# Matrix Rigidity

## Rigidity in Sub-exponential time, Rigidity of Sparse Matrices

Sasha Golovnev

October 12, 2020

# Summary

| construction | rigidity | run-time |
| --- | --- | --- |

# Summary

| construction | rigidity | run-time |
|---|---|---|
| want | $(\varepsilon n, n^{1+\delta})$ | $\mathsf{E}^{\mathsf{NP}}$ |

would imply a new CLB

Time $2^{O(n)}$, an oracle for NP problems (even of exp. size)

# Summary

| construction | rigidity | run-time |
|---|---|---|
| want | $(\varepsilon n, n^{1+\delta})$ | $\mathbf{E}^{\mathsf{NP}}$ |
| brute force | $(\varepsilon n, n^2/\log n)$ | $2^{n^2}$ |

By Prob. Method (by counting)

a random is very rigid

# Summary

| construction | rigidity | run-time |
|---|---|---|
| want | $(\varepsilon n, n^{1+\delta})$ | $\mathsf{E}^{\mathsf{NP}}$ |
| brute force | $(\varepsilon n, n^2/\log n)$ | $2^{n^2}$ |
| explicit | $(r, \frac{n^2}{r} \cdot \log \frac{n}{r})$ | $\mathrm{poly}(n)$ |
| ECC | $(\varepsilon n, \Theta(n))$ | |

# Summary

| construction | rigidity | run-time |
|---|---|---|
| want | $(\varepsilon n, n^{1+\delta})$ | $\mathsf{E}^{\mathsf{NP}}$ |
| brute force | $(\varepsilon n, n^2 / \log n)$ | $2^{n^2}$ |
| explicit | $(r, \frac{n^2}{r} \cdot \log \frac{n}{r})$ | $\text{poly}(n)$ |
| Hankel | $(r, \frac{n^3}{r^2 \log n})$ <br> $(\varepsilon n, \Theta(\frac{n}{\log n}))$ | $2^n$ |

# Summary

| construction | rigidity | run-time |
|---|---|---|
| want | $(\varepsilon n, n^{1+\delta})$ | $\mathsf{E}^{\mathsf{NP}}$ |
| brute force | $(\varepsilon n, n^2 / \log n)$ | $2^{n^2}$ |
| explicit | $(r, \frac{n^2}{r} \cdot \log \frac{n}{r})$ | $\mathrm{poly}(n)$ |
| Hankel | $(r, \frac{n^3}{r^2 \log n})$ | $2^n$ |
| Sub-exponential | $(n^{0.5-\varepsilon}, n^2 / \log n)$ | $2^{n^{1-\varepsilon}}$ |

# Summary

| construction | rigidity | run-time |
|---|---|---|
| want | $(\varepsilon n, n^{1+\delta})$ | $\mathsf{E}^{\mathsf{NP}}$ |
| brute force | $(\varepsilon n, n^2/\log n)$ | $2^{n^2}$ |
| explicit | $(r, \frac{n^2}{r} \cdot \log \frac{n}{r})$ | $\mathrm{poly}(n)$ |
| Hankel | $(r, \frac{n^3}{r^2 \log n})$ | $2^n$ |
| Sub-exponential | $(n^{0.5-\varepsilon}, n^2/\log n)$ | $2^{n^{1-\varepsilon}}$ |
| Sparse | $(\underbrace{\varepsilon n}, \underbrace{n^{1+\delta}})$ | $\boxed{2^{n^{1+\delta}\log n}}$ |

CLB

# Rigidity in Sub-Exponential Time

# Main Theorem

**Theorem** $\mathbb{F}_q$

*For any $r$, in time $q^{O(r^2)}$, one can construct a matrix $A \in \mathbb{F}_q^{n\times n}$ such that*

$$\mathcal{R}_A^{\mathbb{F}_q}(r) \geq \Omega(\underline{n^2/\log r})\,.$$

$\mathbb{F}_q = \mathbb{F}_2$: $\quad R = \sqrt{n}$

In time $2^{O(n)}$, we construct

$$R_A^{\mathbb{F}_2}(\sqrt{n}) \geq \Omega(n^2/\log n)$$

# Main Theorem

**Theorem**

*For any r, in time $q^{O(r^2)}$, one can construct a matrix $A \in \mathbb{F}_q^{n\times n}$ such that*

