Matrix Rigidity

Rigidity of Hadamard, Fourier, and Hankel matrices

Sasha Golovnev

November 11, 2020

Rigidity Lower Bounds

We proved (moderate) lower bounds for:

Rigidity Lower Bounds

We proved (moderate) lower bounds for:

- Linear codes $\frac{n^2}{R} \log\left(\frac{n}{R}\right)$

Rigidity Lower Bounds

We proved (moderate) lower bounds for:

- Linear codes Untouched minoR
- All r-minors are full-rank.

Rigidity Lower Bounds

We proved (moderate) lower bounds for:

- Linear codes
- All *r*-minors are full-rank. Includes Vandermonde, Fourier, Cauchy $\underbrace{C_{ij}}= \frac{1}{x_i - y_j}$

Rigidity Lower Bounds

We proved (moderate) lower bounds for:

- Linear codes
- All r-minors are full-rank. Includes Vandermonde, Fourier, Cauchy
- Generalized Hadamard

Rigidity Lower Bounds

We proved (moderate) lower bounds for:

- Linear codes
- All r-minors are full-rank. Includes Vandermonde, Fourier, Cauchy
- Generalized Hadamard
- Random
  Hankel matrices

(Previous) Conjecture

The following matrices were conjectured to be rigid [Lok09]:

- Hadamard + Gen Had mat
- Fourier + Gen F. mat
- Vandermonde
- Cauchy
- Hankel
- Error-correcting codes
- Projective planes

Limitations

no better $\frac{n^2}{k}\log\left(\frac{n}{k}\right)$

- Limits of Untouched Minor method

Limitations

- Limits of Untouched Minor method
- Upper bound on rigidity of super regular matrices

all minors of all sizes are full-rank

Limitations

- Limits of Untouched Minor method
- Upper bound on rigidity of super regular matrices
- Upper bound on rigidity of good codes

Limitations

- Limits of Untouched Minor method
- Upper bound on rigidity of super regular matrices
- Upper bound on rigidity of good codes
- Upper bound for Hadamard

Limitations

- Limits of Untouched Minor method
- Upper bound on rigidity of super regular matrices
- Upper bound on rigidity of good codes
- Upper bound for Hadamard
- Upper bound for $\underline{M(x, y) = f(x + y)}$

The Queen of Limitations

[DL19]: The following matrices are not rigid enough for circuit lower bounds

- A generalization of the Hadamard matrix

The Queen of Limitations

[DL19]: The following matrices are not rigid enough for circuit lower bounds

- A generalization of the Hadamard matrix
- Fourier

The Queen of Limitations

[DL19]: The following matrices are not rigid enough for circuit lower bounds

- A generalization of the Hadamard matrix
- Fourier
- Hankel / Toeplitz

The Queen of Limitations

[DL19]: The following matrices are not rigid enough for circuit lower bounds

- A generalization of the Hadamard matrix
- Fourier
- Hankel
- Circulant

The Queen of Limitations

[DL19]: The following matrices are not rigid enough for circuit lower bounds

- A generalization of the Hadamard matrix
- Fourier
- Hankel
- Circulant
- Group matrices

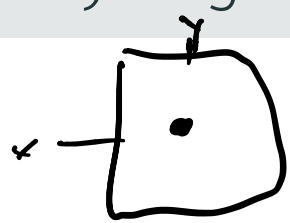
DE17 Limitation

Theorem (DE17)

Let $\mathbb{F}_q$ be a fixed finite field, and let $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ be an arbitrary function. Let $M \in \mathbb{F}_q^{N\times N}$ for $N = q^n$ be the matrix where the (x, y) entry of M equals $f(x+y)$ for every $x, y \in \mathbb{F}_q^n$.

For any $\varepsilon > 0$, there exists $\varepsilon' > 0$ such that $\mathcal{R}_M^{\mathbb{F}_q}(N^{1-\varepsilon'}) \le N^{1+\varepsilon}$ for every large enough n.

$$\boxed{M_{x,y} = \boxed{f(x+y)}}$$



DL19 Limitation

$F(x_1, x_2, x_3) = f(x_3, x_2, x_1) = f(x_2, x_3, x_1) = \cdots$

Theorem (DL19) $\Rightarrow$ non-rigidity of Hadamard!

