Matrix Rigidity

Limitations of Combinatorial Methods

Sasha Golovnev

October 28, 2020

Lower Bound of Shokrollahi, Spielman and Stemann

- Untouched minor.

Lower Bound of Shokrollahi, Spielman and Stemann

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

Lower Bound of Shokrollahi, Spielman and Stemann

- Untouched minor.
- Step 1: $O\boxed{\left(\frac{n^2}{r} \cdot \log \frac{n}{r}\right)}$ changes in $n \times n$ matrix leave an $r \times r$ submatrix untouched.
- Step 2: Take a matrix where each $\underline{r \times r}$ submatrix is full-rank. ✓

$$\Rightarrow \quad R_n(r) \geq \Omega\left(\underline{\frac{n^2}{r} \log\left(\frac{n}{r}\right)}\right)$$

Lower Bound of Shokrollahi, Spielman and Stemann

- Untouched minor.
- Step 1: $O(\frac{n^2}{r} \cdot \log \frac{n}{r})$ 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.
- After $O(\frac{n^2}{r} \cdot \log \frac{n}{r})$ changes, the rank is $\geq r$.

Limitations of Untouched Minor

- This method can give bounds of $O(\frac{n^2}{r} \cdot \log \frac{n}{r})$

Limitations of Untouched Minor

- This method can give bounds of $O(\frac{n^2}{r} \cdot \log \frac{n}{r})$
- Limitation 1:
  There is a set of $O(\boxed{\frac{n^2}{r} \cdot \log \frac{n}{r}})$ elements of a matrix that touches every $r \times r$ submatrix

Ideally: even if we change $n^{3/2}$ entries
there is a $\frac{n}{100} \times \frac{n}{100}$ untouched submatrix

Impossible: change $1000n$ entries
and touch every $\epsilon n \times \epsilon n$ submatrix

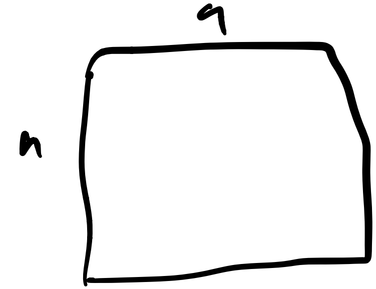
Limitations of Untouched Minor

- This method can give bounds of $O(\frac{n^2}{r} \cdot \log \frac{n}{r})$
- Limitation 1:
  There is a set of $O(\frac{n^2}{r} \cdot \log \frac{n}{r})$ elements of a matrix that touches every $r \times r$ submatrix

  all $r \times r$ submatrices have full rank
- Limitation 2:
  There is a matrix where all submatrices have full rank, yet it is not rigid

Limitation 1

Limitation 1



Theorem ([Lok00,Lok09])

There exists a constant $c > 0$ such that for any large enough n and $\log n \le r \le n$, there exists a set S of $c \boxed{\cdot \frac{n^2}{r} \log \frac{n}{r}}$ entries of an $n \times n$ matrix such that its every $r \times r$ submatrix intersects S.

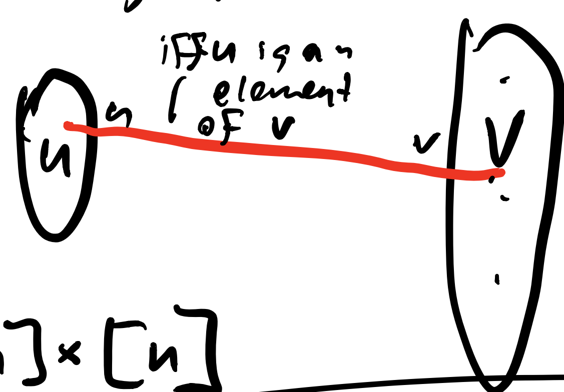
We will find $s = c \cdot \frac{n^2}{R} \cdot \log\left(\frac{n}{R}\right)$ entries of an $n \times n$ matrix that intersect every $R \times R$ submatrix.

