Matrix Rigidity

Rigidity of Hadamard. Review of Part I

Sasha Golovnev

September 14, 2020

Rigidity of Hadamard

Hadamard Matrix

WH, S, IP_2 matrix

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_4 = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{matrix}$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \text{ for } N = 2^n > 2\,.$$

Hadamard Matrix

$$H_4 = H_2 \otimes H_2 = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{matrix}$$

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \text{ for } N = 2^n > 2\,.$$

$$H_N = H_2^{\otimes n}\,.$$

$$\underset{n\times n}{A} \otimes \underset{n\times n}{B} = n^2 \overset{n^2}{\begin{pmatrix} a_{11}\cdot B & a_{12}\cdot B & \cdots & \\ & & & \\ & & & a_{n,n}\cdot B \end{pmatrix}}$$

Hadamard Matrix

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \text{ for } N = 2^n > 2\,.$$

$$H_N = H_2^{\otimes n}\,.$$

$$H_{u,v} = \langle u, v \rangle \text{ for } u, v \in \{0,1\}^n\,.$$

$$2^n \; u \quad 2^n \; v \quad (-1)^{\sum_{i=1}^{n} u_i v_i}$$

Rigidity of Hadamard

rigidity	reference

Rigidity of Hadamard

rigidity	reference
$\frac{n^2}{r^4 \log^2 r}$	Pudlák and Savickỳ, 88
$\frac{n^2}{r^3 \log r}$	Razborov, 88
$\frac{n^2}{r^2}$	Alon, 90
$\frac{n^2}{r^2}$	Lokam, 95
$\frac{n^2}{256r}$	Kashin and Razborov, 98
$\frac{n^2}{4r}$	de Wolf, 06

Rigidity of Hadamard

- We'll show that $\mathcal{R}_H^{\mathbb{R}}(r) \geq \frac{n^2}{4r}$ for every $r \leq n/2$.

Rigidity of Hadamard

- We'll show that $\mathcal{R}^{\mathbb{R}}_H(r) \geq \frac{n^2}{4r}$ for every $r \leq n/2$.
- For $r \geq n/2$, $\mathcal{R}^{\mathbb{R}}_H(r) \leq O(n)$.

Problem 4 (Hadamard is not rigid for high rank)**.** Let $N = 2^n$, and $H_N \in \mathbb{R}^{N \times N}$ be the Walsh-Hadamard matrix defined as follows.

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix}.$$

In particular, $H_N = H_2^{\otimes n}$, where $\otimes$ denotes the Kronecker product.

In this exercise, we will prove that H_N has low rigidity for rank $r \geq N/2$. Namely, $\mathcal{R}^{\mathbb{R}}_{H_N}(N/2) \leq N$.

- Let $A \in \mathbb{R}^{N \times N}$ have eigenvalues $\lambda_1, \ldots, \lambda_N$. Find the eigenvalues of $A - c \cdot I_N$ for $c \in \mathbb{R}$.
- Prove that if $A \in \mathbb{R}^{N \times N}$ has an eigenvalue of multiplicity k, then

$$\mathcal{R}^{\mathbb{R}}_A(N-k) \leq N.$$

- Finally, prove that

$$\mathcal{R}^{\mathbb{R}}_{H_N}(N/2) \leq N.$$

Rigidity of Hadamard

- We'll show that $\mathcal{R}_H^{\mathbb{R}}(r) \geq \frac{n^2}{4r}$ for every $r \leq n/2$.
- For $r \geq n/2, \mathcal{R}_H^{\mathbb{R}}(r) \leq O(n)$.

Problem 4 (Hadamard is not rigid for high rank)**.** Let $N = 2^n$, and $H_N \in \mathbb{R}^{N \times N}$ be the Walsh-Hadamard matrix defined as follows.

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix}.$$

In particular, $H_N = H_2^{\otimes n}$, where $\otimes$ denotes the Kronecker product.

In this exercise, we will prove that H_N has low rigidity for rank $r \geq N/2$. Namely, $\mathcal{R}_{H_N}^{\mathbb{R}}(N/2) \leq N$.

- Let $A \in \mathbb{R}^{N \times N}$ have eigenvalues $\lambda_1, \ldots, \lambda_N$. Find the eigenvalues of $A - c \cdot I_N$ for $c \in \mathbb{R}$.
- Prove that if $A \in \mathbb{R}^{N \times N}$ has an eigenvalue of multiplicity k, then
$$\mathcal{R}_A^{\mathbb{R}}(N-k) \leq N.$$
- Finally, prove that
$$\mathcal{R}_{H_N}^{\mathbb{R}}(N/2) \leq N.$$

- Later in the course we'll prove that H is not rigid for any $r = O(n)$.

