Fourier and Circulant Matrices are Not Rigid

Allen Liu (MIT)
Joint work with Zeev Dvir (Princeton)

July 18, 2019

Matrix Rigidity

Matrix Rigidity

- A matrix M is rigid if it cannot be written as $A + E$ where A is low-rank and E is sparse

Matrix Rigidity

- A matrix M is rigid if it cannot be written as $A + E$ where A is low-rank and E is sparse

Definition

$\mathrm{R}_M(r)$ is the smallest number s for which

- $\mathrm{M} = \mathrm{A} + \mathrm{E}$
- $\mathrm{rank}(A) \leq r$
- E is s-sparse

Motivation

Motivation

- Matrix rigidity was introduced as a method for proving circuit lower bounds

Motivation

- Matrix rigidity was introduced as a method for proving circuit lower bounds

Theorem [Valiant 77]

Let M be an $N \times N$ matrix over a field $\mathbb{F}$. If for some constant $\epsilon > 0$

$$\mathrm{R}_M^{\mathbb{F}}\left(\frac{N}{\log\log N}\right) \geq \Omega\left(N^{1+\epsilon}\right)$$

then M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

Motivation

- Matrix rigidity was introduced as a method for proving circuit lower bounds

Theorem [Valiant 77]

Let M be an $N \times N$ matrix over a field $\mathbb{F}$. If for some constant $\epsilon > 0$

$$\mathrm{R}_M^{\mathbb{F}}\left(\frac{N}{\log\log N}\right) \geq \Omega\left(N^{1+\epsilon}\right)$$

then M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

- A random matrix has $\mathrm{R}_M^{\mathbb{F}}\left(\frac{N}{\log\log N}\right) \geq \Omega\left(N^{2-\epsilon}\right)$

Motivation

- Matrix rigidity was introduced as a method for proving circuit lower bounds

Theorem [Valiant 77]

Let M be an $N \times N$ matrix over a field $\mathbb{F}$. If for some constant $\epsilon > 0$

$$\mathrm{R}_M^{\mathbb{F}}\left(\frac{N}{\log\log N}\right) \geq \Omega\left(N^{1+\epsilon}\right)$$

then M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

- A random matrix has $\mathrm{R}_M^{\mathbb{F}}\left(\frac{N}{\log\log N}\right) \geq \Omega\left(N^{2-\epsilon}\right)$
- It is a long standing open problem to give an explicit construction of a rigid matrix

Previous Work on Rigid Matrices

Previous Work on Rigid Matrices

Theorem [Shokrollahi et. al., 1997]

For any $N \times N$ matrix M for which all minors are nonsingular

$$\mathsf{R}_M(r) \geq \Omega\left(\frac{N^2}{r} \log \frac{N}{r}\right)$$

Previous Work on Rigid Matrices

Theorem [Shokrollahi et. al., 1997]

For any $N \times N$ matrix M for which all minors are nonsingular

$$\mathrm{R}_M(r) \geq \Omega\left(\frac{N^2}{r}\log\frac{N}{r}\right)$$

Theorem [Goldreich, Tal 2016]

Let $A \in \mathbb{F}_2^{N\times N}$ be a (uniformly) random circulant matrix. Then for every $r \in [\sqrt{N}, \frac{N}{32}]$, with $1 - o(1)$ probability

$$\mathrm{R}_A^{\mathbb{F}_2}(r) = \Omega\left(\frac{N^3}{r^2 \log N}\right)$$

Previous Work on Rigid Matrices

Theorem [Shokrollahi et. al., 1997]

For any $N \times N$ matrix M for which all minors are nonsingular

$$\mathrm{R}_M(r) \geq \Omega\left(\frac{N^2}{r}\log\frac{N}{r}\right)$$

Theorem [Goldreich, Tal 2016]