Prob. Method: sample s random entries of an $n \times n$ matrix, then w. prob. > 0 we intersect every $R \times R$ submatrix

$\Rightarrow$ $\exists$ exists a choice of s entries s.t. they intersect every $R \times R$ submatrix

---

Bipartite graph.



$$V = \binom{[n]}{R} \times \binom{[n]}{R}$$

$$U = [n] \times [n]$$

Sample s random vertices on the left, they "cover" all vertices on the right.

$\deg(v) = R^2$ neighbors

Fix $v \in V$,

Sample one random vertex u on the left.

$\Pr[v$ is <u>not</u> covered by $u] =$

$$= 1 - \Pr[v \text{ is a neighbor of } u]$$

$$= 1 - \frac{R^2}{n^2}$$

$\Pr[v$ is <u>not</u> covered by $u_1, u_2, \ldots, u_s]$

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

Union bound: $\exists\, v \in V$ that is not covered?

$\Pr[\exists\, v \in V$ <u>not</u> covered by $u_1, u_2, \ldots, u_s]$

$$\leq |V| \cdot \left(1 - \frac{R^2}{n^2}\right)^s$$

Recall $s = 100 \cdot \frac{n^2}{R} \log\left(\frac{n}{R}\right)$

$1 + x \leq e^x$

$$\leq \binom{n}{R}^2 \cdot e^{-\frac{R^2}{n^2} \cdot s}$$

$\binom{n}{R} \leq \left(\frac{en}{R}\right)^R$

$$\leq \left(\frac{en}{R}\right)^{2R} e^{-\frac{\cancel{R^2}}{\cancel{n^2}} \frac{100 \cancel{n^2}}{\cancel{R}} \log\left(\frac{n}{R}\right)}$$

$$\leq \left(\frac{n}{R}\right)^{10R} \cdot \left(\frac{n}{R}\right)^{-100R} << 1$$

$\Rightarrow \mathbb{P}_R$[all vertices $v \in V$ are covered by q vertices] > 0. $\square$

Limitation 2

Super Regular Matrices

Definition

A matrix $A \in \mathbb{F}^{n \times n}$ is super regular if all of its square submatrices have full rank.

Explicit constructions.

Ideally: all super regular matrices are rigid.

Impossible: $\exists$ exist non-rigid super regular matrices

Super Regular Matrices

Definition

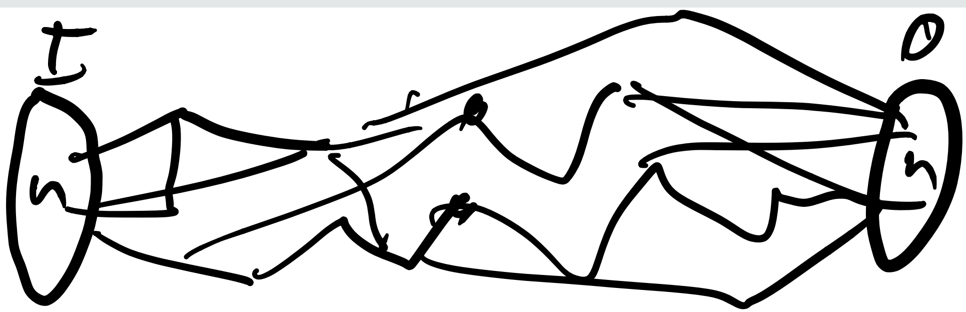
A matrix $A \in \mathbb{F}^{n \times n}$ is super regular if all of its square submatrices have full rank.

Goal: Show that there exists a super regular matrix that is not rigid

Superconcentrators

Definition (Superconcentrator)

Let G be a graph, and let I and O be two disjoint subsets of vertices of G called the inputs and outputs, respectively. G is a superconcentrator if for any $1 \leq k \leq \min\{|I|, |O|\}$, $I' \subset I$ and $O' \subseteq O$ of size $|I'| = |O'| = k$, there exist k vertex-disjoint paths from I' to O'.



