Matrix Rigidity

Lower bounds of Pudlák and Rödl; Shokrollahi, Spielman and Stemann

Sasha Golovnev

September 9, 2020

Recap

- Non-explicit rigid matrices

Recap

- Non-explicit rigid matrices
    - n^2 algebraically independent entries

Recap

- Non-explicit rigid matrices
    - n^2 algebraically independent entries
    - n^2 random bits

Recap

- Non-explicit rigid matrices
    - n^2 algebraically independent entries
    - n^2 random bits
- Explicit lower bounds

Recap

- Non-explicit rigid matrices
  - n^2 algebraically independent entries
  - n^2 random bits
- Explicit lower bounds

$$\mathcal{R}^{\mathbb{F}}_{M_n}(r) = \Omega\left(\frac{n^2}{r} \cdot \log \frac{n}{r}\right) .$$

Explicit Constructions

Explicit Lower Bound

Theorem

Let F be a fixed finite field, and $G \in \mathbb{F}^{n \times k}$ be a generator matrix of a good linear code, then for every $\Omega(\log n) < r < O(n)$,

$$\mathcal{R}_G^{\mathbb{F}}(r) \geq \Omega\left(\frac{n^2}{r} \cdot \log \frac{n}{r}\right) .$$

Linear Codes

- A linear code C is a subspace of $\mathbb{F}^n$.

Linear Codes

- A linear code C is a subspace of $\mathbb{F}^n$.
- Distance

$$d(C) = \min \left(\|w\|_0 : w \in C, w \neq \mathbf{0} \right) .$$

Linear Codes

- A linear code C is a subspace of $\mathbb{F}^n$.
- Distance

$$d(C) = \min\left(\|w\|_1 : w \in C, w \neq \mathbf{0}\right) .$$

- Given be a generator matrix $G \in \mathbb{F}^{n \times k}$ whose columns form a basis of C.

$w \in C$

$\Updownarrow$

$w = G \cdot x \quad x \in \mathbb{F}^k$

Linear Codes

- A linear code C is a subspace of $\mathbb{F}^n$.
- Distance

$$d(C) = \min\left(\|w\|_0 : w \in C, w \neq \mathbf{0}\right) .$$

- Given be a generator matrix $G \in \mathbb{F}^{n \times k}$ whose columns form a basis of C.
- Explicit constructions: $d, k = \Theta(n)$. $\forall \mathbb{F}$

Good codes

Lower Bound of Pudlák and Rödl

Theorem

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of size q. Let $G \in \mathbb{F}^{n \times k}$ be a generator matrix of a code of dimension k and distance δn for a constant $0 < \delta < 1$. Then for any $1 \le r \le \frac{k}{q^2}$,

$$\mathcal{R}_G^{\mathbb{F}}(r) \ge \frac{\delta k n \log_q \frac{k}{r}}{8r} =$$

$q = \Theta(1)$

$k = \Theta(n)$

$\delta n = \Theta(n)$

$\delta = \Theta(1)$

$= \Theta\left(\frac{n^2}{R} \log \frac{n}{R}\right)$

Theorem

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of size q. Let $G \in \mathbb{F}^{n\times k}$ be a generator matrix of a code of dimension k and distance δn for a constant $0 < \delta < 1$. Then for any $1 \le r \le \frac{k}{q^2}$,

$$\mathcal{R}_G^{\mathbb{F}}(r) \ge \frac{\delta k n \log_q \frac{k}{r}}{8r}.$$

$G = L + S$

$\mathrm{Rank}(L) \le R$

$\|S\|_0 \le \frac{\delta k n}{4\ell}$ parameter to be chosen

By Markov (see prev class):

$\exists$ $k/2$ sparsest cols of S,

each of them $\le \|S\|_0 / (k/2) = \frac{\delta n}{2\ell}$ non-zeros

$G', L', S' \in \mathbb{F}^{n\times k/2}$ — G, L, S restricted to the $k/2$ cols.

$\mathrm{Rank}(L') \le \mathrm{Rank}(L) \le R$

<u>Idea:</u>

Lin comb of cols G' = codeword

codewords $\|\ \|_0$ is large.