Let $A \in \mathbb{F}_2^{N\times N}$ be a (uniformly) random circulant matrix. Then for every $r \in [\sqrt{N}, \frac{N}{32}]$, with $1 - o(1)$ probability

$$\mathrm{R}_A^{\mathbb{F}_2}(r) = \Omega\left(\frac{N^3}{r^2 \log N}\right)$$

Neither of these is strong enough for Valiant's method

Special Families of Matrices

Special Families of Matrices

- **(Generalized) Hadamard Matrix** $H_{d,n}$
  $H_{xy} = \omega^{\langle x,y \rangle}$ where $\omega = e^{\frac{2\pi i}{d}}$ and $x, y \in \mathbb{Z}_d^n$

Special Families of Matrices

- **(Generalized) Hadamard Matrix** $H_{d,n}$
  $H_{xy} = \omega^{\langle x,y \rangle}$ where $\omega = e^{\frac{2\pi i}{d}}$ and $x, y \in \mathbb{Z}_d^n$

- **Fourier Matrix** F_N
  $F_{ij} = \zeta^{x \cdot y}$ where $\zeta = e^{\frac{2\pi i}{N}}$ and $x, y \in \mathbb{Z}_N$

Special Families of Matrices

- **(Generalized) Hadamard Matrix** $H_{d,n}$
  $H_{xy} = \omega^{\langle x,y \rangle}$ where $\omega = e^{\frac{2\pi i}{d}}$ and $x, y \in \mathbb{Z}_d^n$
- **Fourier Matrix** F_N
  $F_{ij} = \zeta^{x \cdot y}$ where $\zeta = e^{\frac{2\pi i}{N}}$ and $x, y \in \mathbb{Z}_N$
- **Circulant Matrix** M_N
  $M_{ij} = f(i - j \mod N)$ for $i, j \in \mathbb{Z}_N$

Special Families of Matrices

- **(Generalized) Hadamard Matrix** $H_{d,n}$
  $H_{xy} = \omega^{\langle x,y \rangle}$ where $\omega = e^{\frac{2\pi i}{d}}$ and $x, y \in \mathbb{Z}_d^n$
- **Fourier Matrix** F_N
  $F_{ij} = \zeta^{x \cdot y}$ where $\zeta = e^{\frac{2\pi i}{N}}$ and $x, y \in \mathbb{Z}_N$
- **Circulant Matrix** M_N
  $M_{ij} = f(i - j \mod N)$ for $i, j \in \mathbb{Z}_N$
- **Group Algebra Matrix** M_G
  $M_{ab} = f(ab^{-1})$ for $a, b \in G$

Special Families of Matrices

- **(Generalized) Hadamard Matrix** $H_{d,n}$
  $H_{xy} = \omega^{\langle x,y \rangle}$ where $\omega = e^{\frac{2\pi i}{d}}$ and $x, y \in \mathbb{Z}_d^n$

- **Fourier Matrix** F_N
  $F_{ij} = \zeta^{x \cdot y}$ where $\zeta = e^{\frac{2\pi i}{N}}$ and $x, y \in \mathbb{Z}_N$

- **Circulant Matrix** M_N
  $M_{ij} = f(i - j \mod N)$ for $i, j \in \mathbb{Z}_N$

- **Group Algebra Matrix** M_G
  $M_{ab} = f(ab^{-1})$ for $a, b \in G$

- **Do any of these families contain rigid matrices?**

Special Families of Matrices

- **(Generalized) Hadamard Matrix** $H_{d,n}$
  $H_{xy} = \omega^{\langle x,y \rangle}$ where $\omega = e^{\frac{2\pi i}{d}}$ and $x, y \in \mathbb{Z}_d^n$
- **Fourier Matrix** F_N
  $F_{ij} = \zeta^{x \cdot y}$ where $\zeta = e^{\frac{2\pi i}{N}}$ and $x, y \in \mathbb{Z}_N$
- **Circulant Matrix** M_N
  $M_{ij} = f(i - j \mod N)$ for $i, j \in \mathbb{Z}_N$
- **Group Algebra Matrix** M_G
  $M_{ab} = f(ab^{-1})$ for $a, b \in G$

- **Do any of these families contain rigid matrices?**
- Showing that any of these families contains some rigid matrix would still imply circuit lower bounds

Previous Work on Non-rigid Matrices

Previous Work on Non-rigid Matrices

The Hadamard matrix is not rigid [Alman, Williams 2016]