$$\mathcal{R}_A^{\mathbb{F}_q}(r) \geq \Omega(n^2/\log r)\,.$$

✓

**Corollary**

*For any $\varepsilon > 0$, one can construct in sub-exponential time $2^{O(n^{1-2\varepsilon})}$ a matrix $A \in \mathbb{F}_2^{n\times n}$ such that*

$$\mathcal{R}_A^{\mathbb{F}_2}(\underline{n^{\frac{1}{2}-\varepsilon}}) \geq \Omega(n^2/\log n)\,.$$

**Theorem**

*For any r, in time $q^{O(r^2)}$, one can construct a matrix $A \in \mathbb{F}_q^{n\times n}$ such that*

$$\mathcal{R}_A^{\mathbb{F}_q}(r) \geq \Omega(n^2/\log r)\,.$$

Step I. Small rigid matrix

$\boxed{M \in \mathbb{F}_q^{2R\times 2R}}$, M is

$$R_M^{\mathbb{F}_q}(R) \geq \Omega(R^2/\log R)$$

By Prob Method (by counting),

$\exists\ M \in \mathbb{F}_q^{2R\times 2R}$ is $(R, R^2/\log R)$-rigid

Running time?

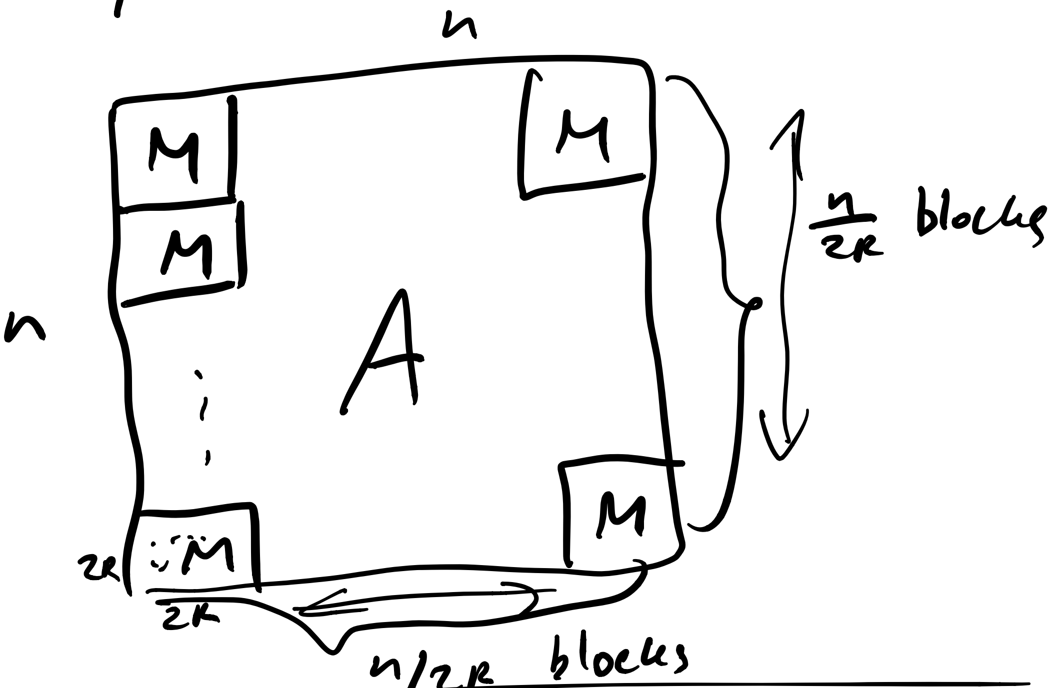
$$\boxed{M} \neq L + S \quad \in \mathbb{F}_q^{2R\times 2R}$$

$$q^{4R^2} \qquad q^{4R^2} \qquad q^{4R^2}$$

Time $(q^{4R^2})^3 \cdot \mathrm{poly}(R) = q^{O(R^2)}$

We have $M \in \mathbb{F}_q^{2R \times 2R}$ $(R, \Omega(R^2/\log R))$-rigid.

