Enumeration of Matrices and Splitting Subspaces over Finite Fields

Divya Aggarwal

Research Seminar
February 12, 2021

Advisor: Dr. Samrith Ram
Department of Mathematics,
IIIT Delhi.

Outline

- Counting Techniques
- Applications to various matrices
- T-splitting subspaces
- Future Directions

Notation

q	a prime power
$\mathbb{F}_q$	finite field with q elements
$\mathbb{F}_q^n$	vector space of all n-tuples over $\mathbb{F}_q$
$\mathrm{GL}_n(q)$	group of $n \times n$ invertible matrices over $\mathbb{F}_q$
$\mathrm{M}_n(q)$	set of $n \times n$ matrices over $\mathbb{F}_q$
$\gamma_n(q)$	order of the group $GL_n(q)$
γ_n	order of the group $GL_n(q)$ with q understood
$[n]$	the set $\{1, 2, \ldots, n\}$ for $n \in \mathbb{N}$

q-Analogues

A q-**analogue** of a mathematical object is an object depending on the variable q that "reduces to" (an admittedly vague term) the original object when we set $q = 1$.

A q-Analogue of permutations as bijections

Let $[n]$ be regarded as a set of n elements. A **permutation** w of the set $[n]$ is a bijection $w : [n] \to [n]$ preserving the "structure" of $[n]$.

Hence a q-analogue of a permutation w is a bijection $A : \mathbb{F}_q^n \to \mathbb{F}_q^n$ preserving the structure of $\mathbb{F}_q^n$. Thus **$\mathrm{GL}_n(q)$ is a q-analogue of the symmetric group S_n.**
The structure under consideration is that of a vector space, so A is simply an invertible linear transformation on $\mathbb{F}_q^n$.

The **number of invertible** $n \times n$ matrices over $\mathbb{F}_q$ is given by

$$\gamma_n(q) := |GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}).$$

$$= q^{\binom{n}{2}}(q-1)^n[n]_q!$$

Gaussian Binomial Coefficient

The number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is given by the **Gaussian binomial coefficient**

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)(q^k-q^2)\dots(q^k-q^{k-1})}$$

Gaussian Binomial Coefficient

The number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is given by the **Gaussian binomial coefficient**

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)(q^k-q^2)\dots(q^k-q^{k-1})}$$

$$= \frac{[n]_q!}{[k]_q![n-k]_q!},$$

where $[n]_q := q^{n-1}+q^{n-2}+\cdots+1$ is called **'the q-analogue of n'** and $[n]_q! := [n]_q[n-1]_q\dots[1]_q$ is called **'the q-analogue of $n!$'**.

Gaussian Binomial Coefficient

The number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is given by the **Gaussian binomial coefficient**

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)(q^k-q^2)\dots(q^k-q^{k-1})}$$

$$= \frac{[n]_q!}{[k]_q![n-k]_q!},$$

where $[n]_q := q^{n-1} + q^{n-2} + \cdots + 1$ is called **'the q-analogue of n'** and $[n]_q! := [n]_q[n-1]_q \dots [1]_q$ is called **'the q-analogue of $n!$'**.

For $q = 1$, it reduces to normal binomial coefficient and hence a q-analogue of the number of k-element subsets of an n-element set.

A q-Analogue of $n!$

A **flag** of length k in a vector space V is an increasing sequence of subspaces

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_k = V.$$

If $\dim V = n$, then a **complete flag** is a flag of length n. Necessarily, $\dim V_i = i$.

A q-Analogue of $n!$

A **flag** of length k in a vector space V is an increasing sequence of subspaces

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_k = V.$$

If dim $V = n$, then a **complete flag** is a flag of length n. Necessarily, dim $V_i = i$.

The number of complete flag of an n-dimensional vector space over $\mathbb{F}_q$ is

$$\binom{n}{1}_q \binom{n-1}{1}_q \cdots \binom{1}{1}_q = [n]_q [n-1]_q \ldots [1]_q = [n]_q!.$$

Now $n!$ is the number of sequences $\phi \subset S_0 \subset S_1 \subset \cdots \subset S_n = [n]$ of subsets of $[n]$. Thus $[n]_q!$ is regarded as a satisfactory q-analogue of $n!$.

An Example : Linear Codes

An $[n, k]$ linear q-ary code is a k-dimensional subspace of the space of ${\mathbb{F}_q}^n$.

An Example : Linear Codes

An $[n, k]$ linear q-ary code is a k-dimensional subspace of the space of ${\mathbb{F}_q}^n$.

Thus, the number of $[n, k]$ linear q-ary codes is the Gaussian binomial coefficient $\binom{n}{k}_q$

An Example : Linear Codes

An $[n, k]$ linear q-ary code is a k-dimensional subspace of the space of ${\mathbb{F}_q}^n$.

Thus, the number of $[n, k]$ linear q-ary codes is the Gaussian binomial coefficient $\binom{n}{k}_q$

Similarly, an $[n, k]$ linear binary code is a k-dimensional subspace of the space of ${\mathbb{F}_2}^n$.

So, the number of $[n, k]$ linear binary codes is the Gaussian binomial coefficient $\binom{n}{k}_2$.