For every $\epsilon > 0$, there exists $\epsilon' > 0$ such that for all sufficiently large n,

$$\mathrm{R}^{\mathbb{Q}}_{H_{2,n}}\left(2^{n(1-\epsilon')}\right) \leq 2^{n(1+\epsilon)}$$

Previous Work on Non-rigid Matrices

The Hadamard matrix is not rigid [Alman, Williams 2016]

For every $\epsilon > 0$, there exists $\epsilon' > 0$ such that for all sufficiently large n,

$$\mathrm{R}^{\mathbb{Q}}_{H_{2,n}}\left(2^{n(1-\epsilon')}\right) \leq 2^{n(1+\epsilon)}$$

Group algebra matrices for $\mathbb{Z}_q^n$ are not rigid [Dvir, Edelman 2017]

Fix $\epsilon > 0$. There is $\epsilon' > 0$ such that group algebra matrices for $\mathbb{Z}_q^n$ with entries over $\mathbb{F}_q$ satisfy

$$\mathrm{R}^{\mathbb{F}_q}_{M}\left(q^{n(1-\epsilon')}\right) \leq q^{n(1+\epsilon)}$$

for fixed q and n sufficiently large

Previous Work on Non-rigid Matrices

The Hadamard matrix is not rigid [Alman, Williams 2016]

For every $\epsilon > 0$, there exists $\epsilon' > 0$ such that for all sufficiently large n,

$$\mathrm{R}^{\mathbb{Q}}_{H_{2,n}}\left(2^{n(1-\epsilon')}\right) \leq 2^{n(1+\epsilon)}$$

Group algebra matrices for $\mathbb{Z}_q^n$ are not rigid [Dvir, Edelman 2017]

Fix $\epsilon > 0$. There is $\epsilon' > 0$ such that group algebra matrices for $\mathbb{Z}_q^n$ with entries over $\mathbb{F}_q$ satisfy

$$\mathrm{R}^{\mathbb{F}_q}_{M}\left(q^{n(1-\epsilon')}\right) \leq q^{n(1+\epsilon)}$$

for fixed q and n sufficiently large

Neither of these matrices is rigid enough to carry out Valiant's method for proving circuit lower bounds.

Our results

Our results

Theorem (informal)

Generalized Hadamard, Fourier, circulant, and group algebra matrices for *abelian* groups are all not Valiant-rigid.

Our results

Theorem (informal)

Generalized Hadamard, Fourier, circulant, and group algebra matrices for *abelian* groups are all not Valiant-rigid.

Theorem

For all sufficiently large N, if M is an $N \times N$ circulant matrix over $\mathbb{C}$ or some fixed finite field $\mathbb{F}_q$,

$$\mathsf{R}_M\left(\frac{N}{2^{\epsilon^6(\log N)^{0.35}}}\right) \leq N^{1+15\epsilon}$$

Our results

Theorem (informal)

Generalized Hadamard, Fourier, circulant, and group algebra matrices for *abelian* groups are all not Valiant-rigid.

Theorem

For all sufficiently large N, if M is an $N \times N$ circulant matrix over $\mathbb{C}$ or some fixed finite field $\mathbb{F}_q$,

$$\mathsf{R}_M\left(\frac{N}{2^{\epsilon^6(\log N)^{0.35}}}\right) \leq N^{1+15\epsilon}$$

- Previous results [AW16, DE17] only work with matrices whose symmetry group has small characteristic

Our results

Theorem (informal)

Generalized Hadamard, Fourier, circulant, and group algebra matrices for *abelian* groups are all not Valiant-rigid.

