Matrix Rigidity

Review of Part I

Sasha Golovnev

September 16, 2020

Tools Used in Part I

Last Lecture

Take a random object
Prove $\Pr[\text{GOOD}] > 0$
$\Pr[\text{BAD}] < 1$
$\Longrightarrow$ $\exists$ exists GOOD obj

we proved $\exists$ rigid matrices

- Probabilistic Method
- Algebraic Independence

Alg ind is often as good as randomness (or even better)

Matrix w alg ind entries is rigid.

Polynomial Method

- In order to prove an upper bound on the number N of zero-patterns, we

Polynomial Method

- In order to prove an upper bound on the number N of zero-patterns, we
  - defined a polynomial for each zero pattern N polynomial's

Polynomial Method

- In order to prove an upper bound on the number N of zero-patterns, we
    - defined a polynomial for each zero pattern
    - showed that all N polynomials are linearly independent

Step 1

subspace V generated by N poly, $\dim(V) = N$

Polynomial Method

- In order to prove an upper bound on the number N of zero-patterns, we
  - defined a polynomial for each zero pattern
  - Step 1 showed that all N polynomials are linearly independent
  - Step 2 but they live in a low-dimensional space

dim(V) is low

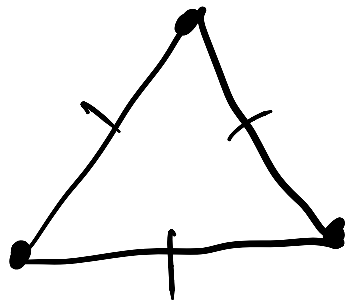
$N = \dim(V)$

is small

Polynomial Method

- In order to prove an upper bound on the number N of zero-patterns, we
  - defined a polynomial for each zero pattern
  - showed that all N polynomials are linearly independent
  - but they live in a low-dimensional space
  - hence, an upper bound on N

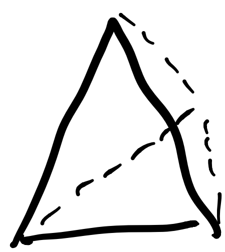
$\mathbb{R}^2$ n points s.t. all pairwise distances are same



$n=3$

$\mathbb{R}^d$ regular simplex in $\mathbb{R}^d$

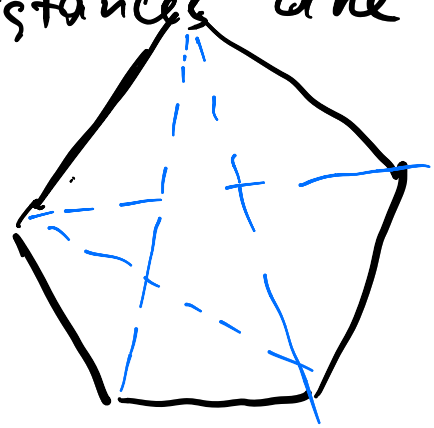
$n = d+1$



---

n points s.t. all pairwise distances are $\{a, b\}$

$\mathbb{R}^2$



$n \geq 5$

$\mathbb{R}^d$ two distances $\{a, b\}$

$n \geq \Omega(d^2)$

$p_1 \ldots p_n \in \{0,1\}^d$

$\|p_i\|_1 = 2$ – has exactly two ones.

$n = \binom{d}{2}$

p_i $\begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline \end{array}$

dist=2

p_j $\begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline \end{array}$

---

p_i $\begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline \end{array}$

dist=$\sqrt{2}$

p_j $\begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ \hline \end{array}$

$\mathbb{R}^d$ two distances (a, b)

Prove an Upper Bound on n

$p_1 \dots p_n \in \mathbb{R}^d$

$f_1 \dots f_n$ - poly $f_i(x)$ $x \in \mathbb{R}^d$

$\quad\quad\quad\quad f_i(x_1, \dots, x_d)$

$$f_i(x) = (\|x - p_i\|_2^2 - a^2) \cdot (\|x - p_i\|_2^2 - b^2)$$

$$f_i(p_i) = a^2 \cdot b^2 \neq 0$$

$$i \neq j: \; f_i(p_j) = (\|p_j - p_i\|_2^2 - a^2)(\|p_j - p_i\|_2^2 - b^2) = 0$$

