The Distribution of Distinct Non-Zero Ranks in 2-d Subspaces of $M_n(\mathbb{F}_q)$

Cian O'Brien Supervisor: Kevin Jennings

Final Year Project

November 18th, 2016

Introduction

The aim of this project was to examine the number of different ranks that can occur in 2-d subspaces of $M_n(\mathbb{F}_q)$, and the distributions of the number of ranks that arise for different fixed values of n and q.

Some Standard Definitions from Linear Algebra

- A set of vectors is *linearly independent* if no vector in the set can be written as a linear combination of the other vectors in the set.

Some Standard Definitions from Linear Algebra

- A set of vectors is *linearly independent* if no vector in the set can be written as a linear combination of the other vectors in the set.
- The *rank* of a matrix is the number of linearly independent rows or columns in that matrix.

Examples

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Examples

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$U = \{\lambda_1 A + \lambda_2 B\}$$

Examples

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$U = \{\lambda_1 A + \lambda_2 B\}$$

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

Examples

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Examples

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Restrictions

The number of distinct 2-d subspaces in $M_n(\mathbb{F}_q)$ is

$$\frac{(q^{n^2}-1)\times(q^{n^2}-q)}{(q^2-1)\times(q^2-q)}.$$

Restrictions

The number of distinct 2-d subspaces in $M_n(\mathbb{F}_q)$ is

$$\frac{(q^{n^2}-1)\times(q^{n^2}-q)}{(q^2-1)\times(q^2-q)}.$$

This formula grows very quickly. For example, if $n=4$ and $q=4$, the formula returns a value of 1.025×10^{17}.

Restrictions

The number of distinct 2-d subspaces in $M_n(\mathbb{F}_q)$ is

$$\frac{(q^{n^2}-1)\times(q^{n^2}-q)}{(q^2-1)\times(q^2-q)}.$$

This formula grows very quickly. For example, if $n=4$ and $q=4$, the formula returns a value of 1.025×10^{17}.

The analogous counting formula for diagonal matrices in $M_n(\mathbb{F}_q)$ is

$$\frac{(q^{n}-1)\times(q^{n}-q)}{(q^2-1)\times(q^2-q)}.$$

Finite Fields

- A field is a set containing at least two elements: an additive identity (0), and a multiplicative identity (1), where all elements have an additive inverse and all non-zero elements have a multiplicative inverse, and where $+$ and $\times$ are compatible. A finite field $\mathbb{F}_n$, $n \in \mathbb{N}$, is a field with n elements.

Finite Fields

- A field is a set containing at least two elements: an additive identity (0), and a multiplicative identity (1), where all elements have an additive inverse and all non-zero elements have a multiplicative inverse, and where $+$ and $\times$ are compatible. A finite field $\mathbb{F}_n$, $n \in \mathbb{N}$, is a field with n elements.
- $\mathbb{Z}_p = \{0, 1, ..., p-1\}$ is the field $\mathbb{F}_p$, with addition and multiplication mod p.

Finite Fields

- A field is a set containing at least two elements: an additive identity (0), and a multiplicative identity (1), where all elements have an additive inverse and all non-zero elements have a multiplicative inverse, and where $+$ and $\times$ are compatible. A finite field $\mathbb{F}_n$, $n \in \mathbb{N}$, is a field with n elements.
- $\mathbb{Z}_p = \{0, 1, ..., p-1\}$ is the field $\mathbb{F}_p$, with addition and multiplication mod p.
- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is not a field: $2 \times 2 = 4 \equiv 0 \mod 4$.

Finite Fields

- A field is a set containing at least two elements: an additive identity (0), and a multiplicative identity (1), where all elements have an additive inverse and all non-zero elements have a multiplicative inverse, and where $+$ and $\times$ are compatible. A finite field $\mathbb{F}_n$, $n \in \mathbb{N}$, is a field with n elements.
- $\mathbb{Z}_p = \{0, 1, ..., p-1\}$ is the field $\mathbb{F}_p$, with addition and multiplication mod p.
- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is not a field: $2 \times 2 = 4 \equiv 0 \mod 4$.
- A field $\mathbb{F}_4$ with four elements exists.