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




What is rigidity of A for rank A? We want drop the rank of A below R, we have to drop the rank of each copy of M below R.

Each copy requires $\Omega(R^2/\log R)$ changes to have rank $< R$.

We have to make

$\Omega(R^2/\log R)$ in each out

$\left(\frac{n}{2R}\right)^2$ copies

$$= \Omega(n^2/\log R).$$

In order to decrease $rk(A) < R$, one has to make $\Omega(n^2/\log R)$ changes

$$\Rightarrow \mathcal{R}_A(R) \geq \Omega(n^2/\log R) \quad \square$$

---

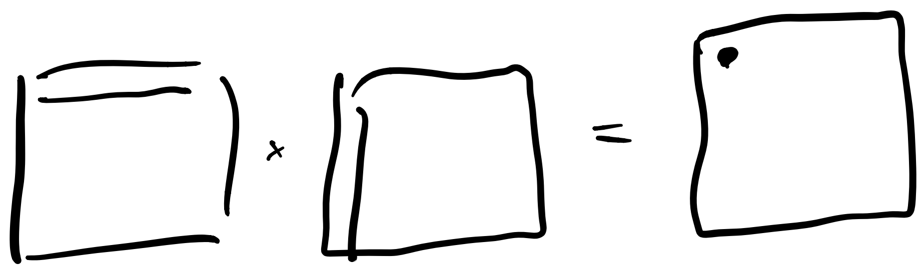
rank $(L)$ $n^3$

Gaussian El $n^\omega$,

$\omega$ - matrix mult. exp.

$A, B$ – matrices $n \times n$.

$A \cdot B$



$\boxed{\text{Trivial } O(n^3)}$

Eq problems: M Mult, M Square, rank of matrix, Gaussian El, Solving a system of n eqs, inverting matrix.

<u>Karatsuba</u> $O(n^{\log_2 7})$

<u>In theory:</u> $\simeq n^{2.3}$

$\omega$ = MM exponent.

$2 \le \omega \le 2.3$

# Rigidity in Super-Exponential Time

# Rigidity of Sparse Matrices

- How rigid can a $t$-sparse matrix $M$ be?

# Rigidity of Sparse Matrices

- How rigid can a $t$-sparse matrix $M$ be?

- At best: $\mathcal{R}(\varepsilon n) \geq \Omega(t)$

$$M = \underbrace{0}_{\text{low-rank}} + \underbrace{M}_{\text{sparsity} \leq t}$$

# Rigidity of Sparse Matrices

- How rigid can a $t$-sparse matrix $M$ be?
- At best: $\mathcal{R}(\varepsilon n) \geq \Omega(t)$
- In fact, this bound is tight

# Main Theorem

**Theorem**

*For every $t$, there exists a matrix $M \in \mathbb{F}_2^{n\times n}$ of sparsity $\|M\|_0 \le t$, and rigidity*

$$\mathcal{R}_M^{\mathbb{F}_2}(n/1000) > t/1000\,.$$

# Main Theorem

## Theorem

*For every $t$, there exists a matrix $M \in \mathbb{F}_2^{n\times n}$ of sparsity $\|M\|_0 \le t$, and rigidity*

later

$$\mathcal{R}_M^{\mathbb{F}_2}(n/1000) > t/1000 \,.$$

## Corollary

*For any $\varepsilon > 0$, one can construct in super-exponential time* $\boxed{2^{O(n^{1+\varepsilon}\log n)}}$ *a matrix $A \in \mathbb{F}_2^{n\times n}$ such that*

$> 2^n$

$$\mathcal{R}_A^{\mathbb{F}_2}(\delta n) \ge \Omega(n^{1+\varepsilon}) \,.$$

sufficient for CLB

Brute force $t$-sparse matrix $M$

whether

$$M = S + L$$

Brute force ONLY $M$ and $S$.

$$\mathrm{rk}(M - S)$$

$M$ is $n^{1+\varepsilon}$- sparse

$S$ is $\frac{n^{1+\varepsilon}}{1000}$- sparse

$$\binom{n^2}{\le n^{1+\varepsilon}} \cdot \binom{n^2}{\le \frac{n^{1+\varepsilon}}{1000}} \le$$

$$\le (n^2)^{n^{1+\varepsilon}} \cdot (n^2)^{\frac{n^{1+\varepsilon}}{1000}} < n^{10 n^{1+\varepsilon}} =$$

$$= 2^{O(n^{1+\varepsilon} \log n)}$$

$\square$

# First Attempt

- Can we prove it by counting?