Theorem

For all sufficiently large N, if M is an $N \times N$ circulant matrix over $\mathbb{C}$ or some fixed finite field $\mathbb{F}_q$,

$$\mathsf{R}_M\left(\frac{N}{2^{\epsilon^6(\log N)^{0.35}}}\right) \leq N^{1+15\epsilon}$$

- Previous results [AW16, DE17] only work with matrices whose symmetry group has small characteristic
- In this presentation treat everything over $\mathbb{C}$

Proof Overview

Diagonalization Trick

Diagonalization Trick

- Observation: F_N diagonalizes any $N \times N$ circulant matrix M

Diagonalization Trick

- Observation: F_N diagonalizes any $N \times N$ circulant matrix M

$$M = F_N^* D F_N = (F_N - E)^* D F_N + E^* D (F_N - E) + E^* D E$$

Diagonalization Trick

- Observation: F_N diagonalizes any $N \times N$ circulant matrix M

$$M = F_N^* D F_N = \underbrace{(F_N - E)^* D F_N + E^* D (F_N - E)}_{\text{Low Rank}} + \underbrace{E^* D E}_{\text{Sparse}}$$

- F_N not rigid $\rightarrow$ all circulant matrices are not rigid

Diagonalization Trick

- Observation: F_N diagonalizes any $N \times N$ circulant matrix M

$$M = F_N^* D F_N = \underbrace{(F_N - E)^* D F_N + E^* D (F_N - E)}_{\text{Low Rank}} + \underbrace{E^* D E}_{\text{Sparse}}$$

- F_N not rigid $\rightarrow$ all circulant matrices are not rigid
- Similar conclusion holds for Hadamard matrix $H_{d,n}$ and group algebra matrix $M_{\mathbb{Z}_d^n}$

Proof Overview

Proof Overview

1. Show generalized Hadamard matrices $H_{d,n}$ are not rigid for fixed d and $n \gg d^2$

Proof Overview

1. Show generalized Hadamard matrices $H_{d,n}$ are not rigid for fixed d and $n \gg d^2$
2. Show $N \times N$ Fourier matrices are not rigid for some N with a nice prime factorization

Proof Overview

1. Show generalized Hadamard matrices $H_{d,n}$ are not rigid for fixed d and $n \gg d^2$
2. Show $N \times N$ Fourier matrices are not rigid for some N with a nice prime factorization
3. Use diagonalization lemma to deduce nonrigidity of all $N \times N$ circulant matrices for these N

Proof Overview

1. Show generalized Hadamard matrices $H_{d,n}$ are not rigid for fixed d and $n \gg d^2$
2. Show $N \times N$ Fourier matrices are not rigid for some N with a nice prime factorization
3. Use diagonalization lemma to deduce nonrigidity of all $N \times N$ circulant matrices for these N
4. Show $N \times N$ Fourier and circulant matrices are not rigid for all N

Embedding Additive structure in Fourier matrices

Embedding Additive structure in Fourier matrices

- Consider the Fourier matrix F_p for a prime p

Embedding Additive structure in Fourier matrices

- Consider the Fourier matrix F_p for a prime p
- Remove the first row and column (i.e. $x \equiv 0 \mod p$ or $y \equiv 0 \mod p$)

$$M'_{xy} = \zeta^{x \cdot y} \ \forall x, y \in \mathbb{Z}_p^*$$

Embedding Additive structure in Fourier matrices

- Consider the Fourier matrix F_p for a prime p
- Remove the first row and column (i.e. $x \equiv 0 \mod p$ or $y \equiv 0 \mod p$)

$$M'_{xy} = \zeta^{x \cdot y} \ \forall x, y \in \mathbb{Z}_p^*$$

- $(\mathbb{Z}_p^*, \times) \cong (\mathbb{Z}_{p-1}, +)$ so M' is a group algebra matrix for $\mathbb{Z}_{p-1}$ (as an additive group)

Embedding Additive structure in Fourier matrices

- Consider the Fourier matrix F_p for a prime p
- Remove the first row and column (i.e. $x \equiv 0 \mod p$ or $y \equiv 0 \mod p$)

$$M'_{xy} = \zeta^{x \cdot y} \ \forall x, y \in \mathbb{Z}_p^*$$

- $(\mathbb{Z}_p^*, \times) \cong (\mathbb{Z}_{p-1}, +)$ so M' is a group algebra matrix for $\mathbb{Z}_{p-1}$ (as an additive group)

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^4 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^3 & \omega \\ 1 & \omega^4 & \omega^3 & \omega & \omega^2 \\ 1 & \omega^3 & \omega & \omega^2 & \omega^4 \end{bmatrix}$$

Embedding Additive structure in Fourier matrices (cont.)