Finite Fields

- A field is a set containing at least two elements: an additive identity (0), and a multiplicative identity (1), where all elements have an additive inverse and all non-zero elements have a multiplicative inverse, and where $+$ and $\times$ are compatible. A finite field $\mathbb{F}_n$, $n \in \mathbb{N}$, is a field with n elements.
- $\mathbb{Z}_p = \{0, 1, ..., p-1\}$ is the field $\mathbb{F}_p$, with addition and multiplication mod p.
- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is not a field: $2 \times 2 = 4 \equiv 0 \mod 4$.
- A field $\mathbb{F}_4$ with four elements exists.
- $\mathbb{F}_4$ is a 2-dimensional vector space over $\mathbb{F}_2$, $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$.

Computer Program

I wrote a computer program to exhaustively analyse all $n \times n$ diagonal matrices, for a given n, initially over fields of prime order.

The program generates all 2-d subspaces of $M_n(\mathbb{F}_q)$, for a given value of q and n. If a subspace is distinct from all subspaces previously generated, it calculates the number of distinct ranks present in the subspace. The program then outputs the distribution of the number of ranks for the given values of q and n.

Computer Results

Number of 2-d subspaces in $M_n(\mathbb{F}_q)$ with t distinct ranks:

n, q	t=1	t=2	t=3	t=4	Total no. of 2-d subspaces
2, 2	0	1	0	0	1
2, 3	0	1	0	0	1
3, 2	1	3	3	0	7
3, 3	0	7	6	0	13
3, 5	0	19	12	0	31
3, 7	0	39	18	0	57
4, 2	4	15	16	0	35
4, 3	8	34	88	0	130
4, 5	0	310	496	0	806
5, 2	10	80	65	0	155
5, 3	40	270	900	0	1210
6, 2	35	325	291	0	651
6, 3	120	3955	5016	1920	11011
7, 2	140	1232	1295	0	2667
8, 2	476	4879	5440	0	10795

Fields of Prime Power Order

We will now build $\mathbb{F}_4$ as an extension field over $\mathbb{F}_2$. $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, which we can see since $f(x)$ has no roots in $\mathbb{F}_2$:

Fields of Prime Power Order

We will now build $\mathbb{F}_4$ as an extension field over $\mathbb{F}_2$. $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, which we can see since $f(x)$ has no roots in $\mathbb{F}_2$:

$$f(0) \equiv 1 \mod 2$$

$$f(1) \equiv 1 \mod 2$$

Fields of Prime Power Order

We will now build $\mathbb{F}_4$ as an extension field over $\mathbb{F}_2$. $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, which we can see since $f(x)$ has no roots in $\mathbb{F}_2$:

$$f(0) \equiv 1 \mod 2$$

$$f(1) \equiv 1 \mod 2$$

Let α be a root of this polynomial. Note that $\alpha \notin \mathbb{F}_2$.

Fields of Prime Power Order

We will now build $\mathbb{F}_4$ as an extension field over $\mathbb{F}_2$. $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, which we can see since $f(x)$ has no roots in $\mathbb{F}_2$:

$$f(0) \equiv 1 \mod 2$$

$$f(1) \equiv 1 \mod 2$$

Let α be a root of this polynomial. Note that $\alpha \notin \mathbb{F}_2$.

$$\begin{aligned} f(\alpha) &= 0 \\ \Rightarrow \alpha^2 + \alpha + 1 &= 0 \\ \Rightarrow \alpha^2 &= 1 + \alpha \end{aligned}$$

Fields of Prime Power Order

We will now build $\mathbb{F}_4$ as an extension field over $\mathbb{F}_2$. $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, which we can see since $f(x)$ has no roots in $\mathbb{F}_2$:

$$f(0) \equiv 1 \mod 2$$

$$f(1) \equiv 1 \mod 2$$

Let α be a root of this polynomial. Note that $\alpha \notin \mathbb{F}_2$.

$$\begin{aligned} f(\alpha) &= 0 \\ \Rightarrow \alpha^2 + \alpha + 1 &= 0 \\ \Rightarrow \alpha^2 &= 1 + \alpha \end{aligned}$$