# First Attempt

- Can we prove it by counting?
- We'd like to say that there exists a $t$-sparse rigid matrix $M$

# First Attempt

- Can we prove it by counting?
- We'd like to say that there exists a $t$-sparse rigid matrix $M$
- I.e., $\exists M, \|M\|_0 \leq t, M \neq L + S$ where

$$\mathrm{rk}(L) \leq r \text{ and } \|S\|_0 \leq s$$

# First Attempt

- Can we prove it by counting?
- We'd like to say that there exists a $t$-sparse rigid matrix $M$

$M = L + S$

- I.e., $\exists M, \|M\|_0 \leq t, M \neq L + S$ where

$L = M - S$

1. low-rank
2. sparse

$$\text{rk}(L) \leq r \text{ and } \|S\|_0 \leq s$$

- It would suffice to show that

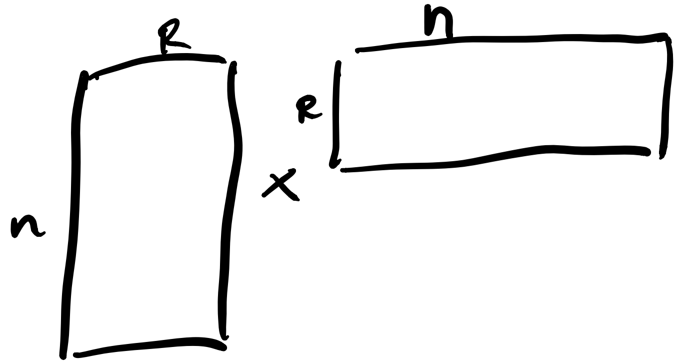
$$\overset{M}{(\#\text{ of } t\text{-sparse})} > \overset{L}{(\#\text{ of low-rank})} \times \overset{S}{(\#\text{ of } s\text{-sparse})}$$

$$\binom{n^2}{n^{1+\epsilon}} = 2^{n^{1+\epsilon}\log n} << 2^{\Omega(n^2)}$$

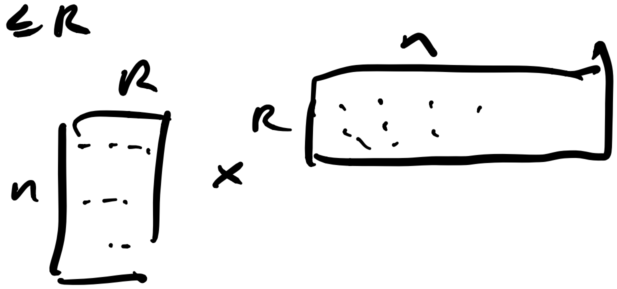
$\epsilon n$-rank

$$2^{\Theta(\epsilon n)} = 2^{\Theta(n^2)}$$

# of $n \times n$ matrices of rank $R$

$\approx$ 


$rk(M) \le R$ $\qquad \mathbb{F}_2$

$M =$ 


# of such matrices $\le 2^{n \cdot R} \cdot 2^{n \cdot R}$

$$\le 2^{2nR}$$

almost tight

# rank-$r$ matrices . $2^{\Theta(nR)}$

# First Attempt

- Can we prove it by counting?
- We'd like to say that there exists a $t$-sparse rigid matrix $M$
- I.e., $\exists M, \|M\|_0 \leq t, M \neq L + S$ where

$$\mathsf{rk}(L) \leq r \text{ and } \|S\|_0 \leq s$$

- It would suffice to show that

$$(\#\text{ of } t\text{-sparse}) > (\#\text{ of low-rank}) \times (\#\text{ of } s\text{-sparse})$$

- But this doesn't hold

# Proof Outline

- For a sparse matrix $M$, if
$$M = L + S\,,$$
then $L$ is sparse, too!