Let $f\colon \mathbb{Z}_d^n \to \mathbb{C}$ be a symmetric function. Let $M \in \mathbb{C}^{N\times N}$ for $N = d^n$ be the matrix where the (x, y) entry of M equals $f(x + y)$ for every $x, y \in \mathbb{Z}_d^n$.

For any $\varepsilon > 0$, there exists $\varepsilon' > 0$ such that $\mathcal{R}_M^{\mathbb{F}_q}(N^{1-\varepsilon'}) \leq N^{1+\varepsilon}$ for every large enough n.

$H_{x,y} \approx (-1)^{\|x \oplus y\|_0/2}$ | $f(z) = \boxed{(-1)^{\|z\|_0/2}}$

Generalized Hadamard

Definition

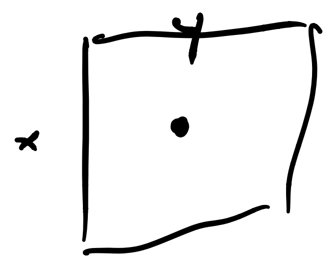
For every d, n, let $N = d^n$, and the generalized Hadamard matrix $H_{d,n} \in \mathbb{C}^{N \times N}$ is defined as

$$(H_{d,n})_{x,y} = \omega^{<x,y>} ,$$

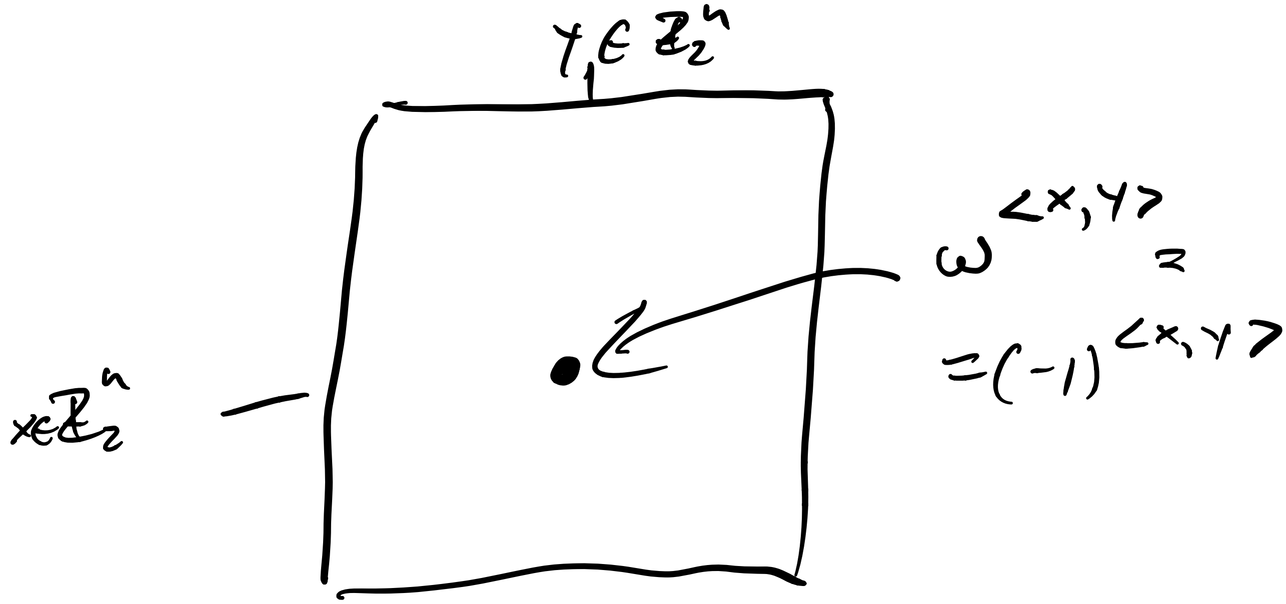
where $\omega = \boxed{2^{\frac{2\pi i}{d}}}$ and $x, y \in \mathbb{Z}_d^n$.

