Matrix Rigidity

Rigidity of Hankel Matrices, Rigidity in Sub-exponential Time

Sasha Golovnev

October 7, 2020

Known Bounds

- Want: $\mathcal{R}(n/100) \geq n^{1.01}$

Known Bounds

- Want: $\mathcal{R}(n/100) \geq n^{1.01}$
- Explicit: $\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$

Known Bounds

- Want: $\mathcal{R}(n/100) \geq n^{1.01}$
- Explicit: $\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$
- Random: $\mathcal{R}(0.5n) \geq \frac{n^2}{\log n}$

Known Bounds

- Want: $\mathcal{R}(n/100) \geq n^{1.01}$
- Explicit: $\mathcal{R}(r) \geq \frac{n^2}{r} \cdot \log \frac{n}{r}$
- Random: $\mathcal{R}(0.5n) \geq \frac{n^2}{\log n}$
- This lecture: $\mathcal{R}(r) \geq \frac{n^3}{r^2 \log n}$

n random bits

Hankel Matrices

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_2 & a_3 & \cdots & a_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n+1} & \cdots & a_{2n-1} \end{pmatrix}$$

2n-1 distinct els

k-Hankel Matrix

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{k+1} & a_{k+2} & \dots & a_{k+n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k(n-1)+1} & a_{k(n-1)+2} & \dots & a_{k(n-1)+n} \end{pmatrix}$$

each row has k new els

Main Theorem

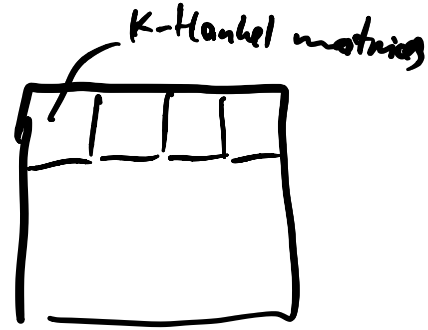
Theorem (GT16)

For any $\sqrt{n} \le r \le \frac{n}{32}$, *a random Hankel matrix* $A \in \mathbb{F}^{n \times n}$ *has*

$$\mathcal{R}_A^{\mathbb{F}_2}(r) \ge \Omega\left(\frac{n^3}{r^2 \log n}\right)$$

with probability $1 - o(1)$.

Proof Outline



Let k be a parameter and $m = \frac{n}{k}$.

Step I Any $n \times n$ Hankel matrix can be partitioned into $m \times m$ matrices each of which is k-Hankel.

Step II A random $m \times m$ k-Hankel matrix is $(m/2, \frac{km}{400 \log m})$-rigid with probability $1 - 2^{-km/20}$.

?

Finished the proof

Step II. Rigidity of k-Hankel Matrices

k-Hankel Matrices are Rigid

Lemma

For any $16 \le k \le m$, a random $m \times m$ k-Hankel matrix B has rigidity

$$\mathcal{R}_B^{\mathbb{F}_2}(m/2) \ge \frac{km}{400 \log m}$$

with probability at least $1 - 2^{-km/20}$.

Lemma

For any $16 \le k \le m$, a random $m \times m$ k-Hankel matrix B has rigidity

$$\mathcal{R}_B^{\mathbb{F}_2}(m/2) \ge \frac{km}{400 \log m}$$

with probability at least $1 - 2^{-km/20}$. ✓

Fix a matrix $S \in \mathbb{F}^{m \times m}$

We'll show that

$$\Pr_B\left[\mathrm{Rk}(B+S) \le \frac{m}{2}\right] \le 2^{-km/10}$$

Use this to finish the proof.