# Proof Outline

- For a sparse matrix $M$, if
$$M = L + S\,,$$
then $L$ is sparse, too!
- Instead of counting # of low-rank $L$, count # of sparse and low-rank

# Proof Outline

- For a sparse matrix $M$, if
$$M = L + S\,,$$
then $L$ is sparse, too!
- Instead of counting # of low-rank $L$, count # of sparse and low-rank
- We'll show that

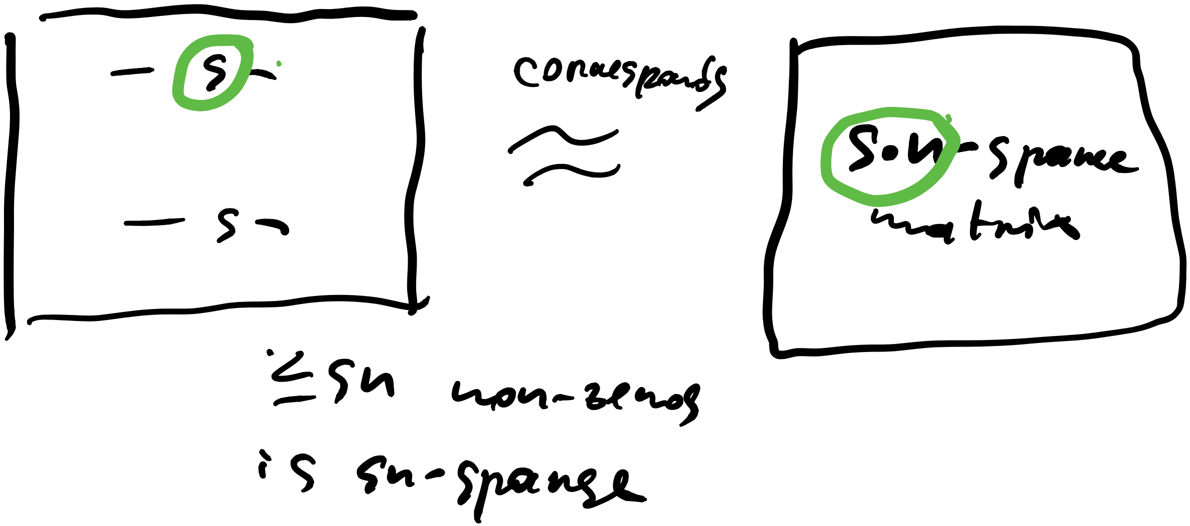
$$\begin{aligned}(\#\text{ of } t\text{-}\overset{M}{\text{sparse}}) > (\#\text{ of } \overset{L}{\text{sparse}} \text{ low-rank}) &\times \\ \times\, (\#\text{ of } s\text{-}\overset{S}{\text{sparse}})&\end{aligned}$$

# Proof Outline

- For a sparse matrix $M$, if
$$M = L + S\,,$$
then $L$ is sparse, too!
- Instead of counting # of low-rank $L$, count # of sparse and low-rank
- We'll show that
$$\begin{aligned}(\#\text{ of } t\text{-sparse}) &> (\#\text{ of sparse low-rank}) \times \\ &\times (\#\text{ of } s\text{-sparse})\end{aligned}$$
- Easier to work with regularly sparse matrices

# Regularly Rigid Matrices

A matrix is $s$-regularly-~~rigid~~ sparse if each row and each column has at most s non-zeros.



# Regularly Rigid Matrices

A matrix is $s$-regularly-~~rigid~~ sparse if each row and each column has at most $s$ non-zeros.

A matrix is $(r, s)$-regularly rigid if it's not a sum of $r$-rank and $s$-regularly-rigid matrices.

$$M \neq L + \underbrace{S}_{\text{reg } s\text{-sparse}}$$

Rigid is regularly rigid

reg rigid is not <u>nec.</u> rigid

# Regularly Rigid Matrices

A matrix is $s$-regularly-~~rigid~~ sparse if each row and each column has at most $s$ non-zeros.

A matrix is $(r, s)$-regularly rigid if it's not a sum of $r$-rank and $s$-regularly-rigid matrices.