$G = L + S \Rightarrow G' = L' + S'$

$L' = G' - S'$

1. We'll show

Short lin comb of L'

$\approx$ lin comb of cols G'

= codeword $\Rightarrow \| \ \|_0$ is high

2. We'll

many lin comb $\| \cdot \|_0$ is

high $\Rightarrow$ Rank(L') large

contradiction

$L' = G' - S'$

$d(G') \geq \delta n$

every col of $S' \leq \frac{\delta n}{2\ell}$ non-zeros

$x \in \mathbb{F}^{k/2} \setminus \{0^{k/2}\}$

$\|x\|_0 \leq \ell$

$$\|L'x\|_0 = \|(G'-S')x\|_0 = \|G'x - S'x\|_0 \geq \|G'x\|_0 - \|S'x\|_0$$

$$\geq \left[\begin{array}{l} G'x \text{ - codeword} \Rightarrow \|G'x\|_0 \geq \delta n \\ \|S'x\|_0 \leq \|x\|_0 \cdot \text{col sparse of } S' \\ \quad \|x\|_0\text{-sparse lin comb of cols of } S' \\ \quad \leq \ell \cdot \frac{\delta n}{2\ell} = \frac{\delta n}{2} \end{array} \right]$$

$$\geq \frac{\delta n}{2} > 0.$$

$\forall x \neq 0, \|x\|_0 \leq \ell, L'x \neq 0$

$\Updownarrow$

$\forall y_1, y_2 \in \mathbb{F}^{k/2}, y_1 \neq y_2, \|y_1\|_0, \|y_2\|_0 \leq \frac{\ell}{2}$

$$L'y_1 \neq L'y_2$$

$$L'y_1 = L'y_2 \iff L' \cdot \underbrace{(y_1 - y_2)}_{\frac{\ell}{2} + \frac{\ell}{2} = \ell} = 0$$

column space of L'

$|\text{col space of } L'| \geq \binom{k/2}{\ell/2} \cdot (|\mathbb{F}| - 1)^{\ell/2}$

$$\geq \binom{k/2}{\ell/2} \geq \left(\frac{k/2}{\ell/2}\right)^{\ell/2} = \left(\frac{k}{\ell}\right)^{\ell/2}$$

$$\binom{n}{k} \geq \left(\frac{n}{k}\right)^k$$

$\mathrm{Rk}(L') = \dim(\text{col sp } L') \geq$

$$\log_q \left(\frac{k}{\ell}\right)^{\ell/2} = \frac{\ell}{2} \log_q \left(\frac{k}{\ell}\right)$$

$$(k) \approx \left(\frac{\cdot}{k}\right)$$

$$\mathrm{Rk}(L') = \dim(\mathrm{col\ sp}\ L') \geq \log_q \left(\frac{k}{\ell}\right)^{\ell/2} = \frac{\ell}{2}\log_q\left(\frac{k}{\ell}\right)$$

$$\ell \approx \frac{2R}{\log_q \frac{k}{R}}$$

$$\mathrm{Rk}(L') \geq \frac{\ell}{2}\log_q\left(\frac{k}{\ell}\right) > R \qquad \square$$

$$C' = \boxed{L'} + S'$$

Lower Bound of Shokrollahi, Spielman and Stemann

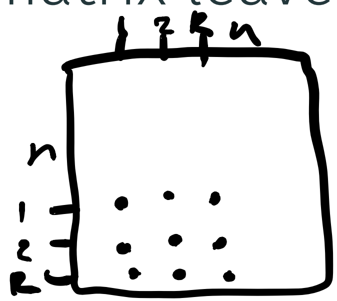
- Untouched minor.

Lower Bound of Shokrollahi, Spielman and Stemann

- Untouched minor.

$\log\left(\frac{n}{R}\right)$

- Step 1: $O(n^2/r)$ changes in $n \times n$ matrix leave an $r \times r$ submatrix untouched.

