Rank and Rigidity of Group-Circulant Matrices

Michael Yang
Mentor: Dr. Minh-Tâm Trinh

Lakeside School

October 14-15, 2023
MIT PRIMES Conference

1 Circulant Matrices

2 Group-Circulant Matrices

3 Matrix Rigidity

4 Acknowledgements

Definition (Circulant Matrix)

A (classical) **circulant matrix** is a square matrix where every row is the same as the previous one, but shifted to the left by one unit (with wrap-around).

Definition (Circulant Matrix)

A (classical) **circulant matrix** is a square matrix where every row is the same as the previous one, but shifted to the left by one unit (with wrap-around).

Example

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

General form of a circulant matrix:

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_1 & c_2 & c_3 & \cdots & c_0 \\ c_2 & c_3 & c_4 & \cdots & c_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \end{bmatrix}$$

Each of the c_is appears exactly once in every row and column.

Circulant matrices are useful in many areas.

Circulant matrices are useful in many areas.

- Signal processing

Circulant matrices are useful in many areas.

- Signal processing
- Discrete Fourier Transform

Circulant matrices are useful in many areas.

- Signal processing
- Discrete Fourier Transform

What are their ranks? When are they invertible?

Circulant matrices are useful in many areas.

- Signal processing
- Discrete Fourier Transform

What are their ranks? When are they invertible?

Example

$$\text{rank}\left(\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 1\\ 3 & 1 & 2\end{bmatrix}\right) = 3 \qquad \text{rank}\left(\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\end{bmatrix}\right) = 2$$

Circulant matrices are useful in many areas.

- Signal processing
- Discrete Fourier Transform

What are their ranks? When are they invertible?

Example

$$\operatorname{rank}\left(\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 1\\ 3 & 1 & 2\end{bmatrix}\right) = 3 \qquad \operatorname{rank}\left(\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\end{bmatrix}\right) = 2$$

We'll actually answer these questions for a larger family of matrices: group-circulants.

Circulant matrices are a special example of a larger class of matrices, called **group-circulant matrices.**

Circulant matrices are a special example of a larger class of matrices, called **group-circulant matrices.**

Definition (Group-Circulant Matrix)

Given a finite group G, a ring Λ, and a function $f : G \to \Lambda$, a G-circulant matrix of f is a $|G| \times |G|$ matrix M with rows and columns indexed by the elements of G, such that $M_{x,y} = f(xy)$ for all $x, y \in G$.

Classical circulant matrices are $\mathbb{Z}/n\mathbb{Z}$-circulant matrices.

Classical circulant matrices are $\mathbb{Z}/n\mathbb{Z}$-circulant matrices.

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ \vdots \\ n-1 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & \cdots & n-1 \end{array} \\ \begin{pmatrix} f(0) & f(1) & f(2) & \cdots & f(n-1) \\ f(1) & f(2) & f(3) & \cdots & f(0) \\ f(2) & f(3) & f(4) & \cdots & f(1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f(n-1) & f(0) & f(1) & \cdots & f(n-2) \end{pmatrix} \end{array}$$

Classical circulant matrices are $\mathbb{Z}/n\mathbb{Z}$-circulant matrices.

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ \vdots \\ n-1 \end{array}\begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & \cdots & n-1 \end{array} \\ \begin{pmatrix} f(0) & f(1) & f(2) & \cdots & f(n-1) \\ f(1) & f(2) & f(3) & \cdots & f(0) \\ f(2) & f(3) & f(4) & \cdots & f(1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f(n-1) & f(0) & f(1) & \cdots & f(n-2) \end{pmatrix} \end{array}$$

If we let $f(i) = c_i$ for $i = 0, 1, \ldots, n-1$, we get the general form for a circulant.

Take $G = K_4 := \{e, x, y, xy\}$, where $xy = yx$ and $x^2 = y^2 = e$.

