}{|S|}} \cdot \frac{1}{\binom{m}{|T|}}$.

$\forall S$ w/ $\frac{n}{10d} \le |S| \le \frac{n}{2}$, $\forall T$ w/ $|T| < |S|$, $\Pr[\Gamma(S) \subseteq T] \le \left(\frac{|T|}{m}\right)^{|S|\cdot d} < \frac{1}{10} \cdot \frac{1}{\binom{n}{|S|}} \cdot \frac{1}{\binom{n}{|S|}}$. $\square$

Ex. Finish the bounds in the two inequalities

∘ Group: A set S, together w/ a binary operation $\cdot : S\times S \to S$ satisfying associativity, existence of identity and inverse.

Eg. $(\mathbb{Z},+)$, $(\mathbb{R}\setminus\{0\},\times)$, $(GL_n(\mathbb{Q}),\times)$, $(S_n,\circ)$, $(\mathbb{Z}_n, + \bmod n)$,

Ring: A set S together w/ two binary operations $+,\cdot : S\times S \to S$, satisfying $(S,+)$ is an Abelian group, $(S,\cdot)$ is a monoid (group except for no inverse requirement) and distributive laws hold.

Eg. $(\mathbb{Z},+,\cdot)$, $(R^{n\times n},+,\cdot)$ for any ring R, $R[x]$ for any ring R, $(\mathbb{Z}/n\mathbb{Z}, +_{\bmod n}, \cdot_{\bmod n})$

RG for any ring R and group G, $\{a_1g_1+\cdots+a_ng_n;\ a_i\in R, g_i\in G\}$.

Field: A ring where $\cdot$ is commutative and multiplicative inverse exists.

Eg. $\mathbb{Q},\mathbb{R},\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}\equiv\mathbb{F}_p$, $\mathbb{F}_p(x)$,

Finite field: $\mathbb{F}_q$, where $q=p^r$ for some prime p.

$+$: $\cong (\mathbb{Z}_p)^{\otimes r}$

$\times$: extend $\mathbb{F}_p$ w/ a formal variable α s.t. $T(\alpha)=0$ for an irreducible polynomial T of degree r in $\mathbb{F}_p(\alpha)$. i.e. $\mathbb{F}_{p^r}\cong\mathbb{F}_p[x]/T(x)$