An Application: Matrices by Rank

The number of $m \times n$ matrices of rank k over $\mathbb{F}_q$ is

$$\binom{m}{k}_q (q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})$$
$$= \frac{(q^m - 1)(q^m - q)\cdots(q^m - q^{k-1})(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})}{(q^k - 1)(q^k - q)\cdots(q^k - q^{k-1})}.$$

An Application: Matrices by Rank

The number of $m \times n$ matrices of rank k over $\mathbb{F}_q$ is

$$\binom{m}{k}_q (q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})$$
$$= \frac{(q^m - 1)(q^m - q) \cdots (q^m - q^{k-1})(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}.$$

- To justify the formula, note that the number of k-dimensional subspaces of $\mathbb{F}_q^m$ to serve as the column space of a rank k matrix is $\binom{m}{k}_q$. Identify the column space with the image of the associated linear map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^m$.
- There are $(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})$ surjective linear maps from $\mathbb{F}_q^n$ to that k-dimensional image.

Generating Functions

Let $a_0, a_1, a_2, \ldots$ be a sequence of real numbers. Then the formal power series

$$A(x) = \sum_{n \geq 0} a_n x^n$$

is called the **ordinary generating function** for the sequence $\{a_i\}_{i \geq 0}$.

Let $a_0, a_1, a_2, \ldots$ be a sequence of real numbers. Then the formal power series

$$A(x) = \sum_{n \geq 0} a_n x^n$$

is called the **ordinary generating function** for the sequence $\{a_i\}_{i \geq 0}$.

We will consider generating functions of the form

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n$$

where the sequence a_n counts some class of $n \times n$ matrices.

$A \in \mathrm{M}_n(q)$ as $\mathbb{F}_q[x]$-Module

Given $A \in \mathrm{M}_n(q)$, then A defines a **$\mathbb{F}_q[x]$-module on the vector space $\mathbb{F}_q^n$**, where the action of x is that of A defined by $x.v = Av$ for $v \in \mathbb{F}_q^n$.

$A \in \mathrm{M}_n(q)$ as $\mathbb{F}_q[x]$-Module

Given $A \in \mathrm{M}_n(q)$, then A defines a **$\mathbb{F}_q[x]$-module on the vector space $\mathbb{F}_q^n$**, where the action of x is that of A defined by $x.v = Av$ for $v \in \mathbb{F}_q^n$.

Using structure theorem for finitely-generated modules over PID's, this module is isomorphic to a direct sum

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbb{F}_q[x] / < \phi_i^{\lambda_{i,j}} >$$

where $\phi_1, \ldots, \phi_k$ are distinct monic irreducible polynomials; for each i, $\lambda_i = (\lambda_{i,1}, \lambda_{i,2}, \ldots, \lambda_{i,l_i})$ such that $\lambda_{i,1} \geq \lambda_{i,2} \geq \ldots \geq \lambda_{i,l_i}$ is a partition of $n_i = \sum_j \lambda_{i,j}$ corresponding to ϕ_i.

$A \in \mathrm{M}_n(q)$ as $\mathbb{F}_q[x]$-Module

Given $A \in \mathrm{M}_n(q)$, then A defines a **$\mathbb{F}_q[x]$-module on the vector space $\mathbb{F}_q^n$**, where the action of x is that of A defined by $x.v = Av$ for $v \in \mathbb{F}_q^n$.

Using structure theorem for finitely-generated modules over PID's, this module is isomorphic to a direct sum

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbb{F}_q[x]/ < \phi_i^{\lambda_{i,j}} >$$

where $\phi_1, \ldots, \phi_k$ are distinct monic irreducible polynomials; for each i, $\lambda_i = (\lambda_{i,1}, \lambda_{i,2}, \ldots, \lambda_{i,l_i})$ such that $\lambda_{i,1} \geq \lambda_{i,2} \geq \ldots \geq \lambda_{i,l_i}$ is a partition of $n_i = \sum_j \lambda_{i,j}$ corresponding to ϕ_i.

Moreover, the characteristic polynomial $\det(xI - A)$ of A is given by

$$\det(xI - A) = \prod_{i=1}^{k} \phi_i^{n_i}.$$

Since A is a $n \times n$ matrix, it follows $n = \sum_i n_i \deg \phi_i$.

Cyclic Decomposition Theorem

Let T be a linear operator on a finite-dimensional vector space V. There exists non-zero vectors $\alpha_1, \ldots, \alpha_r$ in V with respective T-annihilators $p_1, \ldots, p_r$ such that

$(i)\ V = Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_r; T)$;
$(ii)\ p_k$ divides $p_{k-1},\ k = 2, \ldots, r$.

Furthermore, the integer r and the polynomials $p_1, \ldots, p_r$ are uniquely determined by $(i),\ (ii)$, and the fact that no α_k is 0.

Here, $Z(\alpha; T) = \text{span}\ \{\alpha,\ T\alpha,\ T^2\alpha, \ldots,\ T^{d-1}\alpha\}$ is the cyclic subspace generated by α, where d is the degree of the T- annihilator of α.