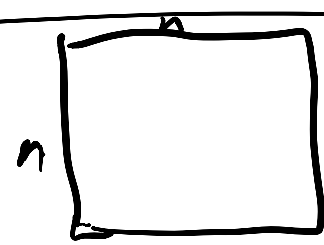
Superconcentrator.

$\Updownarrow$ Informally

$k=1$

$k=2$

Super regular matrices

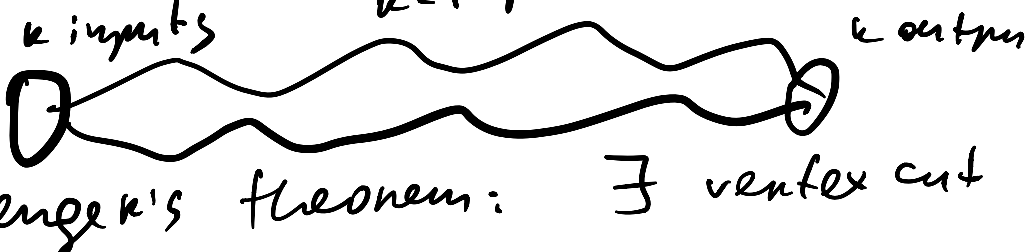
$M =$ 

— super regular

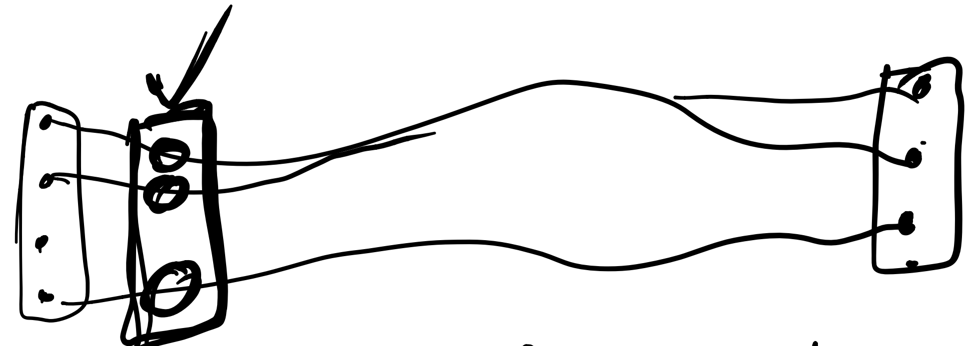
$x \to M \cdot x$

Every circuit that computes M must be a superconcentrator.

Proof: Assume not



Menger's theorem: $\exists$ vertex cut of size $\leq k-1$



$(k-1)$ vertices form a cut:

<u>Every</u> path from left to right must go through one of these vertices.

Then these k outputs compute some functions of $(k-1)$ functions computed in the cut.

$\Rightarrow$ these k outputs have rank $\le k-1$

$\Rightarrow$ matrix is <u>not</u> super regular - contradiction $\square$

Valiant conjectured that superconcentrators must have $\omega(n)$ size.

Valiant refuted this conjecture

Superconcentrators

Definition (Superconcentrator)

Let G be a graph, and let I and O be two disjoint subsets of vertices of G called the inputs and outputs, respectively. G is a superconcentrator if for any $1 \leq k \leq \min\{|I|, |O|\}$, $I' \subset I$ and $O' \subseteq O$ of size $|I'| = |O'| = k$, there exist k vertex-disjoint paths from I' to O'.

size of superconcentrator
= # edges in it.

Theorem

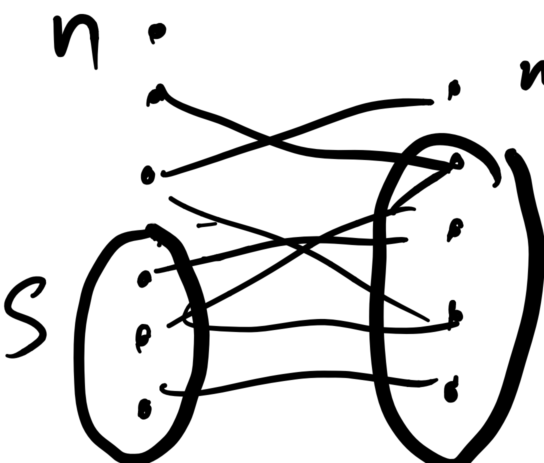
[[Val75]] For any $n \in \mathbb{N}$ large enough, there exists a superconcentrator G of size $O(n)$.