Embedding Additive structure in Fourier matrices (cont.)

- For an integer $N = p_1 p_2 \dots p_n$, the multiplicative subgroup $\mathbb{Z}_N^*$ has the same structure as the additive group

$$\mathbb{Z}_{p_1-1} \otimes \cdots \otimes \mathbb{Z}_{p_n-1}$$

Embedding Additive structure in Fourier matrices (cont.)

- For an integer $N = p_1 p_2 \dots p_n$, the multiplicative subgroup $\mathbb{Z}_N^*$ has the same structure as the additive group

$$\mathbb{Z}_{p_1-1} \otimes \cdots \otimes \mathbb{Z}_{p_n-1}$$

- Decompose $\mathbb{Z}_{p_i-1}$ into a direct product of groups of prime power order

Embedding Additive structure in Fourier matrices (cont.)

- For an integer $N = p_1 p_2 \dots p_n$, the multiplicative subgroup $\mathbb{Z}_N^*$ has the same structure as the additive group

$$\mathbb{Z}_{p_1-1} \otimes \cdots \otimes \mathbb{Z}_{p_n-1}$$

- Decompose $\mathbb{Z}_{p_i-1}$ into a direct product of groups of prime power order

$$\underbrace{(\mathbb{Z}_{2^5} \otimes \mathbb{Z}_{3^2} \otimes \dots)}_{\mathbb{Z}_{p_1-1}} \otimes \underbrace{(\mathbb{Z}_{2^4} \otimes \mathbb{Z}_{3^2} \otimes \mathbb{Z}_5 \dots)}_{\mathbb{Z}_{p_2-1}} \cdots \otimes \underbrace{(\mathbb{Z}_5 \otimes \dots)}_{\mathbb{Z}_{p_n-1}}$$

Embedding Additive structure in Fourier matrices (cont.)

- For an integer $N = p_1 p_2 \dots p_n$, the multiplicative subgroup $\mathbb{Z}_N^*$ has the same structure as the additive group

$$\mathbb{Z}_{p_1-1} \otimes \cdots \otimes \mathbb{Z}_{p_n-1}$$

- Decompose $\mathbb{Z}_{p_i-1}$ into a direct product of groups of prime power order

$$\underbrace{(\mathbb{Z}_{2^5} \otimes \mathbb{Z}_{3^2} \otimes \dots)}_{\mathbb{Z}_{p_1-1}} \otimes \underbrace{(\mathbb{Z}_{2^4} \otimes \mathbb{Z}_{3^2} \otimes \mathbb{Z}_5 \dots)}_{\mathbb{Z}_{p_2-1}} \cdots \otimes \underbrace{(\mathbb{Z}_5 \otimes \dots)}_{\mathbb{Z}_{p_n-1}}$$

Embedding Additive structure in Fourier matrices (cont.)

- For an integer $N = p_1 p_2 \dots p_n$, the multiplicative subgroup $\mathbb{Z}_N^*$ has the same structure as the additive group

$$\mathbb{Z}_{p_1-1} \otimes \cdots \otimes \mathbb{Z}_{p_n-1}$$

- Decompose $\mathbb{Z}_{p_i-1}$ into a direct product of groups of prime power order

$$\underbrace{(\mathbb{Z}_{2^5} \otimes \mathbb{Z}_{3^2} \otimes \dots)}_{\mathbb{Z}_{p_1-1}} \otimes \underbrace{(\mathbb{Z}_{2^4} \otimes \mathbb{Z}_{3^2} \otimes \mathbb{Z}_5 \dots)}_{\mathbb{Z}_{p_2-1}} \cdots \otimes \underbrace{(\mathbb{Z}_5 \otimes \dots)}_{\mathbb{Z}_{p_n-1}}$$

- Collect like terms

$$\underbrace{(\mathbb{Z}_2 \otimes \cdots \otimes \mathbb{Z}_2)}_{t_2} \otimes \underbrace{(\mathbb{Z}_3 \otimes \cdots \otimes \mathbb{Z}_3)}_{t_3} \otimes \dots$$

Embedding Additive structure in Fourier matrices (cont.)