If $d=2 \Rightarrow$ Walsh-Had.

If $n=1 \Rightarrow$ Fourier Matrix

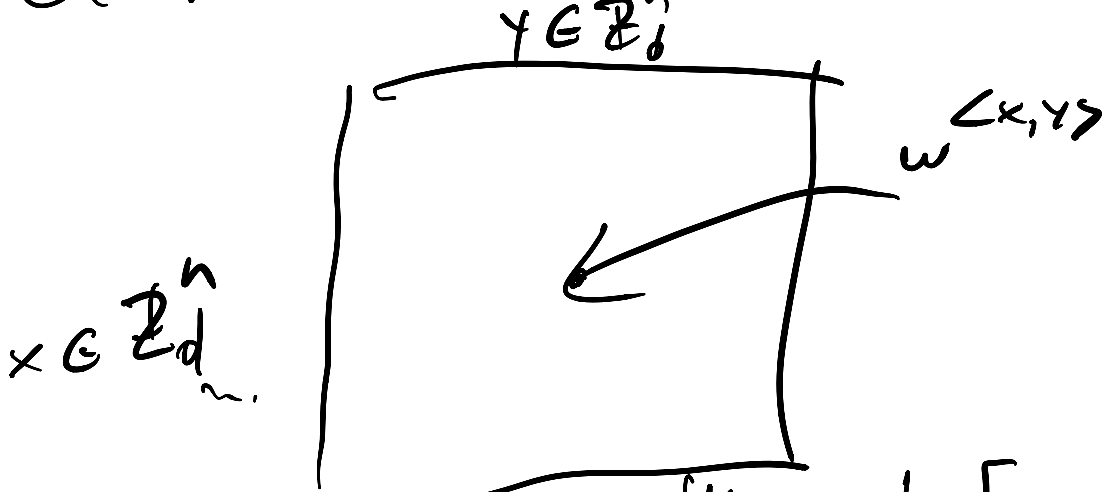


Hadamard



ω - primitive second root of unity $\equiv -1$.

Generalized Hadam:

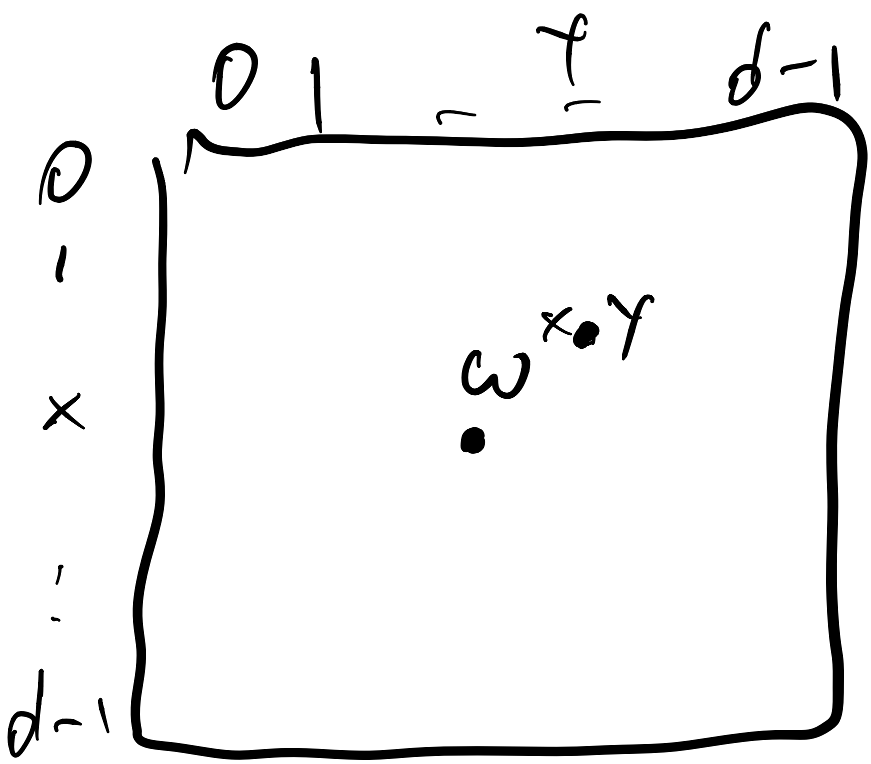


ω - primitive dth root of unity.