✓

Expanders

Definition ((n, m)-bipartite expander)

For any $n, m \in \mathbb{N}$ a (n, m)-bipartite expander is a bipartite graph $E_{n,m}$ with vertex sets U and V, where $|U| = n$ and $|V| = m$, such that for any $S \subseteq U$, $|S| \leq \frac{n}{2}$, $|N(S)| \geq |S|$.



$m = \frac{3n}{4}$

more than $|S|$ neighbors

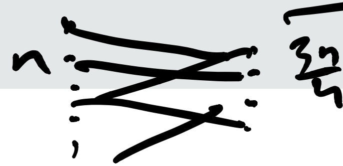
Expanders

Definition ((*n*, *m*)-bipartite expander)

For any $n, m \in \mathbb{N}$ a (n, m)-bipartite expander is a bipartite graph $E_{n,m}$ with vertex sets U and V, where $|U| = n$ and $|V| = m$, such that for any $S \subseteq U$, $|S| \leq \frac{n}{2}$, $|N(S)| \geq |S|$.

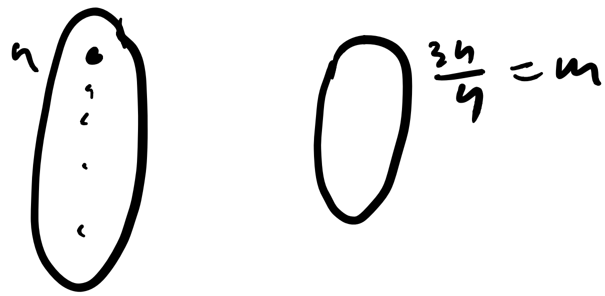
Lemma

For any large enough n and $m = \lceil \frac{3n}{4} \rceil$, there exists an (n, m)-bipartite expander $E_{n,m}$ with at most $\boxed{10n}$ edges.



clique
$\Theta(n^2)$ edges

$\exists$ $(n, \frac{3n}{4})$-bipartite expander by Prob. Method.



Every vertex is connected to 10 random vertices on the right.

Remains to show that w. $p > 0$ such a graph is expander.

Assume it's not expander

$k = |S| \le \frac{n}{2}$ vertices on the left

T = set of neighbors of S has size $|T| < |S| = k$

$\Pr[\exists\, |T| = k :$ all neighbors of S lie inside $T]$

$= \Pr[\underbrace{\exists |T|} = k :$ all $10k$ random vertices lie inside $T]$

$$= \left(\frac{|T|}{3n/4}\right)^{10k} \cdot \binom{3n/4}{k}$$

Union bound over all S

$$\sum_{k=0}^{n/2} \binom{n}{k} \cdot \binom{3n/4}{k} \cdot \left(\frac{|T|}{3n/4}\right)^{10k}$$

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k \qquad \binom{3n/4}{k} \leq \left(\frac{3ne}{4k}\right)^k$$

$$\leq \sum_{k=0}^{n/2} \left(\frac{1}{4}\right)^k < 1$$

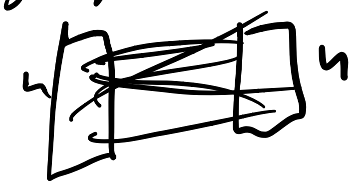
$\Rightarrow \exists$ exist such a graph $\square$