- For an integer $N = p_1 p_2 \dots p_n$, the multiplicative subgroup $\mathbb{Z}_N^*$ has the same structure as the additive group

$$\mathbb{Z}_{p_1-1} \otimes \cdots \otimes \mathbb{Z}_{p_n-1}$$

- Decompose $\mathbb{Z}_{p_i-1}$ into a direct product of groups of prime power order

$$\underbrace{(\mathbb{Z}_{2^5} \otimes \mathbb{Z}_{3^2} \otimes \dots)}_{\mathbb{Z}_{p_1-1}} \otimes \underbrace{(\mathbb{Z}_{2^4} \otimes \mathbb{Z}_{3^2} \otimes \mathbb{Z}_5 \dots)}_{\mathbb{Z}_{p_2-1}} \cdots \otimes \underbrace{(\mathbb{Z}_5 \otimes \dots)}_{\mathbb{Z}_{p_n-1}}$$

- Collect like terms

$$\underbrace{(\mathbb{Z}_2 \otimes \cdots \otimes \mathbb{Z}_2)}_{t_2} \otimes \underbrace{(\mathbb{Z}_3 \otimes \cdots \otimes \mathbb{Z}_3)}_{t_3} \otimes \dots$$

- If $p_1 - 1, \dots, p_n - 1$ factor smoothly, then $t_2, t_3, \dots$ will be large

Hadamard-type Structure

Hadamard-type Structure

- We have a group algebra matrix M for

$$\underbrace{(\mathbb{Z}_{d_1} \otimes \cdots \otimes \mathbb{Z}_{d_1})}_{t_1} \otimes \underbrace{(\mathbb{Z}_{d_2} \otimes \cdots \otimes \mathbb{Z}_{d_2})}_{t_2} \otimes \cdots$$

Hadamard-type Structure

- We have a group algebra matrix M for

$$\underbrace{(\mathbb{Z}_{d_1} \otimes \cdots \otimes \mathbb{Z}_{d_1})}_{t_1} \otimes \underbrace{(\mathbb{Z}_{d_2} \otimes \cdots \otimes \mathbb{Z}_{d_2})}_{t_2} \otimes \cdots$$

- M is diagonalized by

$$H_{d_1,t_1} \otimes H_{d_2,t_2} \otimes \cdots$$

Hadamard-type Structure

- We have a group algebra matrix M for

$$\underbrace{(\mathbb{Z}_{d_1} \otimes \cdots \otimes \mathbb{Z}_{d_1})}_{t_1} \otimes \underbrace{(\mathbb{Z}_{d_2} \otimes \cdots \otimes \mathbb{Z}_{d_2})}_{t_2} \otimes \cdots$$

- M is diagonalized by

$$H_{d_1,t_1} \otimes H_{d_2,t_2} \otimes \cdots$$

- If $t_1 \gg d_1^2, t_2 \gg d_2^2, \ldots$ we can use the nonrigidity of Hadamard matrices and the diagonalization trick to show M is not rigid

Nonrigidity for some Fourier matrices

Nonrigidity for some Fourier matrices

Definition (informal)

An integer N is well-factorable if

- $N = p_1 \dots p_n$
- $p_1, \dots, p_n$ are distinct primes that are roughly the same size as n
- For all i, the largest prime power divisor of $p_i - 1$ is at most $p_i^{0.3}$

Nonrigidity for some Fourier matrices

Definition (informal)

An integer N is well-factorable if

- $N = p_1 \dots p_n$
- $p_1, \dots, p_n$ are distinct primes that are roughly the same size as n
- For all i, the largest prime power divisor of $p_i - 1$ is at most $p_i^{0.3}$

Fourier matrices of well-factorable size are not rigid

For any fixed $0 < \epsilon < 0.1$ and well-factorable integer N, we have

$$\mathsf{r}_{F_N}\left(\frac{N}{2^{\epsilon^6}(\log N)^{0.36}}\right) \leq N^{7\epsilon}$$