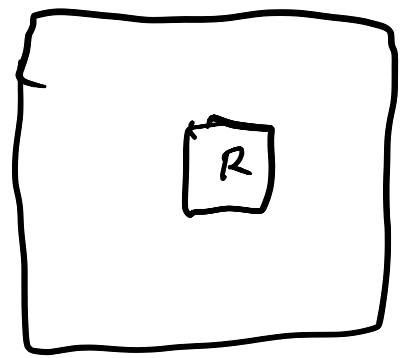


Lower Bound of Shokrollahi, Spielman and Stemann

- Untouched minor.

- Step 1: $O(n^2/r)$ $\log(\frac{n}{r})$ changes in $n \times n$ matrix leave an $r \times r$ submatrix untouched.

- Step 2: Take a matrix where each $r \times r$ submatrix is full-rank.



Lower Bound of Shokrollahi, Spielman and Stemann

- Untouched minor.

  $\log(\frac{n}{r})$
- Step 1: $O(n^2/r)$ changes in $n \times n$ matrix leave an $r \times r$ submatrix untouched.
- Step 2: Take a matrix where each $r \times r$ submatrix is full-rank.

  $\log(\frac{n}{r})$
- After $O(n^2/r)$ changes, the rank is $\geq r$.

Kővári-Sós-Turán Theorem

Theorem

Let $n, s \in \mathbb{N}$ such that $s \leq n$ and G be an $n \times n$ bipartite graph. If G has no $s \times s$ bi-clique, then the number of edges in G is at most

$$(s-1)^{1/s}(n-s+1)n^{1-1/s} + (s-1)n.$$

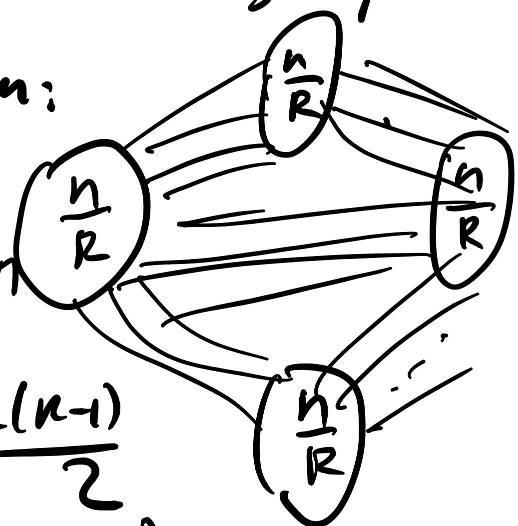
Turán's thm

no $(R+1)$-cliques

K_{R+1}-free graphs

max # edges in such graph?

Turán's thm:



no edges inside

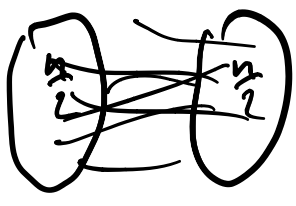
R parts

$$\frac{n^2}{R^2}\cdot\frac{R(R-1)}{2} = \frac{n^2}{2}\cdot\left(1-\frac{1}{R}\right)$$

compare $\simeq \frac{n^2}{2}$

complete graph

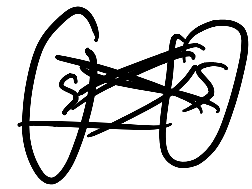
$R=2$ Δ-free



$\sim \frac{n^2}{4}$

Zarankiewicz problem:

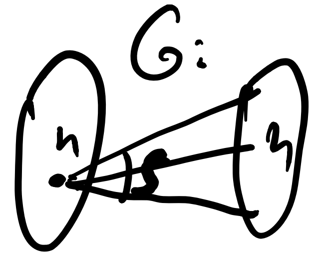
max # edges in $n \times n$ bipartite gr without $K_{s,s}$