Take $G = K_4 := \{e, x, y, xy\}$, where $xy = yx$ and $x^2 = y^2 = e$.

$$\begin{array}{c} \\ e \\ x \\ y \\ xy \end{array} \begin{array}{c} \begin{array}{cccc} e & x & y & xy \end{array} \\ \begin{pmatrix} f(e) & f(x) & f(y) & f(xy) \\ f(x) & f(e) & f(xy) & f(y) \\ f(y) & f(xy) & f(e) & f(x) \\ f(xy) & f(y) & f(x) & f(e) \end{pmatrix} \end{array}$$

Take $G = K_4 := \{e, x, y, xy\}$, where $xy = yx$ and $x^2 = y^2 = e$.

$$\begin{array}{c} \\ e \\ x \\ y \\ xy \end{array} \begin{array}{c} \begin{array}{cccc} e & x & y & xy \end{array} \\ \begin{pmatrix} f(e) & f(x) & f(y) & f(xy) \\ f(x) & f(e) & f(xy) & f(y) \\ f(y) & f(xy) & f(e) & f(x) \\ f(xy) & f(y) & f(x) & f(e) \end{pmatrix} \end{array}$$

$f : G \to \mathbb{R}$ satisfies $f(e) = 1, f(x) = 2, f(y) = 3, f(xy) = 4$.

Take $G = K_4 := \{e, x, y, xy\}$, where $xy = yx$ and $x^2 = y^2 = e$.

$$\begin{array}{c} \\ e \\ x \\ y \\ xy \end{array} \begin{array}{c} \begin{array}{cccc} e & x & y & xy \end{array} \\ \begin{pmatrix} f(e) & f(x) & f(y) & f(xy) \\ f(x) & f(e) & f(xy) & f(y) \\ f(y) & f(xy) & f(e) & f(x) \\ f(xy) & f(y) & f(x) & f(e) \end{pmatrix} \end{array}$$

$f : G \to \mathbb{R}$ satisfies $f(e) = 1, f(x) = 2, f(y) = 3, f(xy) = 4$.

$$\begin{array}{c} \\ e \\ x \\ y \\ xy \end{array} \begin{array}{c} \begin{array}{cccc} e & x & y & xy \end{array} \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} \end{array}$$

Take $G = K_4 := \{e, x, y, xy\}$, where $xy = yx$ and $x^2 = y^2 = e$.

$$\begin{array}{c} \\ e \\ x \\ y \\ xy \end{array} \begin{array}{c} \begin{array}{cccc} e & x & y & xy \end{array} \\ \begin{pmatrix} f(e) & f(x) & f(y) & f(xy) \\ f(x) & f(e) & f(xy) & f(y) \\ f(y) & f(xy) & f(e) & f(x) \\ f(xy) & f(y) & f(x) & f(e) \end{pmatrix} \end{array}$$

$f : G \to \mathbb{R}$ satisfies $f(e) = 1, f(x) = 2, f(y) = 3, f(xy) = 4$.

$$\text{rank}\left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}\right) = 3$$

What are the ranks of group-circulants?

Theorem (Group-Circulant Rank)

For any group G, good field Λ, and function $f : G \to \Lambda$, express f in the form

$$f(x) = \sum_{\rho} \left(\sum_{1 \leq i,j \leq \deg \rho} c_{\rho,i,j} \rho_{i,j}(x) \right)$$

where ρ runs over irreducible representations of G, the functions $\rho_{i,j}$ are the matrix coefficients of ρ, and $c_{\rho,i,j} \in \Lambda$. Then, the rank of the G-circulant corresponding to f equals

$$\sum_{\rho} \left[(\deg \rho) \; rank \left(\begin{bmatrix} c_{\rho,1,1} & c_{\rho,1,2} & \cdots & c_{\rho,1,N} \\ c_{\rho,2,1} & c_{\rho,2,2} & \cdots & c_{\rho,2,N} \\ \vdots & \vdots & \ddots & \vdots \\ c_{\rho,N,1} & c_{\rho,N,2} & \cdots & c_{\rho,N,N} \end{bmatrix} \right) \right].$$

How do we read the theorem?

