Matrix Rigidity

Rigidity of Hankel Matrices

Sasha Golovnev

October 5, 2020

Goal

- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds

Goal

- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds
- Want to prove these lower bounds in E^{NP}

Time $2^{O(n)}$ with an NP oracle

Goal

- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds
- Want to prove these lower bounds in E^{NP}
- Rigid matrix with n random bits will suffice

$2^n \in E$ brute force n bits

E^{NP}

Goal

- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds
- Want to prove these lower bounds in E^{NP}
- Rigid matrix with n random bits will suffice
- Know: n^2 random entries form rigid matrix

Goal

- Rigidity for rank $n/100$ and sparsity $n^{1.01}$ implies super-linear circuit lower bounds
- Want to prove these lower bounds in E^{NP}
- Rigid matrix with n random bits will suffice
- Know: n^2 random entries form rigid matrix
- Will show: n random bits give rigidity $\frac{n^3}{r^2 \log n}$

Not sufficient for CLB

But more rigid than known constructions

$R = n^{1-\varepsilon}$

Known Bounds

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

Known Bounds

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

$(r = \varepsilon n, \quad \Theta(n))$

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: $\mathcal{R}(0.5n) \geq \frac{n^2}{\log n}$

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

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: $\mathcal{R}(r) \geq \frac{n^3}{r^2 \log n}$ $(r = \varepsilon n \quad \Theta(\frac{n}{\log n}))$

If $r = \sqrt{n}$ $\quad R(r) \geq \frac{n^2}{\log n}$

Previously: $r = \sqrt{n}$ $\quad R(r) \geq n^{3/2} \log n$

Hankel Matrices

Definition

$A \in \mathbb{F}^{n \times n}$ is a Hankel matrix if $A_{i,j} = a_{i+j}$ for some $a_2, a_3, \ldots, a_{2n} \in \mathbb{F}$.

$$\begin{array}{cc} & n \\ n & \begin{bmatrix} a_2 & a_3 & a_4 & a_5 & \cdots & a_{n+1} \\ a_3 & a_4 & a_5 & \cdots & & a_{n+2} \\ a_4 & a_5 & & & & a_{n+3} \\ \vdots & & & & & \\ a_{n+1} & & & & & a_{2n} \end{bmatrix} \end{array}$$

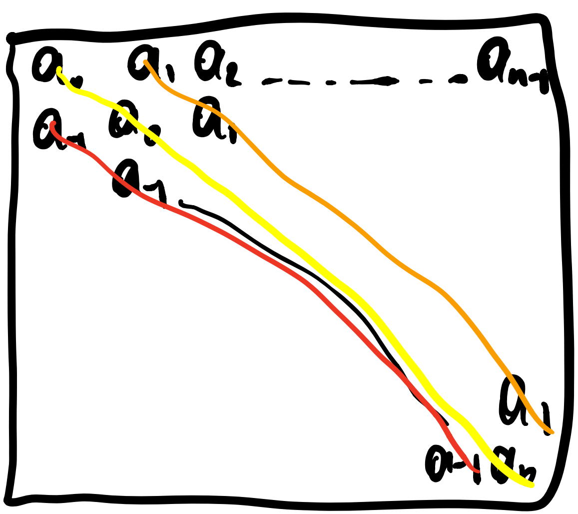
2n-1 distinct values in n×n matrix

Hankel Matrices

Definition

$A \in \mathbb{F}^{n\times n}$ is a Hankel matrix if $A_{i,j} = a_{i+j}$ for some $a_2, a_3, \ldots, a_{2n} \in \mathbb{F}$.

A is a Toeplitz matrix if $A_{i,j} = a_{i-j}$ for some $a_{-(n-1)}, a_{-(n-2)}, \ldots, a_{n-1} \in \mathbb{F}$.



2n-1 entries completely specify n×n matrix

Hankel Matrices

$\Theta(n)$ bits to specify a Hankel matrix, but these matrices are "pseudorandom"

"" for many applications they're as good as random

$A \in \{0,1\}^{n \times n}$ - Hankel matrix

$b \in \{0,1\}^n$

$f_{A,b} : \{0,1\}^n \to \{0,1\}^n$

$f_{A,b}(x) = A \cdot x + b$ (over $\mathbb{F}_2$)

$\{f_{A,b}\}$ – pairwise independent hash functions.

HW 1.

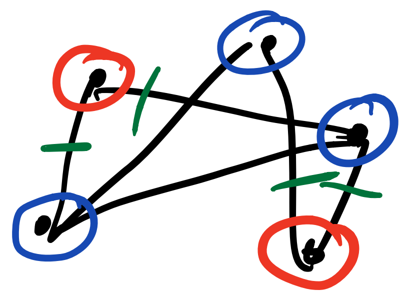
Pairwise independence

MAX-CUT problem

G n vertices m edges.