Theorem

Let $n, s \in \mathbb{N}$ such that $s \leq n$ and G be an $n \times n$ bipartite graph. If G has no $s \times s$ bi-clique, then the number of edges in G is at most

$$(s-1)^{1/s}(n-s+1)n^{1-1/s} + (s-1)n.$$

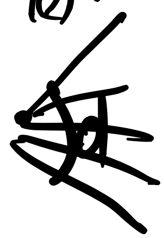


left s-stars

$d_1, \dots, d_n$ – degrees of vert on left

$$|E| = \sum_{i=1}^{n} d_i$$

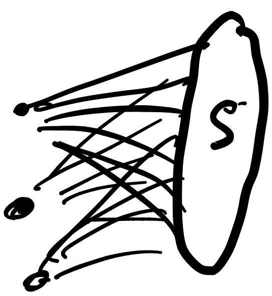
$$\#\text{ left } s\text{-stars} = \sum_{i=1}^{n} \binom{d_i}{s}$$



$$\#\text{ left } s\text{-stars} \leq (s-1) \cdot \binom{n}{s}$$

Right

$$\sum \binom{d_i}{s} \leq (s-1) \cdot \binom{n}{s}$$



$$\sum \frac{d_i!}{\cancel{s!}(d_i-s)!} \leq (s-1) \cdot \frac{n!}{\cancel{s!}(n-s)!}$$

$$\sum \underbrace{d_i(d_i-1)\dots(d_i-s+1)}_{s} \leq (s-1) \cdot \underbrace{n(n-1)\dots(n-s+1)}_{s}$$

$\Downarrow$ convexity

$$\sum (d_i-s+1)^s \leq (s-1) \cdot (n-s+1)^s$$

Hölder's inequality, $p,q>1$

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

$$\sum_{i=1}^{n}|x_i y_i| \leq \left(\sum |x_i|^p\right)^{1/p} \cdot \left(\sum |y_i|^q\right)^{1/q}$$

$p=q=2$: CS :

$$\left(\sum x_i y_i\right)^2 \leq \sum x_i^2 \cdot \sum y_i^2$$

$x_i = d_i - s + 1 \qquad y_i = 1; \quad p = s, \quad \frac{1}{q} = 1 - \frac{1}{s}$

$$\sum d_i - s + 1 = \sum x_i y_i \leq$$

$$\leq \left(\sum |x_i|^s\right)^{1/s} \cdot \left(\underbrace{\sum |1|^q}_{n}\right)^{1/q}$$

$$\leq \left(\sum (d_i - s + 1)^s\right)^{1/s} \cdot n^{1-\frac{1}{s}}$$

$$\leq \left((s-1)^s (n-s+1)\right)^{1/s} \cdot n^{1-\frac{1}{s}}$$

$$\sum d_i - s + 1 = \sum x_i y_i \leq$$

$$\leq \left(\sum |x_i|^s\right)^{1/s} \cdot \Big(\underbrace{\sum |1|^q}_{n}\Big)^{1/q}$$

$$\leq \left(\sum (d_i - s + 1)^s\right)^{1/s} \cdot n^{1-\frac{1}{s}}$$

$$\leq \left((s-1)^{1/s}(n - s + 1)\right) \cdot n^{1-\frac{1}{s}}$$

$$E = \sum_{i=1}^{n} d_i = \sum_{i=1}^{n} (d_i - s + 1) + (s-1) \cdot n$$

$$\leq (s-1)^{1/s} (n - s + 1)\, n^{1-\frac{1}{s}} + (s-1) \cdot n$$

$\square$

Untouched Minor

Lemma

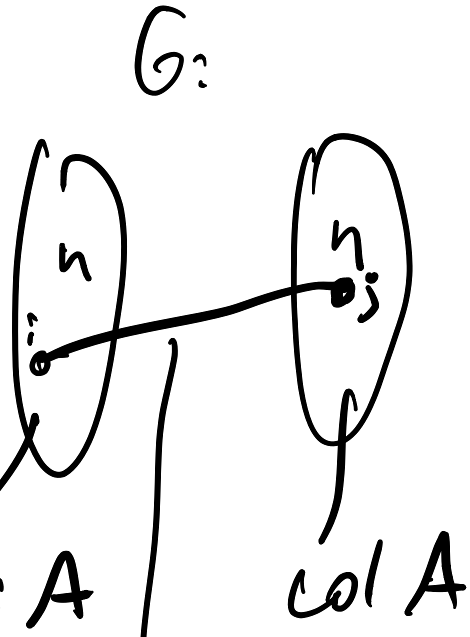
Let $n, r \in \mathbb{N}$ such that $\log n \leq r \leq n$, and A be an $n \times n$ matrix. If fewer than $\frac{n(n-r)}{2(r+1)} \log \frac{n}{r}$ entries of A are changed, then some $(r+1) \times (r+1)$ submatrix of A remains untouched.

