Counting LU Matrices with Fixed Eigenvalues

PRIMES conference 2021

Andrew Gu[1]
Mentored by Dr. Jonathan Wang[2]

[1]Tesoro High school

[2]Perimeter Institute

October 16 - 17, 2021

The Field $\mathbb{F}_q$

Definition

A **field** is a set that satisfies certain basic rules:

The Field $\mathbb{F}_q$

Definition

A **field** is a set that satisfies certain basic rules:

- multiplication

The Field $\mathbb{F}_q$

Definition

A **field** is a set that satisfies certain basic rules:

- multiplication
- addition

The Field $\mathbb{F}_q$

Definition

A **field** is a set that satisfies certain basic rules:

- multiplication
- addition
- subtraction

The Field $\mathbb{F}_q$

Definition

A **field** is a set that satisfies certain basic rules:

- multiplication
- addition
- subtraction
- division

The Field $\mathbb{F}_q$

Definition

A **field** is a set that satisfies certain basic rules:

- multiplication
- addition
- subtraction
- division

Example

Some common examples are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

The Field $\mathbb{F}_q$

Definition ($\mathbb{F}_q$)

$\mathbb{F}_q$ is a field with a finite number of elements, q to be exact.

The Field $\mathbb{F}_q$

Definition ($\mathbb{F}_q$)

$\mathbb{F}_q$ is a field with a finite number of elements, q to be exact.

When q is any prime p, $\mathbb{F}_q$ is like working modulo p. For any other q, it is slightly more complicated.

The Group $GL_n(\mathbb{F}_q)$

Definition

A **group** is a set equipped with an operation.
Satisfies the *group axioms*:

The Group $GL_n(\mathbb{F}_q)$

Definition

A **group** is a set equipped with an operation.
Satisfies the *group axioms*:

- closure

The Group $GL_n(\mathbb{F}_q)$

Definition

A **group** is a set equipped with an operation.
Satisfies the *group axioms*:

- closure
- associativity

The Group $GL_n(\mathbb{F}_q)$

Definition

A **group** is a set equipped with an operation.
Satisfies the *group axioms*:

- closure
- associativity
- identity

The Group $GL_n(\mathbb{F}_q)$

Definition

A **group** is a set equipped with an operation.
Satisfies the *group axioms*:

- closure
- associativity
- identity
- inverse

The Group $GL_n(\mathbb{F}_q)$

Definition

A **group** is a set equipped with an operation.
Satisfies the *group axioms*:

- closure
- associativity
- identity
- inverse

Example

A common example is $\mathbb{Z}$ under addition.

The Group $GL_n(\mathbb{F}_q)$

Definition ($GL_n(\mathbb{F}_q)$)

$GL_n(\mathbb{F}_q)$ is the set of $n \times n$ invertible matrices whose entries are in $\mathbb{F}_q$.

The Group $GL_n(\mathbb{F}_q)$

Definition ($GL_n(\mathbb{F}_q)$)

$GL_n(\mathbb{F}_q)$ is the set of $n \times n$ invertible matrices whose entries are in $\mathbb{F}_q$.

- Group under matrix multiplication

The Group $GL_n(\mathbb{F}_q)$

Definition ($GL_n(\mathbb{F}_q)$)

$GL_n(\mathbb{F}_q)$ is the set of $n \times n$ invertible matrices whose entries are in $\mathbb{F}_q$.

- Group under matrix multiplication
- Main group we will work with

Eigenvalues

Definition

An **eigenvalue** for a matrix $g \in GL_n(\mathbb{F}_q)$ is any scalar λ for which there exists a vector $v \in \mathbb{F}_q^n$ such that $gv = \lambda v$. v is called an *eigenvector*.

Eigenvalues

Definition

An **eigenvalue** for a matrix $g \in GL_n(\mathbb{F}_q)$ is any scalar λ for which there exists a vector $v \in \mathbb{F}_q^n$ such that $gv = \lambda v$. v is called an *eigenvector*.

Example

The eigenvalues of $\begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}$ are 2 and 4 with eigenvectors $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$, respectively.

LU Decomposition

Definition

A matrix admits an **LU decomposition** if it is equal to:

Lower Triangular Matrix $\times$ Upper Triangular Matrix.

LU Decomposition

Definition

A matrix admits an **LU decomposition** if it is equal to:

Lower Triangular Matrix $\times$ Upper Triangular Matrix.

Example

$$\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 14 \end{pmatrix}$$

LU Decomposition Cont.

Matrices with LU Decomposition are called *LU Matrices*.

LU Decomposition Cont.

Matrices with LU Decomposition are called *LU Matrices*.

Theorem

If the Lower Triangular matrix is restricted to have 1's, the LU Decomposition is unique.

LU Decomposition Cont.

Matrices with LU Decomposition are called *LU Matrices*.

Theorem

If the Lower Triangular matrix is restricted to have 1's, the LU Decomposition is unique.

This is a well known fact.