Poly method ♡

Step 1: prove polys are lin ind

Step 2: dim(span) is small

Step 1: f_i are lin ind.

$$\sum_{i=1}^{n} f_i \cdot \alpha_i = 0 \overset{\text{WTS}}{\Longrightarrow} \text{all } \alpha_i = 0$$

$\forall x$

$$\sum_{i=1}^{n} f_i(x) \cdot \alpha_i = 0$$

$\forall j \in \{1, \ldots, n\}$

$x = p_j$

$$\sum_{i=1}^{n} f_i(p_j) \cdot \alpha_i = 0$$

$f_i(p_j) = 0$ iff $i \neq j$

$$\Downarrow$$

$$f_j(p_j) \cdot \alpha_j = 0$$

$f_j(p_j) \neq 0$

$$\Downarrow$$

$$\alpha_j = 0 \leftarrow \forall j \in \{1, \ldots, n\}$$

V – subspace real funs $\mathbb{R}^d \to \mathbb{R}$ spanned $f_1 \ldots f_n$

$$\dim(V) = n$$

It remains to show $\dim(V)$ is small

$$F_i(x_1, \dots, x_d) = (\|x - p_i\|^2 - a^2) \cdot (\|x - p_i\|^2 - b^2)$$

$$= \left(\sum_{j=1}^{d} (x_j - p_{ij})^2 - a^2 \right) \left(\sum_{j=1}^{d} (x_j - p_{ij})^2 - b^2 \right)$$

— poly of deg 4 in $x_1, \dots, x_d$.

	basis
1	1
$x_1, \dots, x_d$	d
$x_1^2, x_1 x_2, x_1 x_3, \dots, x_d^2$	d^2
$x_1^3, x_1^2 x_2, \dots \dots x_d^3$	d^3
$x_1 x_2 x_3 x_4, x_1^4 \dots \dots$	d^4

$n = \dim(V) \leq$ size of the basis $= O(d^4)$

In our case

basis	# of polys
1	1
$x_1, \dots, x_d$	d
$x_1^2, \dots, x_d^2$	d^2
$x_j \sum_{i=1}^{d} x_i^2 \quad \forall j \in [d]$	d
$\left(\sum x_i^2\right)^2$	1

$= O(d^2)$

$\Downarrow$

$n \leq O(d^2)$

Polynomial Method. Example

Theorem

Let $x_1, \ldots, x_n \in \mathbb{R}^d$ be points such that the pairwise distances between them take two values. Then

$$n = O(d^2)\,.$$

Zarankiewicz Problem

- In order to bound the number of edges in a graph it often suffices to exclude some local configurations

Zarankiewicz Problem

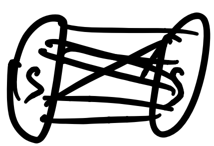
- In order to bound the number of edges in a graph it often suffices to exclude some local configurations
- We showed that a graph without bipartite cliques is not dense

Zarankiewicz Problem

- In order to bound the number of edges in a graph it often suffices to exclude some local configurations
- We showed that a graph without bipartite cliques is not dense

Theorem [KST]

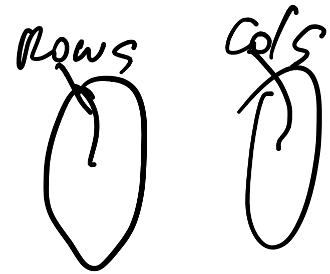
Let $s \in \mathbb{N}$ be a constant. The number of edges in a $K_{s,s}$-free graph is $\underbrace{O(n^{2-1/s})}$.



vs $\Theta(n^2)$ in complete graph

Zarankiewicz Problem

- Concluded that a few changes in a matrix leave an untouched matrix of size $s \times s$



Zarankiewicz Problem

- Concluded that a few changes in a matrix leave an untouched matrix of size $s \times s$
- Thus, matrices with non-zero minors are (moderately) rigid