If $d=2 \Rightarrow$ Walsh-Had.

If $n=1 \Rightarrow$ Fourier (DFT)

ω – primitive dth root of 1.



Fourier

$$\begin{array}{cc} & y \\ x & \begin{bmatrix} 1 & 1 & 1 & \cdots & & 1 \\ 1 & w & w^2 & w^3 & \cdots & w^{n-1} \\ 1 & w^2 & w^4 & w^6 & \cdots & \\ . & w^3 & w^6 & w^9 & \cdots & \\ & & & & & \\ 1 & & & & & \end{bmatrix} \end{array}$$

Rigidity of Generalized Hadamard

Corollary

For every large enough $n, d \in \mathbb{N}$, $\varepsilon \in (0, 0.1)$, $n \geq \frac{d^2 \log^2 d}{\varepsilon^4}$, *and* $\varepsilon' \geq \frac{\varepsilon^4}{d^2 \log^2 d}$. *The generalized Hadamard matrix* $d, n \in \mathbb{C}^{N \times N}$ *for* $N = d^n$ *has rigidity*

$$\mathcal{R}^{\mathbb{C}}_{H_{d,n}}(N^{1-\varepsilon'}) \leq N^{1+\varepsilon} .$$

Corollary

For every large enough $n, d \in \mathbb{N}$, $\varepsilon \in (0, 0.1)$, $n \geq \frac{d^2 \log^2 d}{\varepsilon^4}$, and $\varepsilon' \geq \frac{\varepsilon^4}{d^2 \log^2 d}$. The generalized Hadamard matrix $d, n \in \mathbb{C}^{N \times N}$ for $N = d^n$ has rigidity

$$\mathcal{R}^{\mathbb{C}}_{H_{d,n}}(N^{1-\varepsilon'}) \leq N^{1+\varepsilon}.$$

Thm

If $f: \mathbb{Z}_d^n \to \mathbb{C}$ and symmetric then

$M_{x,y} = \boxed{f(x+y)}$ is non-rigid

$x, y \in \mathbb{Z}_d^n$.

Proof:

$$H_{x,y} = \omega^{\langle x,y \rangle}$$

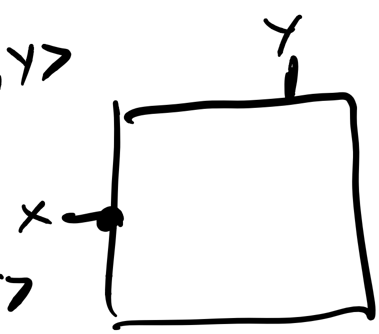
$x, y \in \mathbb{Z}_d^n$

$$\omega = e^{\frac{2\pi i}{d}}$$

$$\alpha = \pm \boxed{e^{\frac{2\pi i}{2d}}}$$

Multiply the xth row $\alpha^{\langle x,x \rangle}$

yth col $\alpha^{\langle y,y \rangle}$



$$H'_{x,y} = H_{x,y} \cdot \alpha^{\langle x,x \rangle} \cdot \alpha^{\langle y,y \rangle}$$

$$= \omega^{\langle x,y \rangle} \cdot \alpha^{\langle x,x \rangle} \cdot \alpha^{\langle y,y \rangle}$$

$$= \alpha^{2\langle x,y \rangle + \langle x,x \rangle + \langle y,y \rangle} = \alpha^{\langle x+y, x+y \rangle} =$$

$$= \alpha^{(x+y)^2}$$

Symmetric fn $f: \boxed{\mathbb{Z}_d^n} \to \mathbb{C}$

s. t. $H'_{x,y} = f(x-y)$,

$$f(\mathbf{z}) = \boxed{\alpha^{\mathbf{z}^2}} = \alpha^{z_1^2 + z_2^2 + \dots z_n^2}$$

