3 Oct 2025

Algebraic Algorithms for Matching

Recap. Bipartite $G = (L \cup R, E)$

$|L| = |R| = n.$

"Bipartite Adjacency Matrix" A_G

where $(A_G)_{ij} = \begin{cases} 1 & \text{if } (u_i, v_j) \in E \\ \emptyset & \text{otherwise} \end{cases}$

$$\text{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$ ← counts matchings

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)}$$ ← easy to compute

Lovász: substitute random numbers for the 1's.

Let $X_G = \begin{cases} x_{ij} & \text{if } (u_i, v_j) \in E \\ \emptyset & \text{otherwise} \end{cases}$

x_{ij}: independent random numbers drawn from $\{1, 2, \ldots, M\}$.

Algorithm: Sample $\{x_{ij}\} \in [N]$ indep. unif. random

compute $\det(X_G)$.

if $\det(X_G) \neq 0$

output "G has a PM"

else

output "probably, G has no PM."

$$\det(X_G) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (X_G)_{i,\sigma(i)}$$

* If G has no PM then $\det(X_G) = 0$. (Regardless of how x_{ij}'s are chosen.)

When algo outputs "G has a PM" it must be correct.

* If G has a PM it is possible to sample x_{ij}'s that yield $\det(X_G) = 0$.

(E.g. G is complete bipartite and $x_{ij} = 1 \quad \forall i,j$.)

When can we assert $\Pr(\det(X_G) = 0) < \delta$?

Properties of $\det(X_G)$.

As a function of variables $\{x_{ij}\}$ it is:

- a multivariate polynomial
- total degree of each monomial equals n
- degree of every variable is ϕ or 1 in every monomial.

Schwartz-Zippel Lemma (+ DeMillo + Lipton)

If $f(x_1, \ldots, x_m)$ is a polynomial whose monomials have max-degree d in each individual variable, indep'tly and each x_i is sampled uniformly at random from a set S_i with at least N elements and f is not the zero polynomial then

$$\Pr\left(f(\vec{x}) = 0\right) \leq \frac{dm}{N}.$$

Example: $f(x_1, x_2, x_3, x_4) =$

$$x_1^2 x_3 x_4 - 4x_2^3 + 5x_1^3 x_2^2 x_3 x_4$$

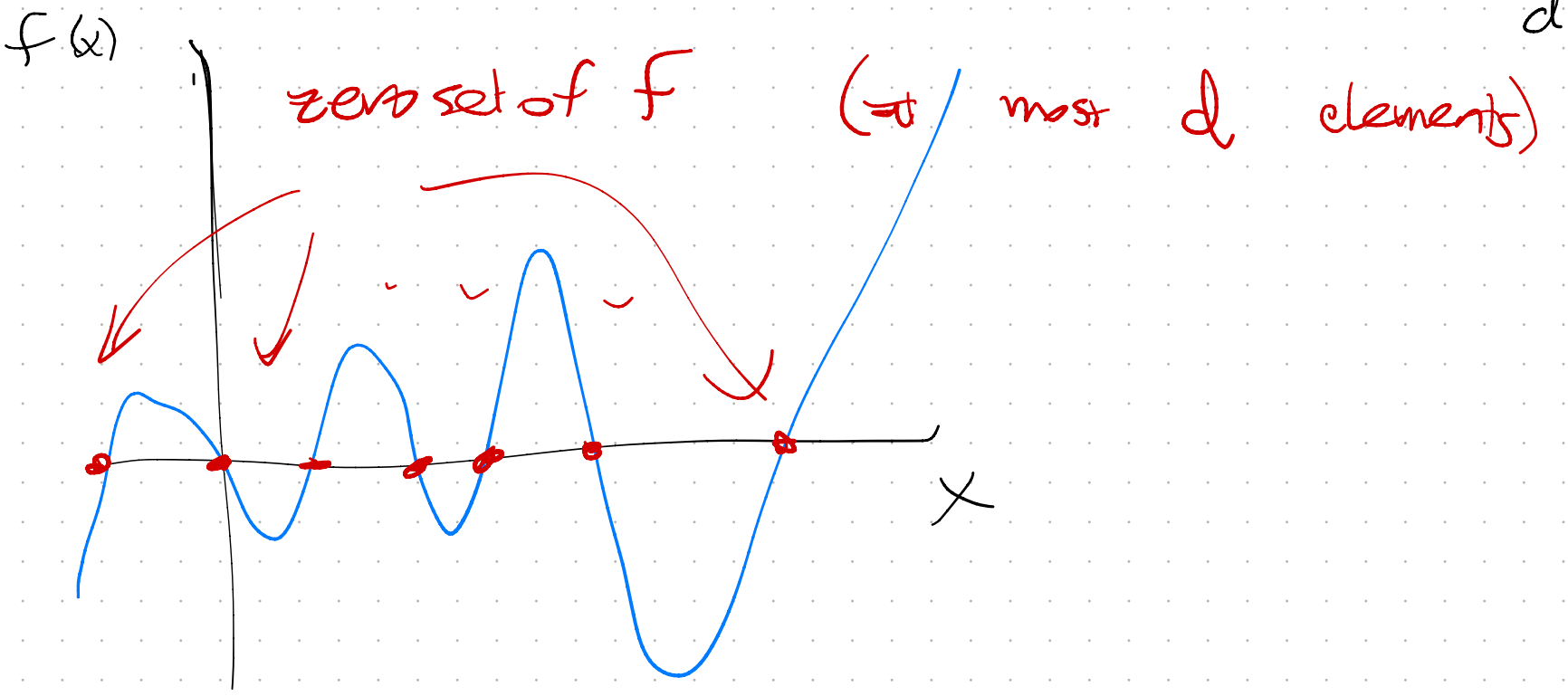
Draw (x_1, x_2, x_3, x_4) at random from

$\{0, 1, \ldots, 99\}^4$.