Union bound over all s-sparse S

$$s \le \frac{k \cdot m}{400 \log m}$$ ✓

$$2^{-km/10} \cdot [\#\ s\text{-sparse } S] =$$

$$= 2^{-km/10} \cdot \binom{m^2}{\le s}$$

$$\binom{n}{\le m} \le n^{2m}$$

$$\le 2^{-km/10} \cdot m^{4s} = 2^{-km/10 + 4s \log m}$$

$$= 2^{-km/10 + km/100} \le \underline{2^{-km/20}}$$

It remains to show that for a fixed

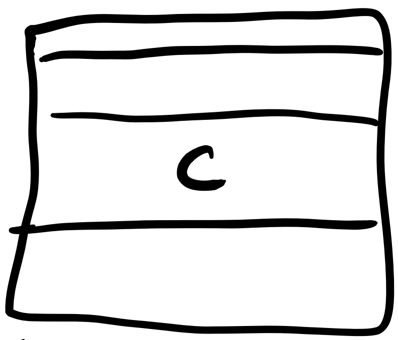
$S \in \mathbb{F}_2^{m \times m}$

$$\Pr_{B}\left[\operatorname{rk}(B+S) \le \frac{m}{2}\right] \le 2^{-km/10}$$

$C = B + S \in \mathbb{F}_2^{m \times m}$

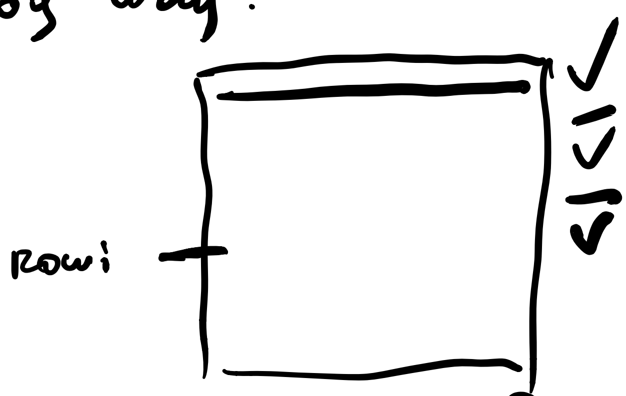
C_i - i^{th} row of C.

Assuming $\operatorname{rk}(C) \le \frac{m}{2}$



$\le \frac{m}{2}$ rows s.t. their lin comb generate all rows of C.

Let me choose row basis of C in a greedy way:



$I \subseteq [m]$ - the set of rows I greedily pick for basis.

$\forall i \in [m]$

$\checkmark$ (i) either $\underline{i \in I}$

(ii) or $C_i \in \underline{\text{span}}(\{C_{i'}\}_{\underline{i' \in [i-1]} \cap \underline{I}})$

We're bounding

$$\Pr_B[\text{rk}(C) \le \tfrac{m}{2}] =$$

$$= \Pr_B\left[\exists I \subseteq [m], |I| \le \tfrac{m}{2} : \quad \forall i \in [m] \setminus I: \; C_i \in \text{span}(\{C_{i'}\}_{i' \in [i-1] \cap I})\right]$$

(*) Fix $I \subseteq [m]$

We'll prove $\forall I \subseteq [m], |I| \le \frac{m}{2}$,

$$\Pr_B\left[\forall i \in [m] \setminus I : C_i \in \text{Span}(\{C_{i'}\}_{i' \in [i-1] \cap I})\right] \le 2^{-km/8} \quad (*)$$

Union bound over all $I \subseteq [m], |I| \le m/2$

$\binom{m}{\le \frac{m}{2}} \le 2^m$ (Because $k \ge 16$)

$$\underbrace{2^{-km/8}} \cdot \underbrace{2^m} \le \underbrace{2^{-km/10}}$$

It remains to show

Fix matrix S, Fix I, $|I| \le \frac{m}{2}$

$$\Pr_B\left[\underbrace{\forall i \in [m] \setminus I}: C_i \in \mathrm{Span}\left(\{C_{i'}\}_{i' \in [i-1] \cap I}\right)\right] \le 2^{-km/8} \quad (*)$$

Choose rows indices $1 \le i_1 < i_2 < \dots < i_\ell \le m$ s.t.

(i) $i_t \notin I$ ✓

(ii) $i_t - i_{t-1} \ge m/k$ ✓

recall in k-Hankel matrix, every row has k new els.
so after m/k rows, you have all (m) new els.

$$\begin{array}{c} \checkmark \\ \\ \checkmark \\ \\ \end{array}\begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ b_3 & b_4 & b_5 & b_6 \\ b_5 & b_6 & b_7 & b_8 \\ b_7 & b_8 & b_9 & b_{10} \end{bmatrix}$$