Homework 1. Problem 5

Let $M \in \mathbb{C}^{m\times n}$, $k = \textbf{min}(m, n)$, $r = \textbf{rank}(M)$,

$$\sigma_1 \geq \ldots \geq \sigma_r > \sigma_{r+1} = \ldots = \sigma_k = 0$$

be the singular values of M. Then

- $\|M\|_F = \left(\sum_{i=1}^m \sum_{j=1}^n |M_{i,j}|^2\right)^{1/2} = \left(\sum_{i=1}^k \sigma_i^2\right)^{1/2}$.
- $\|M\|_2 = \sigma_1$.
- If M' is a submatrix of M, then $\sigma_i(M') \leq \sigma_i(M)$. In particular, $\|M'\|_2 \leq \|M\|_2$.

Rank of Hadamard's Submatrices

Lemma

For any submatrix $H' \in \mathbb{C}^{a \times b}$ *of Hadamard* $H \in \mathbb{C}^{N \times N}$,

$$\operatorname{rank}(H') \geq ab/N\,.$$

HOMEWORK 1. PROBLEM 5

Let $M \in \mathbb{C}^{m\times n}$, $k = \min(m, n)$, $r = \text{rank}(M)$,

$$\sigma_1 \geq \ldots \geq \sigma_r > \sigma_{r+1} = \ldots = \sigma_k = 0$$

be the singular values of M. Then

(1) $\|M\|_F = \left(\sum_{i=1}^m \sum_{j=1}^n |M_{i,j}|^2\right)^{1/2} = \left(\sum_{i=1}^k \sigma_i^2\right)^{1/2}$.

(2) $\|M\|_2 = \sigma_1$.

(3) If M' is a submatrix of M, then $\sigma_i(M') \leq \sigma_i(M)$. In particular, $\|M'\|_2 \leq \|M\|_2$.

Lemma

For any submatrix $H' \in \mathbb{C}^{a\times b}$ of Hadamard $H \in \mathbb{C}^{N\times N}$,

$$\text{rank}(H') \geq ab/N\,.$$

$$\|H'\|_F^2 \overset{(1)}{=} \sum_{i=1}^{r} \sigma_i^2 \leq \sigma_1^2 \cdot \text{Rank}(H')$$

$$\overset{(2)}{=} \|H'\|_2^2 \cdot \text{Rank}(H')$$

$$\overset{(3)}{\leq} \|H\|_2^2 \cdot \text{Rank}(H')$$

$$\|H'\|_2^2 = \sum_{i=1}^{a}\sum_{j=1}^{b} H'^2_{ij}$$

$$= \left[H' \in \{\pm 1\}^{a\times b}\right] = a \cdot b$$

$$\sigma_i(H) = \sqrt{N} \Rightarrow \|H\|_2^2 = N$$

$$\underset{a \cdot b}{\|H'\|_F^2} \leq \underset{= N}{\|H\|_2^2} \cdot \text{rank}(H')$$

$$\sigma_i(H) = \sqrt{N} \qquad \sigma_i(H) = \sqrt{\lambda_i(HH^T)}$$

$$H \cdot H^T = N \cdot I_N$$

H_2 holds

$$H_N = H_{\sqrt{N}} \otimes H_{\sqrt{N}}$$

$$H_N \cdot H_N^T = (H_{\sqrt{N}} \otimes H_{\sqrt{N}}) \cdot (H_{\sqrt{N}}^T \otimes H_{\sqrt{N}})$$

$$= (H_{\sqrt{N}} \cdot H_{\sqrt{N}}^T) \otimes (H_{\sqrt{N}} \cdot H_{\sqrt{N}}^T)$$

$$= (\sqrt{N} \cdot I_{\sqrt{N}}) \otimes (\sqrt{N} \cdot I_{\sqrt{N}})$$

$$= N \cdot I_N$$

Lower Bound for Hadamard

Theorem

Let $H \in \mathbb{C}^{N \times N}$ be the Hadamard matrix. For every $r \leq N/2$,

$$\mathcal{R}_H^{\mathbb{C}}(r) \geq \frac{N^2}{4r} .$$

Theorem

Let $H \in \mathbb{C}^{N \times N}$ be the Hadamard matrix. For every $r \leq N/2$,