Nonrigidity for some Fourier matrices

Definition (informal)

An integer N is well-factorable if

- $N = p_1 \dots p_n$
- $p_1, \dots, p_n$ are distinct primes that are roughly the same size as n
- For all i, the largest prime power divisor of $p_i - 1$ is at most $p_i^{0.3}$

Fourier matrices of well-factorable size are not rigid

For any fixed $0 < \epsilon < 0.1$ and well-factorable integer N, we have

$$\mathsf{r}_{F_N}\left(\frac{N}{2^{\epsilon^6}(\log N)^{0.36}}\right) \leq N^{7\epsilon}$$

Using the diagonalization trick, we can show that $N \times N$ circulant matrices with N well-factorable are not rigid

Nonrigidity of all Fourier matrices

Nonrigidity of all Fourier matrices

- For a given N, we can embed any $N \times N$ circulant matrix in an $N' \times N'$ circulant matrix for $N' \geq 2N - 1$

Nonrigidity of all Fourier matrices

- For a given N, we can embed any $N \times N$ circulant matrix in an $N' \times N'$ circulant matrix for $N' \geq 2N - 1$

$$\begin{bmatrix} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{bmatrix}$$

Nonrigidity of all Fourier matrices

- For a given N, we can embed any $N \times N$ circulant matrix in an $N' \times N'$ circulant matrix for $N' \geq 2N - 1$

$$\begin{bmatrix} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{bmatrix}$$

- Suffices to show that we can find an N' that is well factorable and not too much larger than N i.e. $2N \leq N' \leq N^{1+o(1)}$

Nonrigidity of all Fourier matrices

- For a given N, we can embed any $N \times N$ circulant matrix in an $N' \times N'$ circulant matrix for $N' \geq 2N - 1$

$$\begin{bmatrix} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{bmatrix}$$

- Suffices to show that we can find an N' that is well factorable and not too much larger than N i.e. $2N \leq N' \leq N^{1+o(1)}$
- Finish using a result from analytic number theory [Baker, Harman 1998]

Conclusion

Directions for Future Work

Directions for Future Work

- Group algebra matrices for nonabelian groups

Directions for Future Work

- Group algebra matrices for nonabelian groups
  - Cannot be completely diagonalized

Directions for Future Work

- Group algebra matrices for nonabelian groups
  - Cannot be completely diagonalized
  - Can be block diagonalized i.e. $M_G = F^* D F$ where D is block-diagonal
  - Sizes of the blocks correspond to the sizes of the irreducible reprsentations of G.

Directions for Future Work

- Group algebra matrices for nonabelian groups
  - Cannot be completely diagonalized
  - Can be block diagonalized i.e. $M_G = F^* D F$ where D is block-diagonal
  - Sizes of the blocks correspond to the sizes of the irreducible reprsentations of G.
  - Natural candidates are groups whose irreducible representations are large

Directions for Future Work

Directions for Future Work

Conjecture

Group algebra matrices for $SL_2(p)$ are rigid

Directions for Future Work

Conjecture

Group algebra matrices for $SL_2(p)$ are rigid

- $SL_2(p)$ consists of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with determinant 1

Directions for Future Work

Conjecture

Group algebra matrices for $SL_2(p)$ are rigid

- $SL_2(p)$ consists of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with determinant 1
- $|SL_2(p)| = p^3 - p$

Directions for Future Work

Conjecture

Group algebra matrices for $SL_2(p)$ are rigid

- $SL_2(p)$ consists of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with determinant 1
- $|SL_2(p)| = p^3 - p$
- All nontrivial irreducible representations have size $O(p)$

Directions for Future Work

Conjecture

Group algebra matrices for $SL_2(p)$ are rigid

- $SL_2(p)$ consists of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with determinant 1
- $|SL_2(p)| = p^3 - p$
- All nontrivial irreducible representations have size $O(p)$
- Want to show that for some function $f : SL_2(p) \to \mathbb{F}$ the $(p^3 - p) \times (p^3 - p)$ matrix given by

$$M_{AB} = f(AB^{-1}) \; \forall A, B \in SL_2(p)$$

is rigid

Thanks!