Theorem

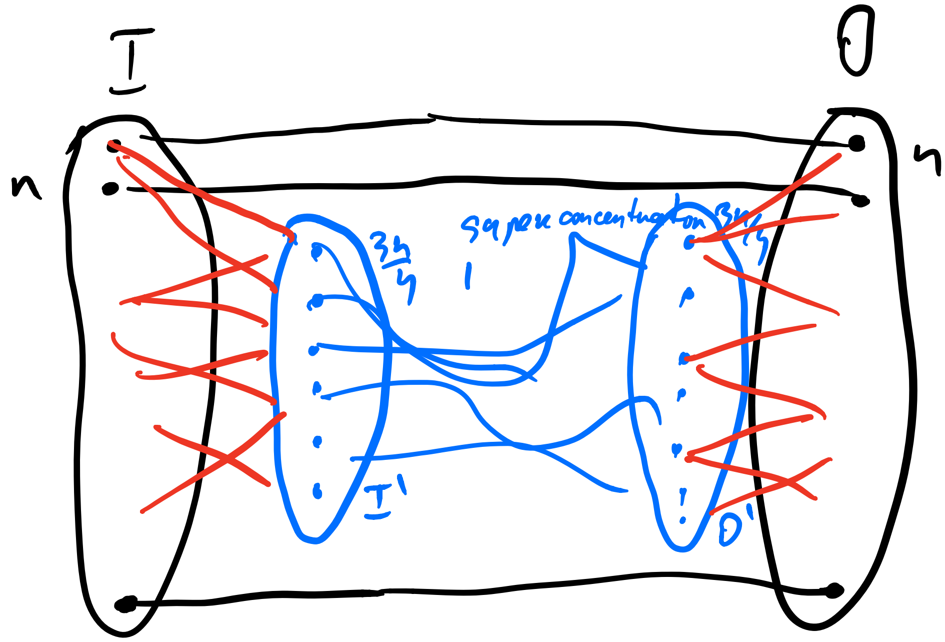
[[Val75]] For any $n \in \mathbb{N}$ large enough, there exists a superconcentrator G of size $O(n)$.

Induction on n. Cn edges

Don't care about small n, because $n \le C$ we take a complete bipartite graph $n^2 \le Cn$



n edges



n edges

superconcentrator from $\frac{3n}{4} \to \frac{3n}{4}$

2 expanders from $n \to \frac{3n}{4}$

Need to prove

(1) This graph is a superconcentrator

(2) It has $O(n)$ edges.

---

(2) $|G_n| \le 100n$

$$|G_n| \le n + |G_{3n/4}| + 20n$$

$$\le 21n + 100 \cdot \frac{3n}{4} < 100n$$

---

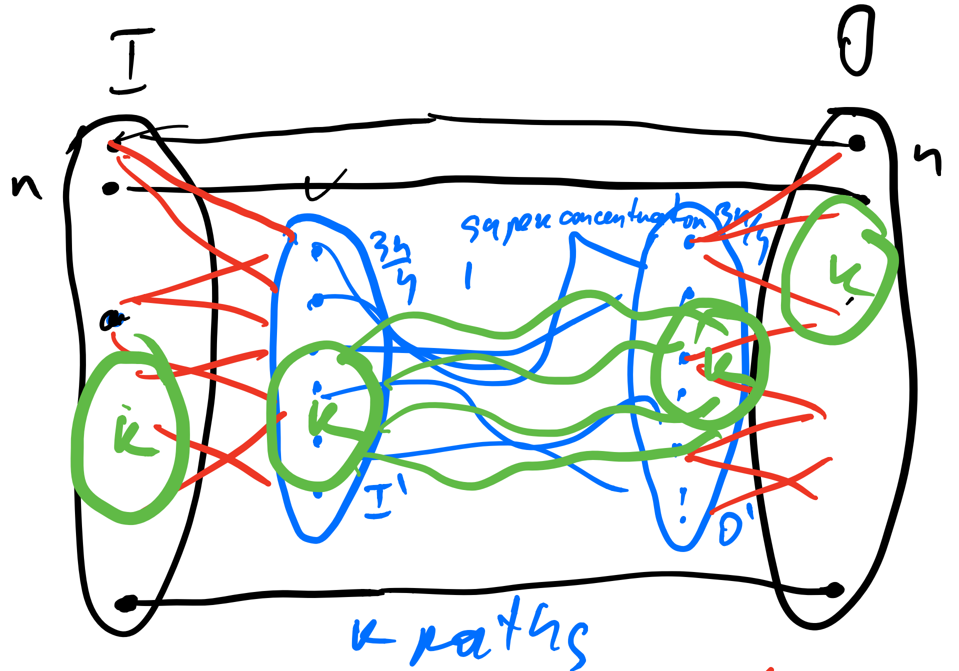
(1) Superconcentrator.