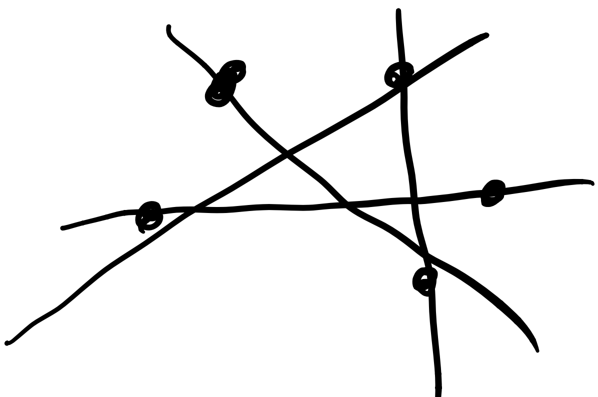
Zarankiewicz Problem. Example

Theorem (Szemerédi–Trotter theorem)

n points and n lines in the plane have $O(n^{4/3})$ point-line incidences.

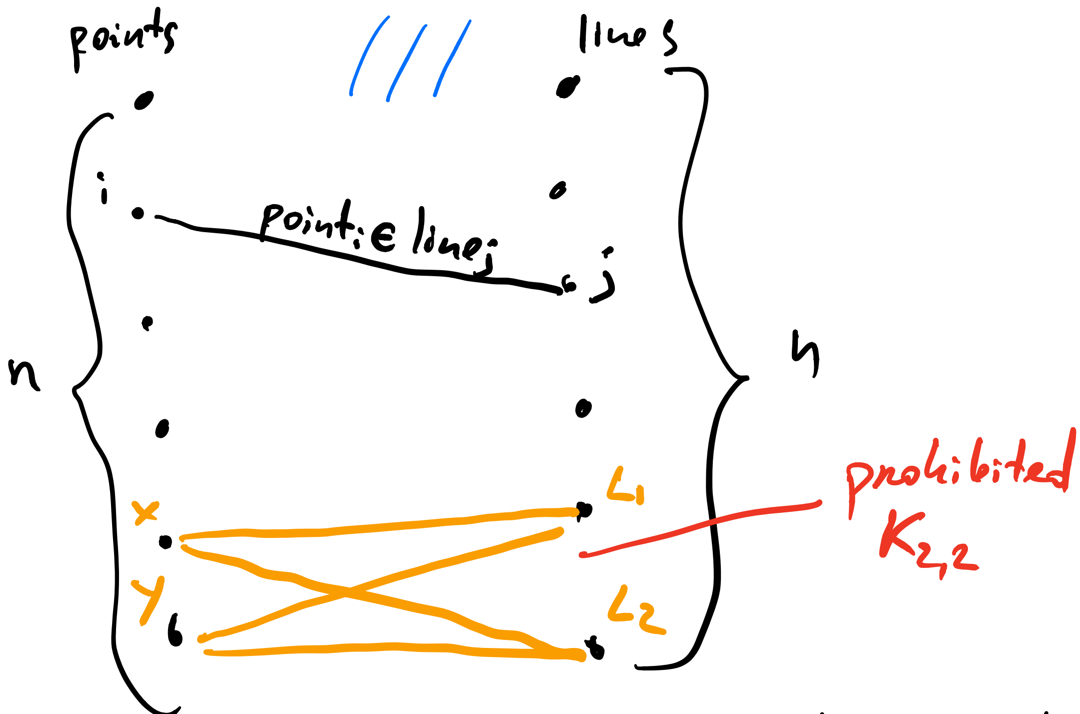
(point, line) s.t. point $\in$ line

$\mathbb{R}^2$



point-line incidences $\leq n^2$

(point-line)-incidences $\leq O(n^{3/2})$



Upper bound on # edges in the graph

Zarankiewicz: no $K_{s,s}$

$\Rightarrow$ # edges $O(n^{2-1/s})$

<u>Cor</u>: no $K_{2,2}$ $\Rightarrow$ # edges $O(n^{3/2})$

Hölder's Inequality

Theorem

For any $x, y \in \mathbb{C}^n$*, any* $p, q \in [1, \infty]$ *with* $1/p + 1/q = 1$:

$$\sum_{i=1}^{n} |x_i y_i| \leq \|x\|_p \|\cancel{x}\, y\|_q .$$

Hölder's Inequality

Theorem

For any x, y $\in \mathbb{C}^n$*, any* $p, q \in [1, \infty]$ *with* $1/p + 1/q = 1$:

$$\sum_{i=1}^{n} |x_i y_i| \leq \|x\|_p \|y\|_q .$$

- Connects different L_p norms

Hölder's Inequality

Theorem

For any x, y $\in \mathbb{C}^n$, *any* $p, q \in [1, \infty]$ *with* $1/p + 1/q = 1$:

$$\sum_{i=1}^{n} |x_i y_i| \leq \|x\|_p \|y\|_q .$$

$\sum d_i^s \leq$ Bound

$|E| = \sum d_i \leq$ Bound'

- Connects different L_p norms
- In Kővári-Sós-Turán Theorem, we had a bound on sth moment of vertices' degrees, needed bound on number of edges

Hölder's Inequality. Example

Theorem

For $v \in \mathbb{C}^n$:

$$\frac{\|v\|_1}{\sqrt{n}} \leq \|v\|_2 \leq \sqrt{\|v\|_1 \|v\|_\infty}\,.$$

Theorem

For $v \in \mathbb{C}^n$*:*

$$\frac{\|v\|_1}{\sqrt{n}} \leq \|v\|_2 \leq \sqrt{\|v\|_1 \|v\|_\infty}\,.$$

Theorem

For any $x, y \in \mathbb{C}^n$*, any* $p, q \in [1, \infty]$ *with* $1/p + 1/q = 1$*:*

$$\sum_{i=1}^{n} |x_i y_i| \leq \|x\|_p \|y\|_q\,.$$

WTS:

$\|v\|_1 \leq \sqrt{n} \cdot \|v\|_2$

$x_i := v_i \quad y_i := 1 \quad p = q = 2 \quad \frac{1}{p} + \frac{1}{q} = 1$

$\|v\|_1 = \sum_{i=1}^{n} |v_i| = \sum |x_i y_i|$

Hölder

$\leq \|x\|_p \cdot \|y\|_q = \|v\|_2 \cdot \sqrt{n}$

$\|v_2\| \leq \sqrt{\|v\|_1 \cdot \|v\|_\infty}$

$p = 1 \quad q = \infty \quad \frac{1}{p} + \frac{1}{q} = 1$

$x_i = y_i = v_i$

$\|v\|_2^2 = \sum v_i^2 = \sum |x_i y_i|$

Hölder

$\leq \|x\|_p \cdot \|y\|_q = \|v\|_1 \cdot \|v\|_\infty$

Hölder's Inequality. Example

Theorem

For $v \in \mathbb{C}^n$:

$$\frac{\|v\|_1}{\sqrt{n}} \leq \|v\|_2 \leq \sqrt{\|v\|_1 \|v\|_\infty}\,.$$

Theorem

For $v \in \mathbb{C}^n$:

This is tight

$$\|v\|_r \leq n^{1/r-1/s} \|v\|_s\,.$$

R=1

S=1

$\sqrt{n}$

Sign-rank

Let $A \in \{1, -1\}^{n \times n}$. Then **signrk**$(A)$ is the minimum rank of B s.t. $sign(b_{ij}) = a_{ij}$ for all $i, i \in [n]$.

Unbounded-error communication complexity

$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$f(x, y)$

Alice gets x
Bob gets y $\to f(x,y)$

---

det
non-det
rand
quant w/o ent
quant w/ ent

comm models

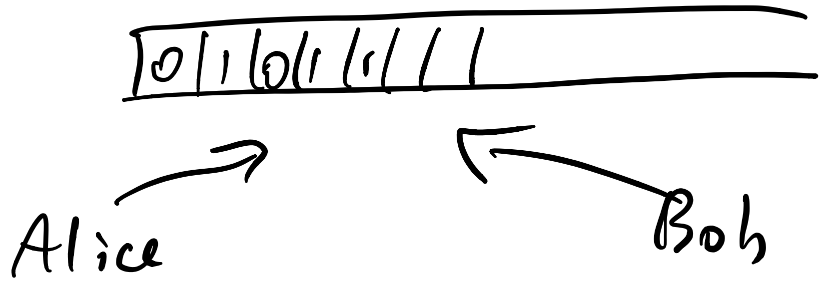
Unbounded-error comm.