$R = O(n)$

$= \Theta\left(\frac{n^2}{R} \log \frac{n}{R}\right)$

Lemma

Let $n, r \in \mathbb{N}$ such that $\log n \le r \le n$, and A be an $n \times n$ matrix. If fewer than $\frac{n(n-r)}{2(r+1)} \log \frac{n}{r}$ entries of A are changed, then some $(r+1) \times (r+1)$ submatrix of A remains untouched.



$(R+1)\times(R+1)$ - unchanged submatrix $\Longleftrightarrow K_{(R+1)\times(R+1)}$

iff A_{ij} is not changed

No unchanged $(R+1)\times(R+1)$ submatrix

$\Rightarrow G$ is $K_{(R+1)\times(R+1)}$-free

$\Rightarrow$ [KST54]

$\#\text{edges} \le n^2 - \frac{n(n-R)\log\frac{n}{R}}{2(R+1)}$

$\Rightarrow$ changes $\geq$

$\square$

Corollary

Corollary

If every $(r+1) \times (r+1)$ submatrix of A is full-rank, then $\mathcal{R}_A(r) \geq \frac{n^2}{4(r+1)} \log \frac{n}{r}$ for $\log n \leq r \leq \frac{n}{2}$.

Previous explicit bounds over finite fields.

Cauchy Matrices

Theorem $(|\mathbb{F}| \geq 2n)$

Let $\mathbb{F}$ be a field containing at least $2n$ distinct elements denoted by $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$. Let $A \in \mathbb{F}^{n \times n}$ be a Cauchy matrix: $A_{ij} = \frac{1}{(x_i - y_j)}$. Then

$$\mathcal{R}_A^{\mathbb{F}}(r) \geq \frac{n^2}{4(r+1)} \log \frac{n}{r}$$

for $\log n \leq r \leq \frac{n}{2}$.

$(r+1) \times (r+1)$ - -submatrix is a Cauchy Matrix

Cauchy Matrices. Proof

- Very simple explicit construction!

Cauchy Matrices. Proof

- Very simple explicit construction!
- Over large enough fields fields.

Cauchy Matrices. Proof

- Very simple explicit construction!
- Over large enough fields fields.
- It suffices to show that every $(r+1) \times (r+1)$ submatrix has full rank.

Cauchy Matrices. Proof

- Very simple explicit construction!
- Over large enough fields fields.
- It suffices to show that every $(r+1) \times (r+1)$ submatrix has full rank.
- Every $(r+1) \times (r+1)$ is a Cauchy matrix too!

Cauchy Matrices. Proof

- Very simple explicit construction!
- Over large enough fields fields.
- It suffices to show that every $(r+1) \times (r+1)$ submatrix has full rank.
- Every $(r+1) \times (r+1)$ is a Cauchy matrix too!
- Homework 1, Problem 3.

Problem 3 (Cauchy determinant)**.** Let $\mathbb{F}$ be a field containing at least $2n$ distinct elements denoted by $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$. Let $A \in \mathbb{F}^{n\times n}$ be a Cauchy matrix: $A_{ij} = \frac{1}{(x_i - y_j)}$. Prove that

$$\det(A) = \frac{\prod_{1\le i<j\le n}(x_j - x_i)(y_i - y_j)}{\prod_{1\le i,j\le n}(x_i - y_j)}.$$

Conclude that $\det(A) \neq 0$.