How do we read the theorem?

- For any group G and good field Λ, the matrix coefficients form a basis for the vector space of functions from G to Λ.

How do we read the theorem?

- For any group G and good field Λ, the matrix coefficients form a basis for the vector space of functions from G to Λ.
- This basis is well-studied and nice to work with.

How do we read the theorem?

- For any group G and good field Λ, the matrix coefficients form a basis for the vector space of functions from G to Λ.
- This basis is well-studied and nice to work with.
- The theorem notes that when we write f as a sum of the matrix coefficients, the rank of the G-circulant can be deduced from the coefficients in that sum.

How do we read the theorem?

- For any group G and good field Λ, the matrix coefficients form a basis for the vector space of functions from G to Λ.
- This basis is well-studied and nice to work with.
- The theorem notes that when we write f as a sum of the matrix coefficients, the rank of the G-circulant can be deduced from the coefficients in that sum.

While this theorem was known to Diaconis, we gave a new, more elementary proof.

When we take $G = \mathbb{Z}/n\mathbb{Z}$ in the theorem, we get the following result on the rank of classical circulant matrices:

When we take $G = \mathbb{Z}/n\mathbb{Z}$ in the theorem, we get the following result on the rank of classical circulant matrices:

Corollary (Circulant Rank)

Let $\omega = e^{2\pi i/n}$. The rank of the $n \times n$ circulant matrix with first row $[c_0, c_1, \ldots, c_{n-1}]$ is the number of nonzero entries in the vector

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-(2n-2)} & \cdots & \omega^{-(n-1)^2} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}.$$

When we take $G = \mathbb{Z}/n\mathbb{Z}$ in the theorem, we get the following result on the rank of classical circulant matrices:

Corollary (Circulant Rank)

Let $\omega = e^{2\pi i/n}$. The rank of the $n \times n$ circulant matrix with first row $[c_0, c_1, \dots, c_{n-1}]$ is the number of nonzero entries in the vector

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-(2n-2)} & \cdots & \omega^{-(n-1)^2} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}.$$

Vanishing sums of roots of unity $\implies$ singular circulants

Definition (Matrix Rigidity)

Fix a square matrix M. The **rank-r rigidity** of M, denoted $\mathcal{R}_M(r)$, is the minimum number of entries one needs to change in M to decrease its rank to at most r.

Definition (Matrix Rigidity)

Fix a square matrix M. The **rank-r rigidity** of M, denoted $\mathcal{R}_M(r)$, is the minimum number of entries one needs to change in M to decrease its rank to at most r.

Example

For the $n \times n$ identity matrix I_n,

$$\mathcal{R}_{I_n}(r) = n - r.$$

We can change $n - r$ of the diagonal 1s to 0s to make the rank r.

Example

Let

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then, $\mathcal{R}_{I_3}(1) = 2$.

Example

Let

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then, $\mathcal{R}_{I_3}(1) = 2$.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & {\color{red}1} & 0 \\ 0 & 0 & {\color{red}1} \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & {\color{cyan}0} & 0 \\ 0 & 0 & {\color{cyan}0} \end{bmatrix}$$

Example

Let

$$M = \begin{bmatrix} 2 & 3 & 5 \\ 1 & 0 & 1 \\ 4 & 6 & 7 \end{bmatrix}.$$

Then, $\mathcal{R}_M(1) = 3$.