compute $f(x,y)$ with prob $> \frac{1}{2}$

say, $\frac{1}{2} + \frac{1}{2^n}$

Alice & Bob use private randomness

If we had shared randomness



Then $CC(\text{every problem}) \le 1$

Alice:

sends 1 iff first n bits of randomness $= x$

sends 0.

Bob:

receives 1. Knows $x \Rightarrow f(x,y)$

else . Random bit.

Prob of success:

$$2^{-n} + (1-2^{-n}) \cdot \frac{1}{2} = \frac{1}{2} + \frac{1}{2^{n+1}} > \frac{1}{2}$$

Important: Randomness is Private

Sign-rank

Let $A \in \{1,-1\}^{n\times n}$. Then $\mathrm{signrk}(A)$ is the minimum rank of B s.t. $sign(b_{ij}) = a_{ij}$ for all $i, i \in [n]$.

Theorem (Paturi, Simon)

Unbounded-error communication complexity of a problem is $\log(\mathrm{signrk}(A))$ *of its communication matrix A.*

$\operatorname{signrk}(A)$ $\qquad A \in \{\pm 1\}^{n \times n}$

$B \in \mathbb{R}^{n \times n}$ $\qquad \operatorname{sign}(b_{ij}) = a_{ij}$

$\min \operatorname{rk} B \leftarrow \operatorname{signrk}(A)$

$B_0 = A$

$$A \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \qquad B_1 \begin{bmatrix} 7 & 0.5 \\ -3 & -1 \end{bmatrix}$$

$$B_2 \begin{bmatrix} 0.1 & 11 \\ -1 & -1 \end{bmatrix}$$

Sometimes $\operatorname{signrk}(A) < \operatorname{rk}(A)$

Ex.

$$A \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$\operatorname{rk}(A) \geq n-1$

$\operatorname{rk}(A+J) =$

$= \operatorname{rk}(2 \cdot T_R)$

$= n$

$$B \begin{bmatrix} 1 & -1 & -3 & -5 \\ 3 & 1 & -1 & -3 \\ 5 & 3 & 1 & -1 \\ 7 & 5 & 3 & 1 \end{bmatrix}$$

$1 \quad -1 \quad -3 \quad -5$

$2 \quad 2 \quad 2 \quad 2$

$\operatorname{rk}(B) = 2$

$\mathrm{Rk}(A) = n-1$

$\mathrm{signrk}(A) = 2$

$\mathrm{signrk}(A) <<<< \mathrm{rk}(A)$

Unbounded error Comm Comp

$= \log_2(\mathrm{signrk}(A)) \pm 1$

Zero-patterns

- A vector $\sigma \in \{0,1\}^n$ is a zero-pattern of polynomials $p_1, \ldots, p_n$ if there exists $x \in \mathbb{R}^t$ s.t. $p_i(x) = 0$ iff $\sigma_i = 0$

n polys of t variables

Zero-patterns

- A vector $\sigma \in \{0,1\}^n$ is a zero-pattern of polynomials $p_1, \ldots, p_n$ if there exists $x \in \mathbb{R}^t$ s.t. $p_i(x) = 0$ iff $\sigma_i = 0$
- The number of zero-patterns is $\leq 2^n$

Zero-patterns

- A vector $\sigma \in \{0,1\}^n$ is a zero-pattern of polynomials $p_1, \ldots, p_n$ if there exists $x \in \mathbb{R}^t$ s.t. $p_i(x) = 0$ iff $\sigma_i = 0$
- The number of zero-patterns is $\leq \underline{\underline{2^n}}$