SSS Bound

Theorem

Let $\mathbb{F}$ be a field, $n \in \mathbb{N}$, $\varepsilon \in (0,1)$, and $\boxed{C \subseteq \mathbb{F}^{2n}}$ be an explicit linear code of dimension n with minimum distance $(1-\varepsilon)n$. Then, there exists a matrix $A \in \mathbb{F}^{n \times n}$ that can be efficiently constructed from any generator matrix of C such that

$$\mathcal{R}_A^{\mathbb{F}}(r) \geq \frac{n^2}{8(r+1)} \log \frac{n}{(2r+1)} \simeq \Theta\left(\frac{n^2}{r} \log \frac{n}{r}\right)$$

for any $\varepsilon n \leq r \leq \frac{n-2}{2}$.

$G \in F^{2n \times n}$ Gaus elim

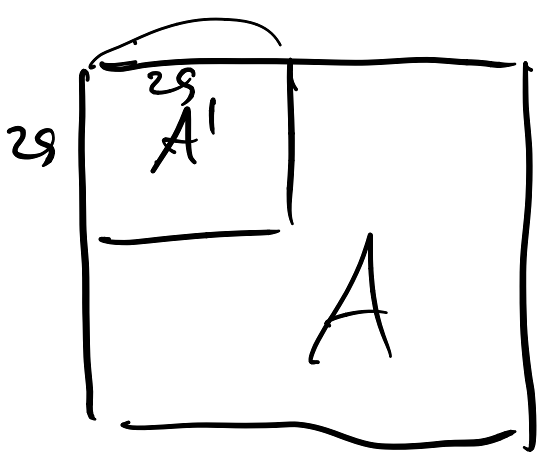
$$G' = \begin{bmatrix} I_n \\ A \end{bmatrix}$$

$A \in F^{n \times n}$

generator matrix of the same code

We'll prove A is rigid

2R × 2R submatrix of has rank $\geq R$. $\Rightarrow$ A is rigid

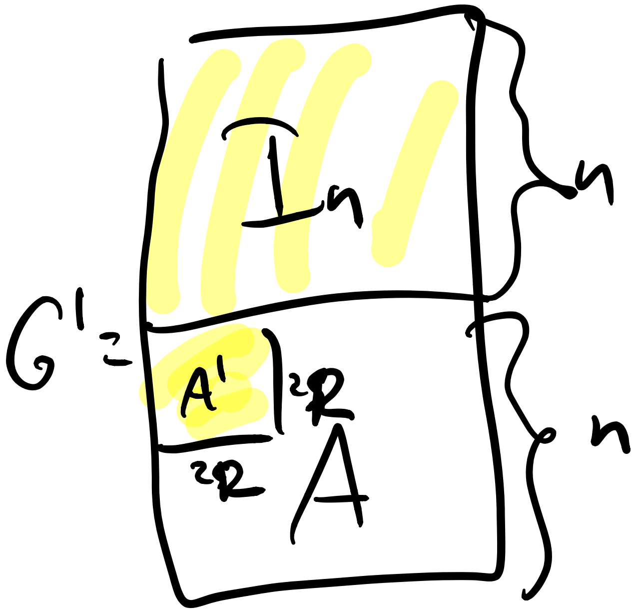


Assume A'-subm A has rank <

$A' \in F^{2R \times 2R}$

$\text{Rank}(A') < R$

$\Rightarrow$ lin comb of R cols of A' $= 0$



lin comb of $\leq R$ cols $A' = 0^{2R}$

same lin comb of s cols $G' \Rightarrow x \in \mathbb{F}^{2n}$

in top part $\leq R$ non-zeros

in bottom part $\geq 2R$ zeros

$$\|x\|_0 \leq R + (n - 2R) = n - R$$

$$\leq n - \varepsilon n = n(1-\varepsilon) =$$

$=$ distance of the code

codeword of weight $<$ distance of code $\square$

Explicit Codes

Proposition

There are explicit constructions of algebraic-geometric codes of dimension n in $\mathbb{F}_q^{2n}$ with minimum distance $\underline{\underline{(1-\varepsilon)n}}$ for $\varepsilon = \frac{2}{\sqrt{q}-1}$ for every prime square q.

For our constr $\varepsilon n \le R \le \frac{n}{2}$

$\varepsilon < \frac{1}{2}$ $\quad q \geq 49$