k inputs $S \subseteq I$ $\quad 1 \le k \le n$

k outputs $T \subseteq O$

$\Rightarrow$ I have k vertex disjoint paths from S to T.

Case 1 $k \le \frac{n}{2}$.



k paths

$k \Rightarrow k$ EXP PROP

SUPERC. PROP

$k \Leftarrow k$ EXP PROP

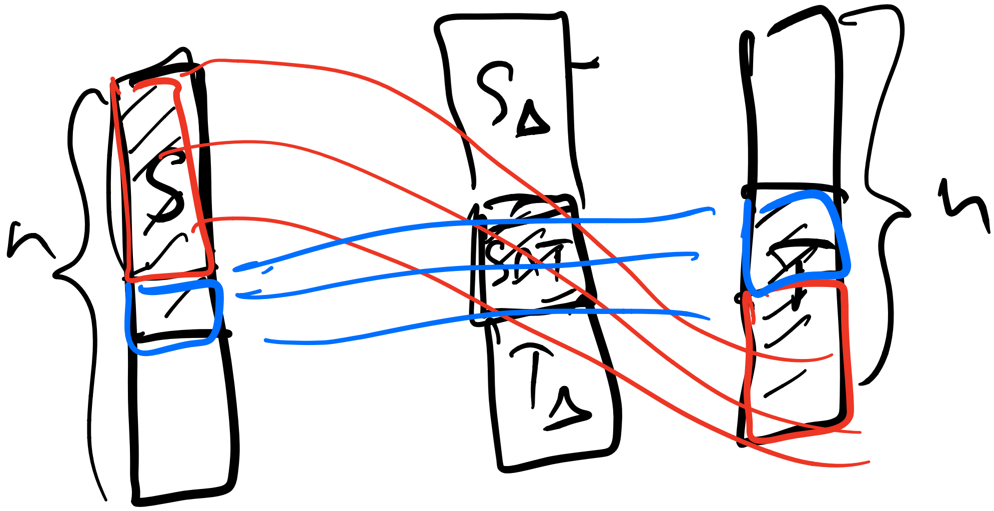
Case 2 $k \geq \frac{n}{2}$

$|S| = |T| = k$

$S, T \subseteq [n]$

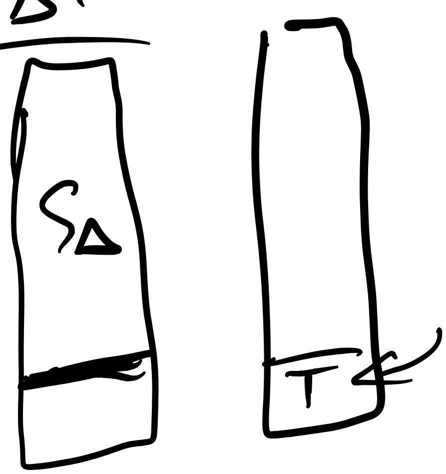
$$S_\Delta = S \setminus (S \cap T)$$

$$T_\Delta = T \setminus (S \cap T)$$



$$|S_\Delta| < n/2$$

$$|T_\Delta| < n/2$$



$|T| > \frac{n}{2}$

We want to find k paths from $S \to T$

(1) $|S_\Delta| \to |T_\Delta|$

$|S_\Delta| = |T_\Delta|$ paths

(2) $S \cap T$ paths from

$S \cap T \to S \cap T$

black edges

$S \to T$ $\square$