completely independent

$m \times m$

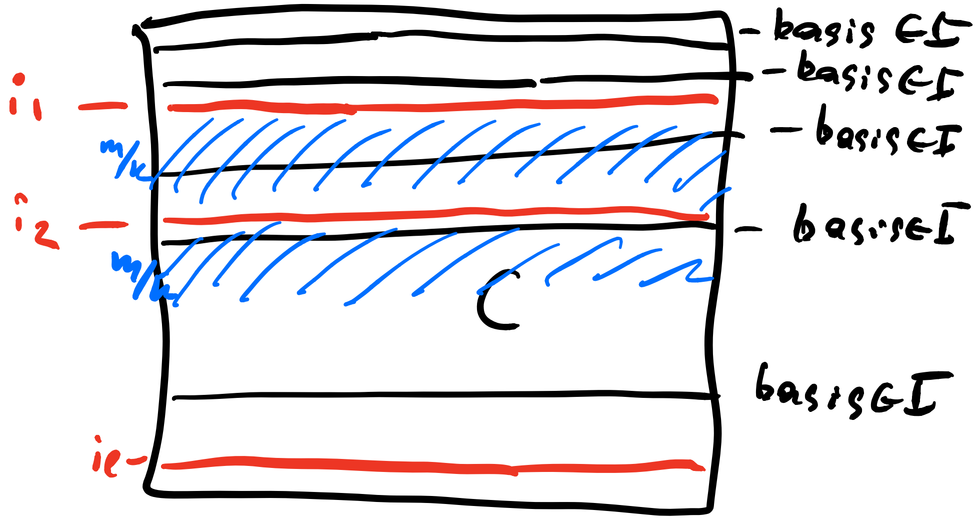
$m = 4$

k-Hankel

$k = 2$

$\frac{m}{k} = 2$

Choose in a greedy way $i_1, \dots, i_\ell$



Non-basis rows $[m] \setminus I$

at least $m/2$ of those

$\frac{m/2}{\lceil m/k \rceil} \geq k/4$ rows

$\ell \geq k/4$ ✓

$t \in [\ell]$

for red rows only

event E_t = the row $\boxed{i_t}$ is spanned

by $\{C_{i'}\}_{i' \in [i_t] \cap I}$

$$(*) \leq \Pr[E_1, E_2, \ldots, E_\ell]$$

$$= \Pr[E_1] \cdot \Pr[E_2 \mid E_1] \cdot \Pr[E_3 \mid E_1, E_2] \cdots \cdot \Pr[E_\ell \mid E_1 \ldots E_{\ell-1}]$$

We'll show that

✓ $\Pr_{B}[E_i \mid E_{i'}\ \forall i'<i] \leq 2^{-m/2}$

$(*) \leq (2^{-m/2})^{k/4} = 2^{-mk/8}$

which will finish the proof!

It remains to show that

$\Pr_{B}[E_t \mid E_{i'}\ \forall i'<t] \leq 2^{-m/2}$

Instead of conditioning on this

$\Pr_{B}[E_t \mid b_1, b_2, \ldots b_k \text{ s.t. } \underset{\text{happen}}{E_1 \ldots E_{t-1}}]$

---

we'll prove a stronger statement:

$\forall$ values $b_1, \ldots, b_{k(i_t-1)}$

$\Pr_{B}[E_t \mid b_1 \ldots b_{k(i_t-1)}] \leq 2^{-m/2}$

B (k-Hankel)

Fix

$$\begin{array}{l|cccc}
 & b_1 & b_2 & \cdots & b_m \\
 & b_{k+1} & b_{k+2} & \cdots & b_{k+m} \\
i_{t-1} & \cdots & & & \\
i_t - \frac{m}{k} & b_{k(i_t-1)-m+1} & \cdots & & b_{k(i_t-1)} \\
\updownarrow \ \frac{m}{k}-1 \text{ rows here} & & & & \\
i_t & b_{k(i_t-1)+1} & \cdots & & b_{k(i_t-1)+m}
\end{array}$$

Once I fix the green part of the matrix, the events $E_1, E_2, E_3, \dots, E_{t-1}$ determined

$$\Pr_B[E_t \mid b_1 \dots b_{k(i_t-1)}] \le 2^{-m/2}$$

(I only need to show $\Pr[E_t \mid E_1, \dots E_{t-1}] < 2^{-m/2}$)

It remains to show that for any set $b_1 \ldots b_{k(i_t-1)}$,

$$\Pr_B[E_t \mid b_1 \ldots b_{k(i_t-1)}] \le 2^{-m/2}$$

Assume that E_t holds:

c_{i_t} = linear comb of basis rows above it.

$$c_{i_t} = \sum_{i' \in [i_t-1] \cap I} d_{i'} \cdot c_{i'}, \quad \boxed{d_{i'} \in \{0,1\}}$$