Theorem

For constant degree polynomials, the number of zero-patterns is $\leq \boxed{n^t} \ll \underline{\underline{2^n}}$ *(for small t)*

n – # polys
t – # var

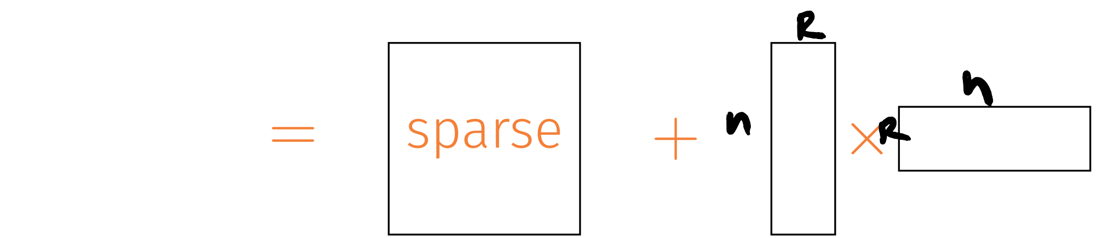
Zero-patterns

- Non-rigid M:

$$\boxed{} = \boxed{\text{sparse}} + \boxed{\text{low-rank}}$$

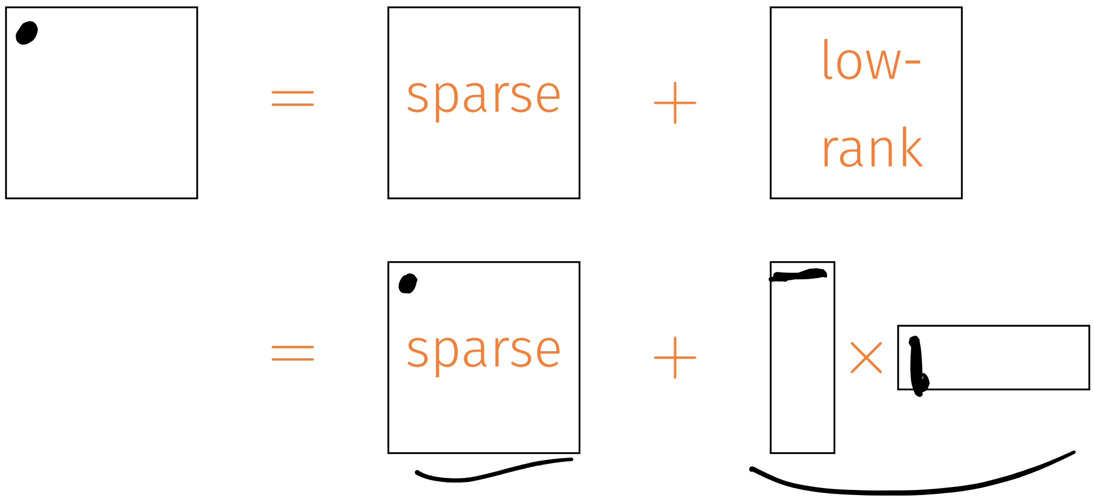
Zero-patterns

- Non-rigid M:



Zero-patterns

- Non-rigid M:



- Each (out of n^2) entries on the left is a degree-2 polynomial of the entries on the right

Zero-patterns

- By the zero-pattern theorem, there are only a few zero-non-zero matrices low-degree polynomials can generate

Zero-patterns

- By the zero-pattern theorem, there are only a few zero-non-zero matrices low-degree polynomials can generate
- In particular, only a few $\{0, 1\}$-matrices

Zero-patterns

- By the zero-pattern theorem, there are only a few zero-non-zero matrices low-degree polynomials can generate
- In particular, only a few $\{0,1\}$-matrices
- Therefore, a random $\{0,1\}$-matrix is rigid

Brute force 2^{n^2}

Sign-patterns. Example

Theorem

The number of sign-patterns of n constant-degree polynomials of t variables is (also) $\leq n^t$.

Sign-patterns. Example

Theorem

The number of sign-patterns of n constant-degree polynomials of t variables is (also) $\leq n^t$.

Theorem [Alon et al 1985]

There exist matrices of high sign-rank. (There exist problems of high unbounded-error communication complexity.)