$S \subseteq [n]$ - subset of vertices

$cut(S)$ = # of edges between S and $\overline{S}$



O - S

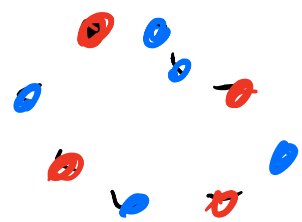
O - $\overline{S}$

MAX-CUT problem asks you to find S that maximizes $cut(S)$

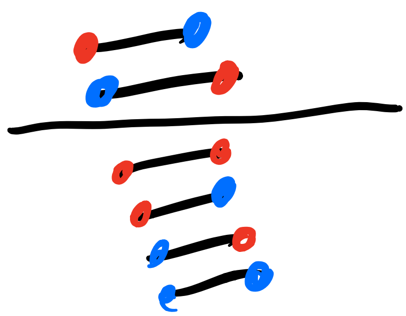
Trivial 0.5-apx for MAX-CUT

Every vertex v is included in S ind. w $p = \frac{1}{2}$.

$\forall$ every edge e



$\Pr[e \text{ is cut}]$

$=$  $= \frac{1}{2}$

$$E[\text{cut edges}] = E\left[\sum_e I_e\right]$$

$$= \sum_e E[e \text{ is cut}]$$

$$= \sum_e \frac{1}{2} = \frac{m}{2}$$

Derandomization

Randomized Alg:

pick n random bits

$b_1 \ldots b_n$

If $b_i = 1$ Then

include v_i in S

Else

do not include v_i in S

In the analysis, we only used the fact that for every pair of vertices

$\frac{1}{2}$ we have red-blue pair.

---

n random bits

$\Downarrow$

n pairwise independent bits

You only need $O(\log n)$ random bits to generate n pairwise ind. bits

---

This derandomizes MAX-CUT

brute-force $O(\log n)$ bits in time $2^{O(\log n)} = \text{poly}(n)$

$\Downarrow$

poly-time deterministic alg for MAX-CUT

BPP – poly-time using randomness

P – poly-time det. alg.

$$P \stackrel{?}{=} BPP$$

is derandomization of poly-time algs possible?

Derandomization E, EXP

Main Theorem

Theorem (GT16)

For any $\sqrt{n} \le r \le \frac{n}{32}$, with probability $1 - o(1)$ a random Hankel/Toeplitz matrix A has

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

$r = \sqrt{n} \implies R(r) \geq \Omega\left(\frac{n^2}{\log n}\right)$

k-Hankel Matrix

Definition

$A \in \mathbb{F}^{n\times n}$ is a k-Hankel matrix if $A_{i,j} = a_{k(i-1)+j}$ for some $a_1, a_2, \ldots, a_{(n-1)k+n} \in \mathbb{F}$

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

Ex. $k=1$

$$\begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ a_2 & a_3 & \cdots & a_{n+1} \\ a_3 & a_4 & \cdots & a_{n+2} \\ \vdots & & & \\ a_n & & \cdots & a_{2n-1} \end{bmatrix}$$

Hankel.

In particular, every row has one new random elt.

Ex. $k=n$

$$\begin{matrix} a_1 & \cdots & a_n \\ a_{n+1} & & a_{2n} \\ a_{2n+1} & & a_{3n} \\ \vdots & & \\ a_{n^2-n+1} & & a_{n^2} \end{matrix}$$

— completely random matrix.

Random k-Hankel matrix

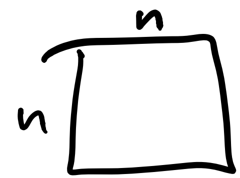
$k=1$ – Hankel (each row has one new random bit)

k-Hankel k new random bits per row

$k=n$ – Random (each row has n new random bits)

Proof Outline

Hankel ≡ 1-Hankel is rigid



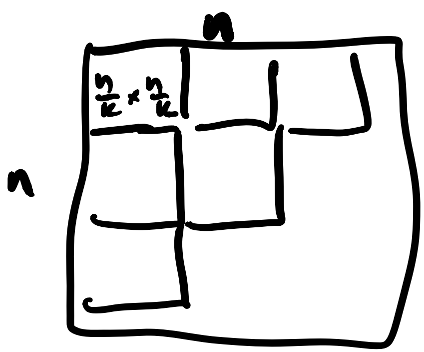
Let k be a parameter and $m = \frac{n}{k}$.

Proof Outline

∀ value of k.

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

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



k^2 matrices

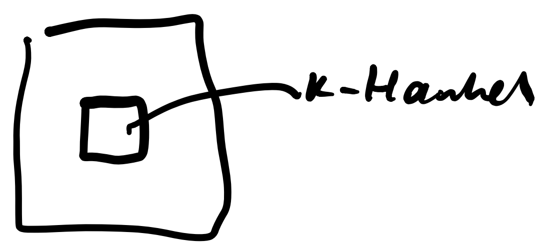
each matrix is $\boxed{\text{k-Hankel}}$

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 $1 - 2^{-km/20}$.