$$\mathcal{R}_H^{\mathbb{C}}(r) \geq \frac{N^2}{4r}.$$

$H = L + S$

$\mathrm{Rank}(H+S) \leq R$

$\|S\|_0 = s$

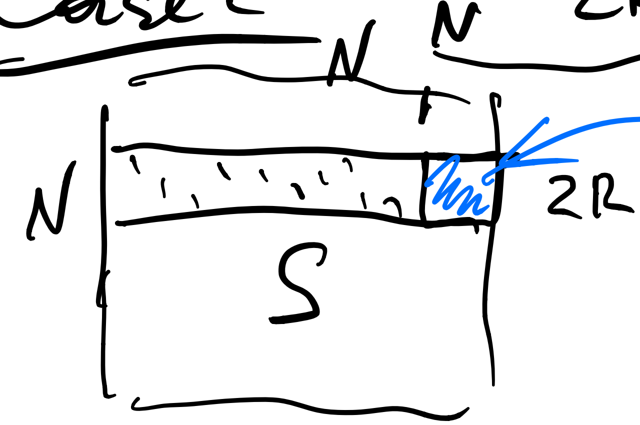
2R sparsest rows of S

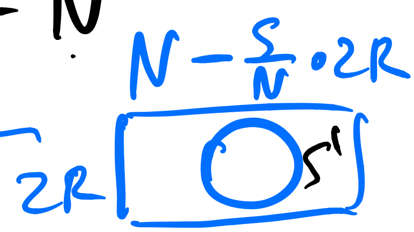
$\leq \frac{s}{N} \cdot 2R$ non-zeros

Case 1. $\frac{s}{N} \cdot 2R \geq N$

Done: $s \geq \frac{N^2}{2R} > \frac{N^2}{4R}$

Case 2 $\frac{s}{N} \cdot 2R < N$





$H' \in \mathbb{R}^{a \times b}$ $\mathrm{rk}(H') \geq a \cdot b / N$

$\mathrm{Rk}(H+S) \geq \mathrm{Rk}(H'+S') = \mathrm{Rk}(H')$

$$\mathrm{Rk}(H+S) \geq \mathrm{Rk}(H') = \underline{a} \cdot \underline{\underline{b}} / \underline{\underline{\underline{N}}}$$

$$= \underline{2R} \cdot \underline{\underline{\left(N - \frac{S}{N} \cdot 2R\right)}} / \underline{\underline{\underline{N}}} \leq R$$

$$\Downarrow$$

$$S \geq \frac{N^2}{4R} \qquad \square$$

Review of Part I

Review of Part I

- Moderately rigid matrices imply super-linear circuit lower bounds

Review of Part I

- Moderately rigid matrices imply super-linear circuit lower bounds
- A random matrix is extremely rigid

Review of Part I

- Moderately rigid matrices imply super-linear circuit lower bounds
- A random matrix is extremely rigid
- Construct rigid matrices non-explicitly (using randomness or large entries or super-exponential time)

Review of Part I

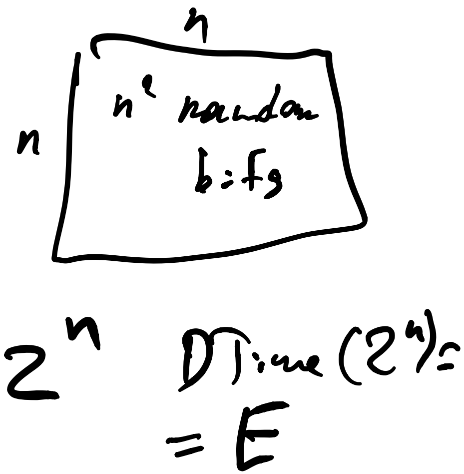
- Moderately rigid matrices imply super-linear circuit lower bounds
- A random matrix is extremely rigid
- Construct rigid matrices non-explicitly (using randomness or large entries or super-exponential time)
- Construct explicit matrices with rigidity $\frac{n^2}{r} \log \frac{n}{r}$

Overview of Part 2

- We will see semi-explicit constructions of rigid matrices

Overview of Part 2

- We will see semi-explicit constructions of rigid matrices
- Use fewer bits of randomness



Overview of Part 2

- We will see semi-explicit constructions of rigid matrices
- Use fewer bits of randomness
- Use fewer algebraically independent/large entries

n^2 entries
alg ind

Overview of Part 2

- We will see semi-explicit constructions of rigid matrices
- Use fewer bits of randomness
- Use fewer algebraically independent/large entries
- Use faster super-exponential algorithms $2^{O(n^2)}$