Fix all $d_{i'} \in \{0,1\}$

$\le |I| \le \frac{m}{2}$

There are only $2^{m/2}$ ways to fix them

Union bound over all values of $d_{i'}$

$\Pr[E_t$ for a fixed $d_{i'}] \le 2^{-m}$

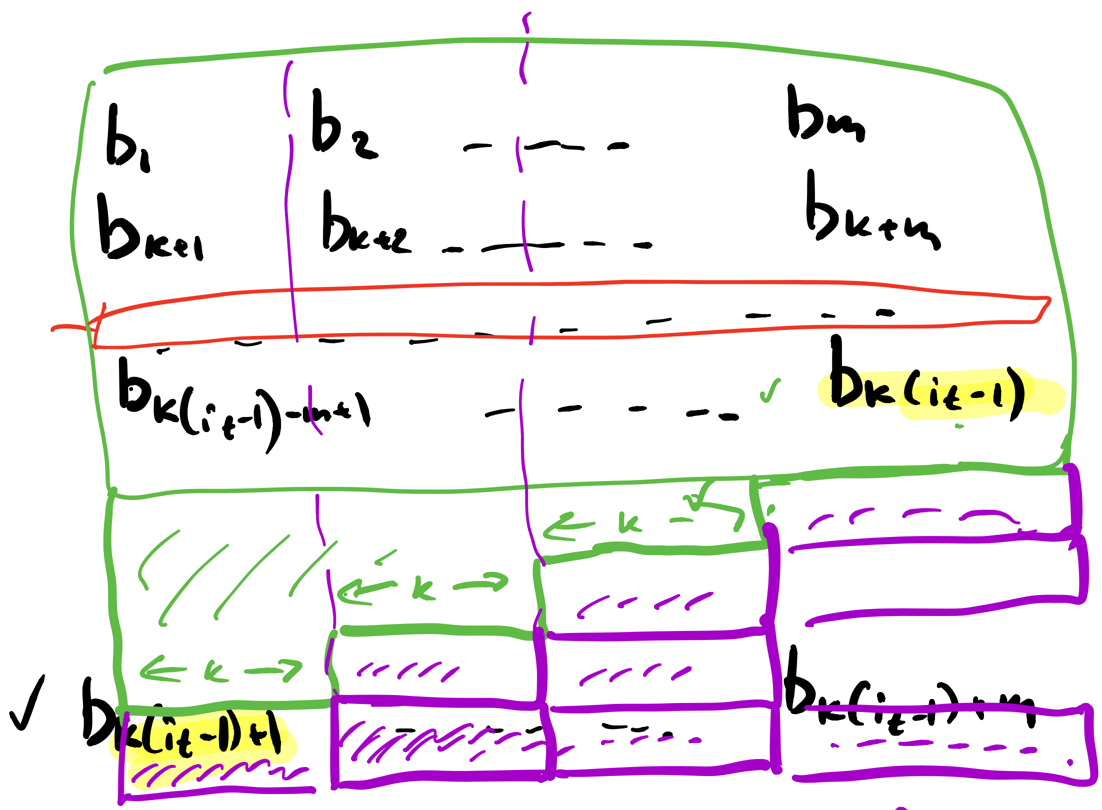
By UB: $2^{m/2} \cdot 2^{-m} \le 2^{-m/2}$

what we wanted.

Remains: $d_{i'} \in \{0,1\}$ are fixed

$$C_{i_t} = \sum_{i' \in [i_t - 1] \cap I} d_{i'} \cdot C_{i'}$$ ✓

$$\Pr[E_t \mid \ldots] \le 2^{-m}$$



Unique assignment to the m $\{0,1\}$ variables in the row i_t that satisfies fixed linear comb. $\Rightarrow$ $\Pr[E_t \mid \ldots] \le 2^{-m}$

$\square$

Explicitness

Theorem (GT16)

For any $\sqrt{n} \le r \le \frac{n}{32}$, *a random Hankel matrix* $A \in \mathbb{F}^{n \times n}$ *has*

$$\mathcal{R}_A^{\mathbb{F}_2}(r) \ge \Omega\left(\frac{n^3}{r^2 \log n}\right)$$

with probability $1 - o(1)$.

Rigidity:

given $A \in \mathbb{F}_2^{n \times n}$

R, S

check whether $\mathcal{R}_A^{\mathbb{F}_2}(R) \geq S$?

---

co-Rigidity

$$\mathcal{R}_A^{\mathbb{F}_2}(R) < S$$

$$A = S + L.$$

co-Rigidity $\in NP$

given solution

S, L

it is easy check

1. $A = S + L$
2. $\|S\|_0 \leq s$
3. $RK(L) \leq R$

poly-time

$\Rightarrow$ co-Rigidity $\in NP$

$\Rightarrow$ Rigidity $\in coNP$

$E^{\text{co-NP}} = E^{NP}$

Somewhat rigid matrix in E^{NP}.

Brute force all assignments to $b_1, \dots, b_{2n-1} \in \{0,1\}$.

Time $2^{O(n)}$

For each $b_1, \dots, b_{2n-1}$

I construct Hankel matrix$(b_1, \dots, b_{2n-1})$

co-NP oracle to check if it's rigid.

If it's rigid $\Rightarrow$ output it.

$$\frac{E^{NP}}{\exists \text{ somewhat rigid Hankel matrix.}}$$

In HW 2, you'll prove that this matrix is actually in E.