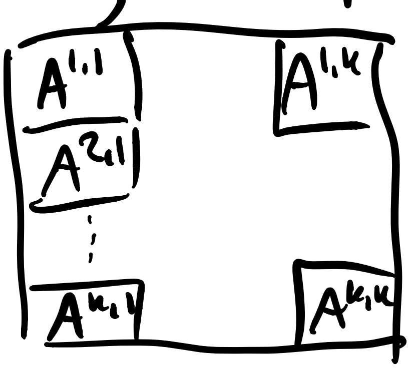
Theorem (GT16)

For any $\sqrt{n} \le r \le \frac{n}{32}$, with probability $1 - o(1)$ a random Hankel/Toeplitz matrix A has

$$\mathcal{R}_A^{\mathbb{F}_2}(r) \ge \Omega\left(\frac{n^3}{r^2 \log n}\right). \quad \checkmark \quad \ge \frac{n^3}{1600 R^2 \log n}$$

$m = 2 \cdot R \qquad k = \frac{n}{m}$

Using Step I: partition A into k^2 matrices A^{ij}, each A^{ij} is $m \times m$, is k-Hankel



$A = S + L$,

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

$\|S\|_0 = \frac{n^3}{1600 R^2 \log n} = \frac{n^3}{400 m^2 \log n}$

$A^{ij} = S^{ij} + L^{ij}$

$$\|S\|_0 = \frac{n^3}{1600\,k^2 \log n} = \frac{n^3}{400 m^2 \log n}$$

$$S = \begin{bmatrix} S_{11} & S_{k1} \\ S_{k1} & S_{kk} \end{bmatrix}$$

$$\exists\ \underline{\underline{i,j}} : \quad \|S^{ij}\|_0 \le \frac{\|S\|_0}{k^2}$$

$$= \frac{n^3}{400 m^2 k^2 \log n} =$$

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

$$= \frac{n}{400 \log n} = \frac{km}{400 \log n}$$

$$\boxed{A^{i,j} = S^{i,j} + L^{i,j}}$$

$$\|S^{i,j}\| \le \frac{km}{400 \log n}$$

$$\mathrm{Rk}(L^{i,j}) \le \mathrm{Rk}(L) \le \frac{m}{2}$$

$$A^{i,j} = S^{i,j} + L^{i,j}$$

$$\|S^{i,j}\| \le \frac{km}{400\log n}$$

$$Rk(L^{i,j}) \le Rk(L) \le \frac{m}{2}$$

$A^{i,j}$ is k-Hankel

Step II.

which is k-Hankel.

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

$$A^{i,j} \ne L^{i,j} + S^{i,j}$$

$$Rk(L^{i,j}) = \frac{m}{2}$$

$$\|S^{i,j}\|_0 = \frac{km}{400\log m}$$

Step II says

A_{ij} is rigid / we get contradiction

$1-2^{-n/20}$

There are k^2 $i,j\in[k]$.

One hand $\Pr \le 2^{-n/20}$

At least one of k^2 Bad events happens $\Pr \le k^2 \cdot 2^{-n/20}$

$$\le n^2 \cdot 2^{-n/20}$$

$$\le 2^{-n/10}$$

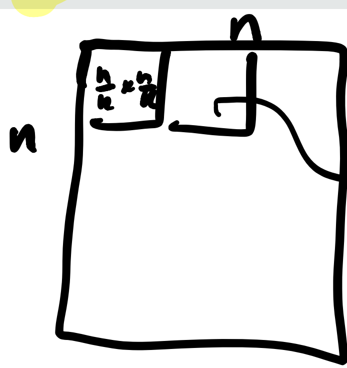
If I take random Hankel matrix A, then w p

$1-2^{-n/10}$, A is rigid $\square$

Step I. Partitioning Hankel Matrices

Lemma

Let $n, k \in \mathbb{N}$ such that k divides n. Then an $n \times n$ Hankel matrix can be partitioned into $\frac{n}{k} \times \frac{n}{k}$ k-Hankel matrices.



k^2 matrices

k-Hankel

Trivial

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

want to partition into k^2 $m \times m$ matrices

$\to$ Hankel matrix

$\underbrace{2m-1}$ random bits

m

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

$\to$ $\frac{n}{m}$-Hankel, i.e., k-Hankel

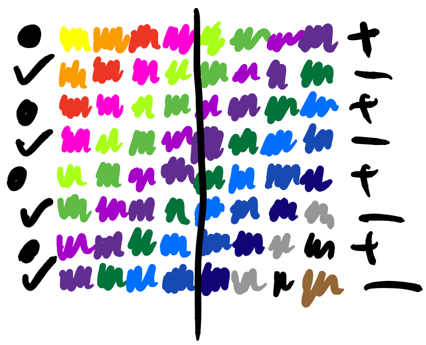
random bits in such submatrix:

$$m + \underbrace{k + k + \dots + k}_{m-1}$$

$= \Theta(n)$ bits

The big matrix has $2n$ random bits,

each submatrix has essentially all randomness from big matrix



• ✓ + — all are κ-Hankel.

$\square$