Tools Used in Part I

Probabilistic Method

- A non-rigid matrix has structure:

$$A = \begin{pmatrix} B & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

$$A_{22} = A_{21} B^{-1} A_{12}$$

Probabilistic Method

- A non-rigid matrix has structure:

$$A = \begin{pmatrix} B & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad A_{22} = A_{21} B^{-1} A_{12}$$

- A random matrix does not have structure

Probabilistic Method

- A non-rigid matrix has structure:

$$A = \begin{pmatrix} B & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad A_{22} = A_{21} B^{-1} A_{12}$$

- A random matrix does not have structure

- Hence, a random matrix is rigid

Probabilistic Method. Example

Theorem

There exists a graph on $n = 2^{k/2-1}$ *vertices without cliques and independent sets of size* k. $(R(k,k) > 2^{k/2-1}.)$

∃ graph G on $n = 2^{k/2-1}$

G doesn't have k-clique, k-IS

Counting:

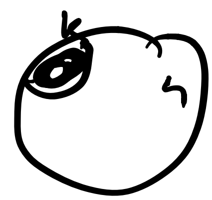
\# of Graphs on n vertices >

\# of Graphs on n vertices with k-cliques and k-IS.

$$\# \text{ of Graphs} = 2^{\binom{n}{2}}$$

\# of Graphs contains k-clique or k-IS $\quad 2^{\binom{n}{2}-\binom{k}{2}}$

$$\leq \binom{n}{k} \cdot 2 \cdot 2^{\binom{n}{2}-\binom{k}{2}}$$



$$2^{\binom{n}{2}} > 2^{\binom{n}{2}-\binom{k}{2}+1} \cdot \binom{n}{k}$$

$$2^{\binom{k}{2}-1} > \binom{n}{k}$$

$$n = 2^{k/2 - 1}$$

$$\binom{n}{k} \le n^k = 2^{\frac{k^2}{2} - k} \ll 2^{\binom{k}{2}}$$

<u>Prob.</u> Random graph G on n vertices, where each edge is included w.p. $\frac{1}{2}$.

$\Pr$[G does not contain k-clique or k-IS] > 0

$\Rightarrow \exists G$ does not contain k-clique or k-IS

$\Pr$[G contains k-clique or k-IS] < 1

$$\Pr[G \text{ contains a } k\text{-clique or } k\text{-ind}]$$

$$\leq \sum_{\substack{V' \subseteq V(G) \\ |V'| = k}} \Pr[V' \text{ is a } k\text{-clique or } k\text{-ind}]$$

$\binom{k}{2}$ edges

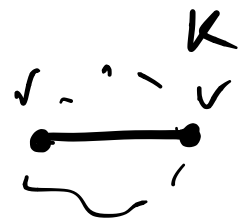
$$= \sum_{V'} \frac{2}{2^{\binom{k}{2}}} = \binom{n}{k} \cdot \frac{2}{2^{\binom{k}{2}}} < 1$$

$$\binom{n}{k} \leq n^k = \left(2^{\frac{k}{2}-1}\right)^k = 2^{\frac{k^2}{2}-k} \ll 2^{\binom{k}{2}}$$

□

k vertices

$$\binom{k}{2} = \frac{K \cdot (k-1)}{2}$$



Pr

$\Pr[V' \text{ is a clique OR } V' \text{ is an IS}]$

$= \Pr[V' \text{ is a clique}] + \Pr[V' \text{ is an IS}]$

$= \Pr[\binom{k}{2} \text{ is included}] + \Pr[\binom{k}{2} \text{ not included}]$

$= \left(\frac{1}{2}\right)^{\binom{k}{2}} + \left(\frac{1}{2}\right)^{\binom{k}{2}} = 2^{1-\binom{k}{2}}$

Prob. method:

- Sample a random graph
- GOOD w p. > 0

Conclude ∃ GOOD graph!