**Claim**

The existence of $(\Omega(n), s)$-regularly-rigid matrix implies the existence of $(\Omega(n), \Omega(sn))$-rigid matrix.

Rigid matrix

$$M \neq L + S$$

Assume it's not rep rigid:

$$M = L' + S'$$

rep $S'$ is sparse,

---

**Claim** $M$ is $(\varepsilon n, s)$ - RR

$\Rightarrow$ $M$ is $\left(\frac{\varepsilon n}{2}, \frac{s \cdot n \cdot \varepsilon}{4}\right)$-rigid

**Proof.** Assume $M$ is not rigid.

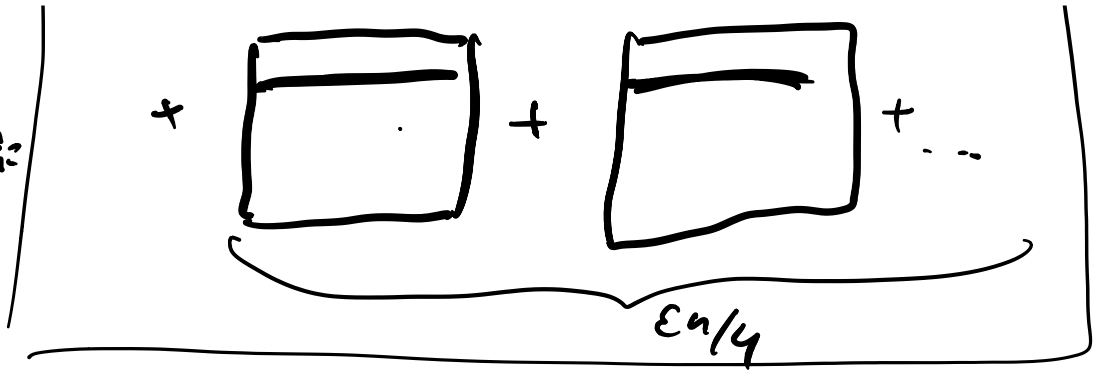
$M = L + S$.

Let me pick $\frac{\varepsilon n}{4}$ densest rows & $\frac{\varepsilon n}{4}$ densest cols in $S$,

$S'$ - be the rest of $S$.

$$M = \underbrace{L}_{\varepsilon n/2} + \underbrace{\square + \square + \dots}_{\varepsilon n/4}$$

rank ≤ $\frac{\varepsilon n}{2} + \frac{\varepsilon n}{4} + \frac{\varepsilon n}{4}$ $= \varepsilon n$




$+ S'$

$S$ was $s \cdot n \cdot \frac{\varepsilon}{4}$ - sparse

average row-sparsity was $s \cdot \frac{\varepsilon}{4}$

Markov's ineq:

$\leq \frac{1}{2}$ sparsity $\geq 2 \cdot s \cdot \frac{\varepsilon}{4}$

$\underbrace{\leq \frac{\varepsilon}{4}}$ sparsity $\geq \frac{4}{\varepsilon} \cdot s \cdot \frac{\varepsilon}{4} = s$

We removed $\frac{\varepsilon}{4} n$ densest rows $\Rightarrow$

remaining rows sparsity $\leq s$

---

Same for cols.

---

All rows cols of $S'$ have $\leq s$ non-zeros

$S'$ - reg sparse.

$M = L' + S'$, $\operatorname{rk}(L') \leq \varepsilon n$

$S'$ is $s$-reg-sparse $\square$

# Sparse Low-rank Matrices

**Lemma**

*The number of s-regularly sparse matrices $\in \mathbb{F}_2^{n \times n}$ of rank $\mathrm{rk}(M) \le r$ is at most*

$$n^{6rs}.$$

Compare # low-rank $2^{\theta(nr)}$

# Encoding of Matrices

**Lemma**

*Let $\mathcal{M}_n^r$ be the set of $\mathbb{F}^{n\times n}$ matrices of rank $r$. The mapping*

$$\phi\colon \mathcal{M}_n^r \to (\mathbb{F}^{1\times n})^r \times (\mathbb{F}^{n\times 1})^r \times [n]^{2r}$$