Again, working over $\mathbb{F}_2$:

$$\begin{aligned} \alpha^3 &= \alpha \times \alpha^2 = \alpha \times (1 + \alpha) \\ &= \alpha + \alpha^2 = \alpha + (1 + \alpha) \\ &= 1 + (\alpha + \alpha) = 1 \end{aligned}$$

Fields of Prime Power Order

We can therefore say that $\mathbb{F}_4 \equiv \{0, 1, \alpha, 1+\alpha\} \equiv \{0, \alpha, \alpha^2, \alpha^3\}$, with the following table showing how the two operations on F are related:

Multiplicative	Additive
0	0
α	α
α^2	$1+\alpha$
α^3	1

A similar process may be applied to construct any $\mathbb{F}_q$, with $q = p^r$.

Extending the Computer Program

- A polynomial of degree 2 or 3 is irreducible if and only if it has no root in $\mathbb{F}_p$.

Extending the Computer Program

- A polynomial of degree 2 or 3 is irreducible if and only if it has no root in $\mathbb{F}_p$.
- If $q = p^r$, where r is greater than 3, then verifying that a polynomial is irreducible over $\mathbb{F}_p$ is more difficult.

Extending the Computer Program

- A polynomial of degree 2 or 3 is irreducible if and only if it has no root in $\mathbb{F}_p$.
- If $q = p^r$, where r is greater than 3, then verifying that a polynomial is irreducible over $\mathbb{F}_p$ is more difficult.
- For example, the polynomial $f(x) = x^4 + x^2 + 1$ has degree four and is reducible, even though it has no root over $\mathbb{F}_2$:

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 + x + 1).$$

Further Computer Results

Number of 2-d subspaces in $M_n(\mathbb{F}_q)$ with t distinct ranks:

n, q	t = 1	t = 2	t = 3	t = 4	Total
3, 4	0	12	9	0	21
3, 8	0	52	21	0	73
3, 9	0	67	24	0	91
4, 4	0	123	234	0	357
4, 8	0	2407	2388	0	4745
5, 4	162	505	5130	0	5797

Known Bounds

If t is the number of distinct ranks in a 2-d subspaces of $M_n(\mathbb{F}_q)$:

$$t \leq n$$

Known Bounds

If t is the number of distinct ranks in a 2-d subspaces of $M_n(\mathbb{F}_q)$:

$$t \leq n$$

We also have that

$$t \leq q + 1.$$

A Tight Bound

An Optimal Construction: One matrix should have every entry on the diagonal equal to one, and the other should have the first entry equal to zero, the next two entries equal to one, ..., the next k entries equal to $k-1$. So, for example, the optimal 6×6 subspace would have four distinct ranks and would be generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

A Tight Bound

The optimal 10×10 subspace would contain five distinct ranks and would be generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

This leads to the following formula, which tells you the minimum n such that it is possible to generate t distinct ranks in the 2-d subspace:

$$n \geq \frac{t \times (t-1)}{2}$$

A Tight Bound

To derive this formula, notice that there is 1 zero, 2 ones, 3 twos, ..., k $(k-1)$'s along the diagonal of the second matrix:

$$\begin{pmatrix}
0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\
0 & 1 & \ddots & & & & & & & \vdots \\
\vdots & \ddots & 1 & \ddots & & & & & & \vdots \\
\vdots & & \ddots & 2 & \ddots & & & & & \vdots \\
\vdots & & & \ddots & 2 & \ddots & & & & \vdots \\
\vdots & & & & \ddots & 2 & \ddots & & & \vdots \\
\vdots & & & & & \ddots & \ddots & \ddots & & \vdots \\
\vdots & & & & & & \ddots & k-1 & \ddots & \vdots \\
\vdots & & & & & & & \ddots & \ddots & 0 \\
0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & k-1
\end{pmatrix}$$

 Galois, E., *Sur la thorie des nombres*, Bulletin des Sciences mathmatiques XIII, 1830

 Lidl, R. & Niederreiter, H., *Encyclopedia of Mathematics and its Applications 20: Finite Fields*, Cambridge University Press, 2nd Edition, 1997