Motivating Question

We would like to investigate the number of matrices with the following properties:

Motivating Question

We would like to investigate the number of matrices with the following properties:

- Admits an LU decomposition

Motivating Question

We would like to investigate the number of matrices with the following properties:

- Admits an LU decomposition
- The eigenvalues form a set $s \subset \mathbb{F}_q$

Motivating Question

We would like to investigate the number of matrices with the following properties:

- Admits an LU decomposition
- The eigenvalues form a set $s \subset \mathbb{F}_q$
- These eigenvalues are distinct i.e. $|s| = n$

Motivating Question

We would like to investigate the number of matrices with the following properties:

- Admits an LU decomposition
- The eigenvalues form a set $s \subset \mathbb{F}_q$
- These eigenvalues are distinct i.e. $|s| = n$

We call this set of matrices X_s.

Example

Example

Case $n = 2$: LU matrices have the form

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} ac & d \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} ac & d \\ abc & bd + c^{-1} \end{pmatrix}.$$

Example

Example

Case $n = 2$: LU matrices have the form

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} ac & d \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} ac & d \\ abc & bd + c^{-1} \end{pmatrix}.$$

The eigenvalues are roots of the polynomial $t^2 - (ac + c^{-1} + bd)t + a$.

Example

Example

Case $n = 2$: LU matrices have the form

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} ac & d \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} ac & d \\ abc & bd + c^{-1} \end{pmatrix}.$$

The eigenvalues are roots of the polynomial
$t^2 - (ac + c^{-1} + bd)t + a$.
If $s = \{ae, e^{-1}\}$, we want roots to be ae and e^{-1}. Casework gives us $q^2 + 1$ solutions.

Another Example

Example

For $n = 3$, the equations are:

Another Example

Example

For $n = 3$, the equations are:

- $d + e + f + ax + by + cz = r + s + t$

Another Example

Example

For $n = 3$, the equations are:

- $d + e + f + ax + by + cz = r + s + t$
- $de + ef + df + czd + axf + bye + acxz - acey - bxz = rs + st + ts$

Another Example

Example

For $n = 3$, the equations are:

- $d + e + f + ax + by + cz = r + s + t$
- $de + ef + df + czd + axf + bye + acxz - acey - bxz = rs + st + ts$
- $def = rst$

Another Example

Example

For $n = 3$, the equations are:

- $d + e + f + ax + by + cz = r + s + t$
- $de + ef + df + czd + axf + bye + acxz - acey - bxz = rs + st + ts$
- $def = rst$

if r, s, t are the eigenvalues.

Another Example

Example

For $n = 3$, the equations are:

- $d + e + f + ax + by + cz = r + s + t$
- $de + ef + df + czd + axf + bye + acxz - acey - bxz = rs + st + ts$
- $def = rst$

if r, s, t are the eigenvalues. Very difficult.

Another Example

Example

For $n = 3$, the equations are:

- $d + e + f + ax + by + cz = r + s + t$
- $de + ef + df + czd + axf + bye + acxz - acey - bxz = rs + st + ts$
- $def = rst$

if r, s, t are the eigenvalues. Very difficult.

A *computer program* seems more appropriate now. That gives $q^6 + 4q^3 + 1$.

Extrapolation

Let's see if we can find a pattern with these expressions:

Extrapolation

Let's see if we can find a pattern with these expressions:

- $n = 1 : 1$

Extrapolation

Let's see if we can find a pattern with these expressions:

- $n = 1 : 1$
- $n = 2 : q^2 + 1$

Extrapolation

Let's see if we can find a pattern with these expressions:

- $n = 1 : 1$
- $n = 2 : q^2 + 1$
- $n = 3 : q^6 + 4q^3 + 1$

Extrapolation

Let's see if we can find a pattern with these expressions:

- $n = 1 : 1$
- $n = 2 : q^2 + 1$
- $n = 3 : q^6 + 4q^3 + 1$

Is there a pattern?

Extrapolation

Let's see if we can find a pattern with these expressions:

- $n = 1 : 1$
- $n = 2 : q^2 + 1$
- $n = 3 : q^6 + 4q^3 + 1$

Is there a pattern? *Yes, but the formula is quite complicated.*

The Formula

Theorem (G)

For all n-element subsets s of $\mathbb{F}_q$, *we have*

$$|X_s| = \sum_{\lambda \in Y_n} q^{c(1)+c(\lambda)} D_\lambda^2.$$

The Formula

Theorem (G)

For all n-element subsets s of $\mathbb{F}_q$*, we have*

$$|X_s| = \sum_{\lambda \in Y_n} q^{c(1)+c(\lambda)} D_\lambda^2.$$

We will not talk about the proof because it is rather lengthy and complex.

Partitions

Definition

A **partition** of a positive integer n is a way to write it as a sum of unordered positive integers. We can write a partition λ as $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1$.

Partitions

Definition

A **partition** of a positive integer n is a way to write it as a sum of unordered positive integers. We can write a partition λ as $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1$.