Then $\Pr(f(x_1, \ldots, x_4) = 0) \leq \frac{3.4}{100} = 0.12$

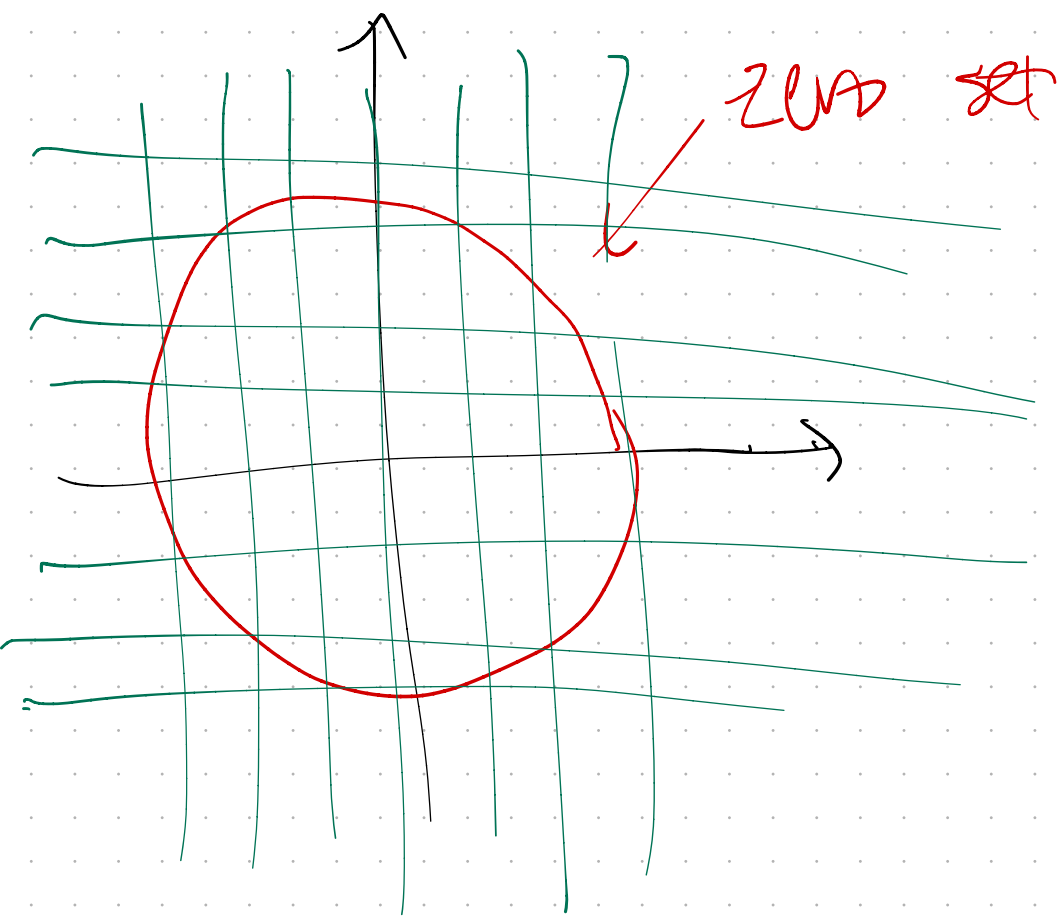
Visualization #1. $m = 1$.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$



Visualization #2. $m = 2$

$$f(x_1, x_2) = x_1^2 + x_2^2 - 25$$



Proof of S-Z. Induct on m, number of variables.

Base case $m=1$ was visualization #1.

Induction step Think of $f(x_1,\dots,x_m)$ as a polynomial in x_m, of degree $\le d$, whose coefficients are functions of $x_1,\dots,x_{m-1}$.

Since $f\not\equiv 0$, at least one of these coeffs is not the zero function.

Say $g(x_1,\dots,x_{m-1})$ is the highest degree coefficient that isn't $\equiv 0$.

When we sample $x_1,\dots,x_{m-1}$ at random

$$\Pr\left(g(x_1,\dots,x_{m-1})=0\right) \le \frac{d(n-1)}{M}. \quad \text{[Ind Hyp]}$$

When $g(x_1,\dots,x_{m-1}) \neq 0$ we know f is a polynomial in x_m of degree $\le d$ with at least one $\neq 0$ coefficient.

$$\Pr\left(g(x_1,\dots,x_{m-1})\neq 0 \text{ but } f(x_1,\dots,x_m)=0\right) \le \frac{d}{M}.$$

Summing,

$$\Pr\left(f(x_1,\dots,x_m)=0\right) \le \frac{d(n-1)}{M} + \frac{d}{M}$$

$$= \frac{dn}{M}.$$

To make this $< \delta$, choose $M > \frac{dn}{\delta}$.

For $\det(X_G)$, $d=1$, $n=|E|$, use

$$M \ge \frac{|E|}{\delta}.$$

To compute $\det(X_G)$ in $\tilde{O}(n^\omega)$ operations, use arithmetic in $\mathbb{F}_p$ where p is a prime between M and $2M$, $M = \frac{1}{\delta}\cdot|E|$.