Algebraic Independence

- A non-rigid matrix satisfies a system of rational equations:

$$A = \begin{pmatrix} B & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad A_{22} = A_{21} B^{-1} A_{12}$$

Algebraic Independence

- A non-rigid matrix satisfies a system of rational equations:

$$A = \begin{pmatrix} B & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad A_{22} = A_{21} B^{-1} A_{12}$$

- Algebraically independent entries do not satisfy rational equations

Algebraic Independence

- A non-rigid matrix satisfies a system of rational equations:

$$A = \begin{pmatrix} B & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad A_{22} = A_{21} B^{-1} A_{12}$$

- Algebraically independent entries do not satisfy rational equations
- Hence, a matrix with algebraically independent entries is rigid

Algebraic Independence

- A non-rigid matrix satisfies a system of rational equations:

$$A = \begin{pmatrix} B & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad\qquad A_{22} = A_{21} B^{-1} A_{12}$$

- Algebraically independent entries do not satisfy rational equations
- Hence, a matrix with algebraically independent entries is rigid
- Lindemann-Weierstrass Theorem gives a simple way to construct such matrices

$e^{\sqrt{2}}, e^{\sqrt{3}}, e^{\sqrt{5}}, \ldots$

Lindemann–Weierstrass. Example

$\sqrt{2}$ $x^2 = 2$

$\frac{3}{5} = x$

$x \in \mathbb{C}$ is algebraic if it is a root of a non-zero polynomial with rational coefficients.

Non-algebraic numebrs are called transcendental.

Lindemann–Weierstrass. Example

$x \in \mathbb{C}$ is algebraic if it is a root of a non-zero polynomial with rational coefficients. Non-algebraic numebrs are called transcendental. e, π

Theorem (Lindemann–Weierstrass)

If $x_1, \ldots x_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then $e^{x_1}, \ldots, e^{x_n}$ are algebraically independent over $\mathbb{Q}$.

Lindemann–Weierstrass. Example

$x \in \mathbb{C}$ is algebraic if it is a root of a non-zero polynomial with rational coefficients.
Non-algebraic numebrs are called transcendental.

Theorem (Lindemann–Weierstrass)

If $x_1, \ldots x_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then $e^{x_1}, \ldots, e^{x_n}$ are algebraically independent over $\mathbb{Q}$.

Corollary

e, π are transcendental.

$\boxed{\{1\}}$ is lin ind over $\mathbb{Q}$

$\alpha_1 \cdot 1 \neq 0$

$\alpha_1 \neq 0$

lin ind: $\{\sqrt{2}, \sqrt{3}\}$

not alg ind: $(\sqrt{2})^2 + 1 = (\sqrt{3})^2$

LW $\{e^1\}$ is alg ind.

trans

π is trans

Euler: $e^{\pi i} = -1$

transcendental.

Theorem (Lindemann–Weierstrass)

If $x_1, \ldots x_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then $e^{x_1}, \ldots, e^{x_n}$ are algebraically independent over $\mathbb{Q}$.

Assume π is alg. Then $\pi \cdot i$ is alg. Then can apply LW:

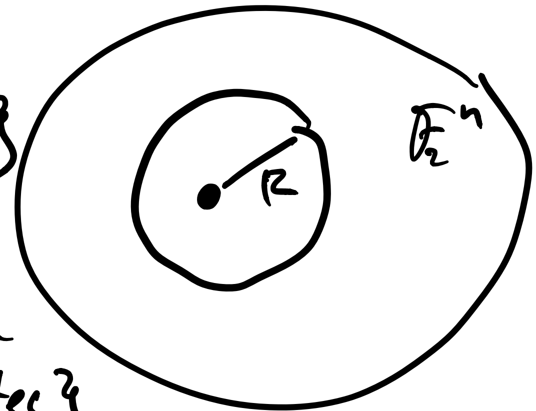
$e^{\pi i}$ is alg ind

" -1 – root $x+1=0$

Contradiction $\square$

$\mathbb{F}_2$ Volume of Hamming Ball

Volume of Hamming Ball of radius R in $\mathbb{F}_2^n$



$$B(x) = \{ y : \mathbb{F}_2^n : \|x-y\|_0 \le R \}$$

$= \{ y : \mathbb{F}_2^n :$ x & y differ in $\le R$ coordinates$\}$

x | 1 0 0 1 1 0 - - - 1 |

Pick $\le R$ coordinates where y differs from x.

$$\binom{n}{\le R} = \sum_{i=0}^{R} \binom{n}{i}$$

$\binom{n}{0} = 1$

$\binom{n}{1} = n$ – differ in 1 pos

. . . $\binom{n}{R}$

$|\mathbb{F}| = q$

$\mathbb{F}_2^n$

$B(x) = \{ y : \mathbb{F}^n : \|x-y\|_0 \leq R \}$

$= \{ y : \mathbb{F}^n :$ x & y differ in $\leq R$ coordinates $\}$

y anything but 0 : q-1 options

y differs from x

$\binom{n}{i} \cdot (q-1)^i$

$\sum_{i=0}^{R} \binom{n}{i} \cdot (q-1)^i$