One common way to represent a partition is using a *Young diagram*. Y_n is then the set of Young diagrams of size n.

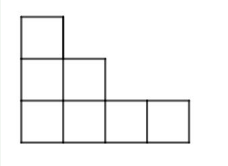
Partitions

Definition

A **partition** of a positive integer n is a way to write it as a sum of unordered positive integers. We can write a partition λ as $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1$.

One common way to represent a partition is using a *Young diagram*. Y_n is then the set of Young diagrams of size n.

Example



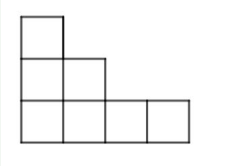
Partitions

Definition

A **partition** of a positive integer n is a way to write it as a sum of unordered positive integers. We can write a partition λ as $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1$.

One common way to represent a partition is using a *Young diagram*. Y_n is then the set of Young diagrams of size n.

Example



λ is $(4, 2, 1)$ in this example.

The Hook Length Formula

Definition

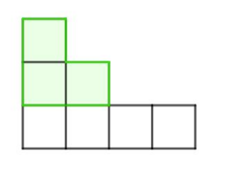
For (i, j) the square in row i, column j, we let $h(i, j)$ denote the number of squares (i', j') in the Young diagram λ such that $i' \geq i, j' = j$ or $i' = i, j' \geq j$. Then, the **Hook Length Formula** says $D_\lambda = \dfrac{n!}{\prod_{i,j} h(i, j)}$.

The Hook Length Formula

Definition

For (i,j) the square in row i, column j, we let $h(i,j)$ denote the number of squares (i',j') in the Young diagram λ such that $i' \geq i, j' = j$ or $i' = i, j' \geq j$. Then, the **Hook Length Formula** says $D_\lambda = \frac{n!}{\prod_{i,j} h(i,j)}$.

Example

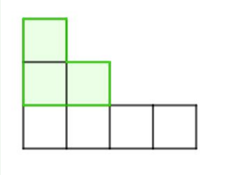


The Hook Length Formula

Definition

For (i,j) the square in row i, column j, we let $h(i,j)$ denote the number of squares (i',j') in the Young diagram λ such that $i' \geq i, j' = j$ or $i' = i, j' \geq j$. Then, the **Hook Length Formula** says $D_\lambda = \frac{n!}{\prod_{i,j} h(i,j)}$.

Example



D_λ is $\frac{7!}{6 \cdot 4 \cdot 2 \cdot 1 \cdot 3 \cdot 1 \cdot 1} = 35$ in this example.

Content

Definition

The **content** of a partition $c(\lambda)$ is defined as $\sum_{i=1}^{k} \sum_{j=1}^{\lambda_i} j - i$.

Content

Definition

The **content** of a partition $c(\lambda)$ is defined as $\sum_{i=1}^{k}\sum_{j=1}^{\lambda_i} j - i$.

Note: similar to subtracting the sum of y-coordinates from the sum of x-coordinates.

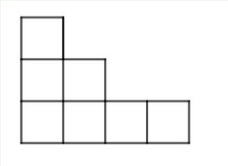
Content

Definition

The **content** of a partition $c(\lambda)$ is defined as $\sum_{i=1}^{k}\sum_{j=1}^{\lambda_i} j - i$.

Note: similar to subtracting the sum of y-coordinates from the sum of x-coordinates.

Example



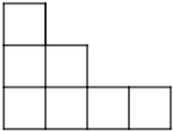
Content

Definition

The **content** of a partition $c(\lambda)$ is defined as $\sum_{i=1}^{k}\sum_{j=1}^{\lambda_i} j - i$.

Note: similar to subtracting the sum of y-coordinates from the sum of x-coordinates.

Example



The content is 3 in this example.

Using The Formula

Theorem (G)

For all n-element subsets s of $\mathbb{F}_q$, we have

$$|X_s| = \sum_{\lambda \in Y_n} q^{c(1)+c(\lambda)} D_\lambda^2.$$

Using The Formula

Theorem (G)

For all n-element subsets s of $\mathbb{F}_q$*, we have*

$$|X_s| = \sum_{\lambda \in Y_n} q^{c(1)+c(\lambda)} D_\lambda^2.$$

After some work, we find for $n = 4$:

Using The Formula

Theorem (G)

For all n-element subsets s of $\mathbb{F}_q$*, we have*

$$|X_s| = \sum_{\lambda \in Y_n} q^{c(1)+c(\lambda)} D_\lambda^2.$$

After some work, we find for $n = 4$:

$$q^{12} + 3q^{10} + 2q^6 + 3q^2 + 1.$$

Acknowledgements

I would like to thank

- Dr. Jonathan Wang, for mentoring me.
- PRIMES USA, for the research opportunity.
- Professor Bezrukavnikov, for suggesting my project.
- Dr. Minh-Tam Trinh, for sharing ideas.
- My parents, for their support.