*defined as*

$$\phi(M) = (R, C, i_1, \ldots, i_r, j_1, \ldots, j_r)\ ,$$

*is a one-to-one mapping, where $R = (\mathrm{Row}_{i_1}(M), \ldots, \mathrm{Row}_{i_r}(M))$ and $C = (\mathrm{Col}_{j_1}(M), \ldots, \mathrm{Col}_{j_r}(M))$ are a row space basis and a column space basis of $M$.*

**Lemma**

*Let $\mathcal{M}_n^r$ be the set of $\mathbb{F}^{n\times n}$ matrices of rank r. The mapping*

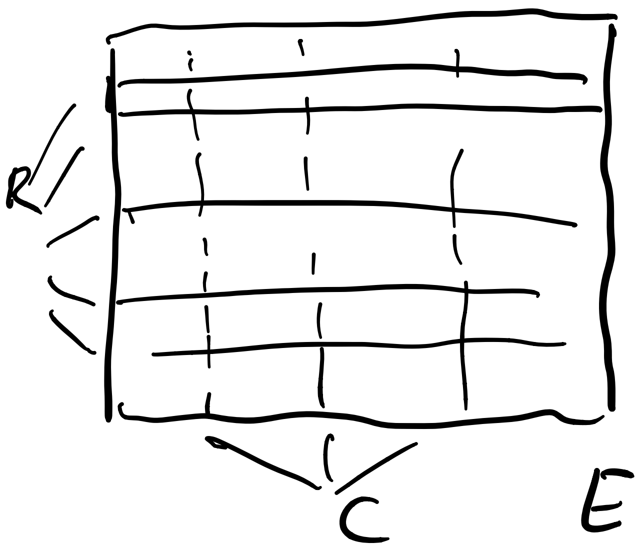
$$\phi\colon \mathcal{M}_n^r \to (\mathbb{F}^{1\times n})^r \times (\mathbb{F}^{n\times 1})^r \times [n]^{2r}$$

*defined as*

$$\phi(M) = (R, C, i_1, \ldots, i_r, j_1, \ldots, j_r)\ ,$$

*is a one-to-one mapping, where $R = (\mathrm{Row}_{i_1}(M), \ldots, \mathrm{Row}_{i_r}(M))$ and $C = (\mathrm{Col}_{j_1}(M), \ldots, \mathrm{Col}_{j_r}(M))$ are a row space basis and a column space basis of M.*

Rk(M) = R

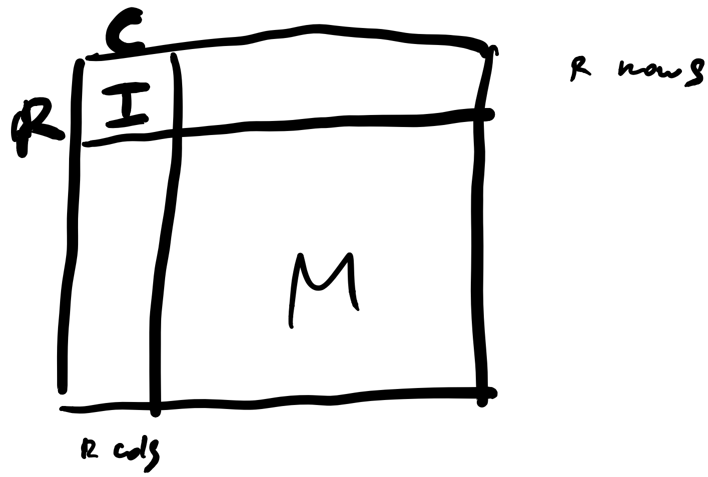



R, C – row & col bases

Encoding:

R, C, indices of these rows/cols in my matrix

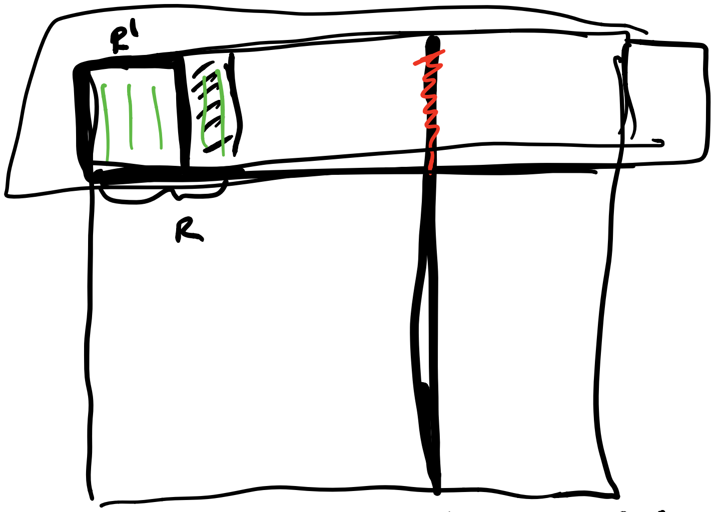
Given Encoding, I can <u>uniquely</u> identify M




Step I. $I$ is full-rank.

$$rk(I) = rk(M) = R$$

Assume $rk(I) = R' < R$




$$Col_m = \sum_{i \in R} \alpha_i \cdot Col_i$$

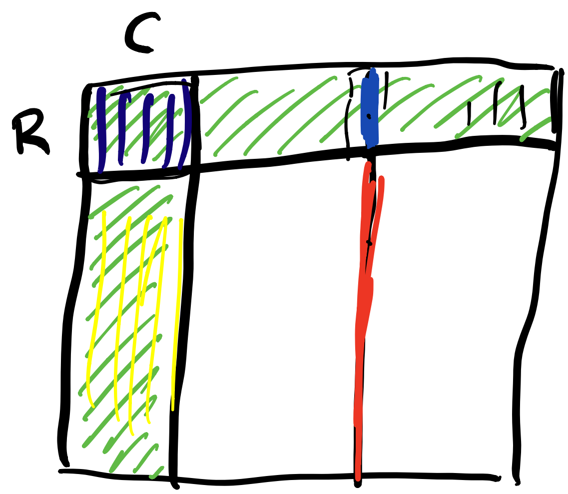
$$Col_m^{\le R} = \sum_{i \in R} \alpha_i \cdot Col_i^{\le R} = \sum_{i \in R'} \beta_i \cdot Col_i^{\le R}$$

The first R rows can be generated by just R' cols $\Rightarrow$ rank(R rows) $= R' < R$ – contradiction

## Step II

$R$, $C$, their indices

uniquely identify $M$



| = unique lin comb of |||| ,

because $I$ has full rank

| = the same lin comb of |||| .

We know lin comb, we know |||| ,

thus, recover | $\square$

# Main Theorem

**Theorem**

*For every $t$, there exists a matrix $M \in \mathbb{F}_2^{n \times n}$ of sparsity $\|M\|_0 \leq t$, and rigidity*

$$\mathcal{R}_M^{\mathbb{F}_2}(n/1000) > t/1000\,.$$

# t-sparse > # sparse low rank

× # $\frac{t}{1000}$ - sparse

**Lemma**

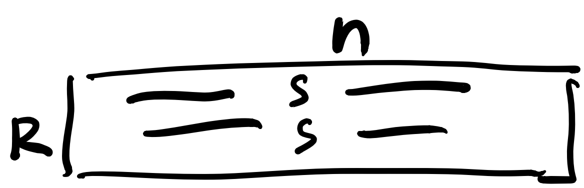
*The number of s-regularly sparse matrices $\in \mathbb{F}_2^{n\times n}$ of rank $\mathrm{rk}(M) \le r$ is at most*

$$n^{6rs}.$$

Every low-rank reg-sparse matrix can be encoded

$R, C, i_1, \ldots, i_R, j_1, \ldots, j_R$

# of low-rank reg-sparse matrices $\le$ # of such encodings.




$\le s \cdot R$ non-zeros

# matrices $R \le \binom{nR}{\le sR}$

# matrices $C \le \binom{nR}{\le sR}$

# $i_1, \ldots, i_R, j_1, \ldots, j_R \le n^{2R}$

(

$$\binom{nR}{\leq sR}^2 \cdot n^{2R} \leq$$

$$\leq (nR)^{3sR} \cdot n^{2R}$$

$[R \leq n]$

$$\leq n^{6Rs} \qquad \square$$