Example

Let

$$M = \begin{bmatrix} 2 & 3 & 5 \\ 1 & 0 & 1 \\ 4 & 6 & 7 \end{bmatrix}.$$

Then, $\mathcal{R}_M(1) = 3$.

$$\begin{bmatrix} 2 & 3 & 5 \\ 1 & 0 & 1 \\ 4 & 6 & 7 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 3 & 5 \\ 1 & 3/2 & 5/2 \\ 4 & 6 & 10 \end{bmatrix}$$

Example

Let

$$M = \begin{bmatrix} 2 & 3 & 5 \\ 1 & 0 & 1 \\ 4 & 6 & 7 \end{bmatrix}.$$

Then, $\mathcal{R}_M(1) = 3$.

$$\begin{bmatrix} 2 & 3 & 5 \\ 1 & 0 & 1 \\ 4 & 6 & 7 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 3 & 5 \\ 1 & 3/2 & 5/2 \\ 4 & 6 & 10 \end{bmatrix}$$

Changing any two entries will leave a 2×2 rectangle of full rank unchanged.

Theorem (Valiant 1977)

If M is a Valiant-rigid $N \times N$ matrix, then the linear map corresponding to M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

Theorem (Valiant 1977)

If M is a Valiant-rigid $N \times N$ matrix, then the linear map corresponding to M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

Valiant-rigid matrices are highly rigid.

Goal: find an **explicit** Valiant-rigid matrix.

Theorem (Valiant 1977)

If M is a Valiant-rigid $N \times N$ matrix, then the linear map corresponding to M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

Valiant-rigid matrices are highly rigid.

Goal: find an **explicit** Valiant-rigid matrix.

Not rigid:

Theorem (Valiant 1977)

If M is a Valiant-rigid $N \times N$ matrix, then the linear map corresponding to M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

Valiant-rigid matrices are highly rigid.

Goal: find an **explicit** Valiant-rigid matrix.

Not rigid:

- Super-regular matrices

Theorem (Valiant 1977)

If M is a Valiant-rigid $N \times N$ matrix, then the linear map corresponding to M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

Valiant-rigid matrices are highly rigid.

Goal: find an **explicit** Valiant-rigid matrix.

Not rigid:

- Super-regular matrices
- Walsh-Hadamard transform

Theorem (Valiant 1977)

If M is a Valiant-rigid $N \times N$ matrix, then the linear map corresponding to M cannot be computed by circuits of size $O(N)$ and depth $O(\log N)$.

Valiant-rigid matrices are highly rigid.

Goal: find an **explicit** Valiant-rigid matrix.

Not rigid:

- Super-regular matrices
- Walsh-Hadamard transform
- G-circulants for abelian G

Theorem (Dvir–Liu 2019)

Let G be an abelian group. The family of G-circulant matrices is not Valiant-rigid over any field of characteristic relatively prime to $|G|$.

Theorem (Dvir–Liu 2019)

Let G be an abelian group. The family of G-circulant matrices is not Valiant-rigid over any field of characteristic relatively prime to $|G|$.

Theorem (Trinh–Y. 2023)

For groups G with relatively large abelian normal subgroups, the family of G-circulant matrices is not Valiant-rigid.

Acknowledgements

Thank you to my mentor, Dr. Minh-Tâm Trinh, for proposing the project and resourcefully and patiently guiding me to the discovery of these results. Thank you also to the PRIMES-USA Program for the incredible opportunity to conduct this research. Lastly, thank you to my parents; without your unwavering support, none of this would have been possible.

References

[Val77] Leslie G Valiant. "Graph-theoretic arguments in low-level complexity". In: *International Symposium on Mathematical Foundations of Computer Science*. Springer. 1977, pp. 162–176.

[Dia90] Persi Diaconis. "Patterned matrices". In: *Proc. of Symposia in Applied Mathematics*. Vol. 40. 1990, pp. 37–58.

[DE17] Zeev Dvir and Benjamin Edelman. "Matrix rigidity and the Croot-Lev-Pach lemma". In: *arXiv preprint arXiv:1708.01646* (2017).

[DL19] Zeev Dvir and Allen Liu. "Fourier and circulant matrices are not rigid". In: *arXiv preprint arXiv:1902.07334* (2019).