We ~~need to show~~:

$$\boxed{\alpha^{(z+d)^2} = \alpha^{z^2}}$$

$$\alpha^{z^2+d^2+2zd} = \alpha^{z^2}$$

$$\alpha^{d^2} \cdot \boxed{\alpha^{2zd}} = 1$$

$$\overset{\shortparallel}{1}$$

$$\alpha^{d^2} = 1.$$

1. If d is even, then $\alpha = + e^{\frac{2\pi i}{d}}$

$$\alpha^{d^2} = 1.$$

2. If d is odd, then $\alpha = - e^{\frac{2\pi i}{d}}$

$$\boxed{\alpha^{d^2}} = 1$$

Fourier Matrix

$\omega^{i \cdot j}$

$$F_N = \begin{array}{cc} & \begin{array}{cccccc} & \phantom{\omega^{N-1}} & \phantom{\omega^{2(N-1)}} & j & & \phantom{\omega^{(N-1)(N-1)}} \end{array} \\ \begin{array}{c} \\ \\ \\ \\ i \\ \\ \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix} \end{array}$$

where $\omega = e^{2\pi i/N}$.

Rigidity of Fourier

Theorem

For every $\varepsilon \in (0, 0.1)$, the Fourier matrix $F \in \mathbb{C}^{N \times N}$ has rigidity

$$\mathcal{R}_F^{\mathbb{C}}\left(\frac{N}{2^{\mathrm{poly}(\varepsilon)(\log N)^{0.35}}}\right) \leq \boxed{N^{1+\varepsilon}}$$

for every large enough N.

Circulant Matrices

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \dots & a_n \\ a_2 & a_3 & a_4 & a_5 & \dots & a_1 \\ a_3 & a_4 & a_5 & a_6 & \dots & a_2 \\ a_4 & a_5 & a_6 & a_7 & \dots & a_3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_1 & a_2 & a_3 & \dots & a_{n-1} \end{pmatrix}$$

Rigidity of Circulant Matrices

Theorem

For every $\varepsilon \in (0, 0.1)$, every circulant matrix $M \in \mathbb{C}^{N \times N}$ has rigidity

$$\mathcal{R}_F^{\mathbb{C}}\left(\frac{N}{2^{\mathrm{poly}(\varepsilon)(\log N)^{0.35}}}\right) \leq N^{1+\varepsilon}$$

for every large enough N.

F diagonalizes <u>every</u> circulant <u>matrix</u>.

$M \in \mathbb{C}^{N \times N}$ circulant matrix

$F \in \mathbb{C}^{N \times N}$ – Fourier matrix.

Then:

$$M = \underline{F}^* \cdot \overset{\text{diagonal}}{D} \cdot \underline{F}$$

We know F is not rigid =>

$$F = \boxed{L} + S$$

$$\boxed{M} = F^* \cdot D \cdot F =$$

$$= (\underline{F} - S)^* \cdot \underline{D} \cdot \underline{F} +$$

$$+ S^* \cdot D \cdot F$$

$$= \underline{(F-S)}^* \cdot D \cdot F +$$

$$S^* \cdot D \cdot \underline{(F-S)} +$$

$$+ S^* D S$$

$$= \boxed{L^* \cdot D \cdot F} + \boxed{S^* \cdot D \cdot L}$$

$$+ S^* D S$$

$\leq$ Rank 2R

– sparse

Hankel Matrices

circulant

$$\begin{array}{cc} & n/2 \\ n/2 & \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \dots & a_n \\ a_2 & a_3 & a_4 & a_5 & \dots & a_1 \\ a_3 & a_4 & a_5 & a_6 & \dots & a_2 \\ a_4 & a_5 & a_6 & a_7 & \dots & a_3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_1 & a_2 & a_3 & \dots & a_{n-1} \end{pmatrix} \end{array}$$

If Hankel was rigid $\Rightarrow$ all circulant matrices containing this Hankel in the corner would be rigid $\Rightarrow$ contradiction

(Previous) Conjecture

The following matrices were conjectured to be rigid [Lok09]:

- ~~Hadamard~~
- ~~Fourier~~
- Vandermonde
- Cauchy
- ~~Hankel~~. none of them
- ~~Error-correcting codes~~ some of them
- ~~Projective planes~~