Similarity Class Type

- The *similarity class* of A is determined by the data consisting of the finite set of distinct monic irreducible polynomials $\phi_1, \ldots, \phi_k$ and the corresponding partitions $\lambda_1, \ldots, \lambda_k$.
- If d_i is the degree of ϕ_i, then the *similarity class type* or *type* of A is the data consisting of the finite multiset $\{(d_1, \lambda_1), \ldots, (d_k, \lambda_k)\}$.
- For instance, if $\frac{F_q[x]}{(x+1)^2} \oplus \frac{F_q[x]}{(x+1)}$ is the module corresponding to a matrix A, then the similarity class of A is $\{x+1, (2,1)\}$ while the similarity class type of A is $\{1, (2,1)\}$.
- Thus, the type of T remembers only the degrees of the polynomials (and not the polynomials themselves) for which ϕ_i takes a certain value λ_i.

Cycle Index of $\mathrm{M}_n(q)$

Φ	Set of all nonconstant irreducible monic polynomials ϕ over $\mathbb{F}_q$.
Λ	Set of all partitions of all nonnegative integers.

For every $\phi \in \Phi$ and every partition $\lambda \neq \emptyset, \lambda \in \Lambda$, let $x_{\phi,\lambda}$ be an indeterminate. If $\lambda = \emptyset$, then set $x_{\phi,\lambda} = 1$. The **cycle index for conjugation action of $\mathrm{GL}_n(q)$ on $\mathrm{M}_n(q)$** is a polynomial in the indeterminates $x_{\phi,\lambda}$ defined by

$$\frac{1}{\gamma_n} \sum_{A \in \mathrm{M}_n(q)} \prod_{\phi \in \Phi} x_{\phi,\lambda_\phi(A)}$$

where $\lambda_\phi(A)$ is the partition associated to ϕ in the conjugacy class data for A. If ϕ does not occur in the polynomials associated to A, then $\lambda_\phi(A)$ is the empty partition, and thus $x_{\phi,\lambda_\phi(A)} = 1$.

We construct the generating function for the cycle index

$$1 + \sum_{n \geq 1} \frac{u^n}{\gamma_n} \sum_{A \in \mathrm{M}_n(q)} \prod_{\phi \in \Phi} x_{\phi, \lambda_\phi(A)}.$$

Generating Function for Cycle Index of $\mathrm{M}_n(q)$

We construct the generating function for the cycle index

$$1 + \sum_{n \geq 1} \frac{u^n}{\gamma_n} \sum_{A \in \mathrm{M}_n(q)} \prod_{\phi \in \Phi} x_{\phi, \lambda_\phi(A)}.$$

Theorem (Kung; 1981)

We have

$$1 + \sum_{n \geq 1} \frac{u^n}{\gamma_n} \sum_{A \in \mathrm{M}_n(q)} \prod_{\phi \in \Phi} x_{\phi, \lambda_\phi(A)} = \prod_{\phi \in \Phi} \sum_{\lambda \in \Lambda} \frac{x_{\phi,\lambda} u^{|\lambda| \deg \phi}}{c_\phi(\lambda)},$$

where $c_\phi(\lambda)$ is the order of the group of module automorphisms of the $\mathbb{F}_q[x]$-module $\bigoplus_j \mathbb{F}_q[x]/ < \phi^{\lambda_i} >$.

Some Important Results

Lemma

Let Φ' be a subset of the irreducible monic polynomials. Let a_n be the number of $n \times n$ matrices whose conjugacy class data involves only polynomials $\phi \in \Phi'$. Then

$$
\begin{aligned}
1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n &= \prod_{\phi \in \Phi'} \sum_{\lambda \in \Lambda} \frac{u^{|\lambda| \text{ deg } \phi}}{c_\phi(\lambda)} \\
&= \prod_{\phi \in \Phi'} \prod_{r \geq 1} \left(1 - \frac{u^{\text{deg } \phi}}{q^{r \text{ deg } \phi}}\right)^{-1}.
\end{aligned}
$$

Some Important Results

Lemma

For each irreducible monic polynomial ϕ, let L_ϕ be a subset of all partitions of the positive integers. Let a_n be the number of $n \times n$ matrices such that $\lambda_\phi(A) \in L_\phi$ for all ϕ. Then

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{\phi \in \Phi} \sum_{\lambda \in L_\phi} \frac{u^{|\lambda| \text{ deg } \phi}}{c_\phi(\lambda)}.$$

Diagonalizable Matrices

Let d_n be the number of **diagonalizable** $n \times n$ matrices over $\mathbb{F}_q$. Then

$$1 + \sum_{n \geq 1} \frac{d_n}{\gamma_n} u^n = \Big(\sum_{m \geq 0} \frac{u^m}{\gamma_m} \Big)^q.$$

It follows that

$$d_n = \sum_{n_1 + \cdots + n_q = n} \frac{\gamma_n}{\gamma_{n_1} \cdots \gamma_{n_q}}.$$

Solutions of $A^2 = I$

Let a_n be the number of $n \times n$ matrices A over $\mathbb{F}_q$ satisfying $A^2 = I$.

In characteristic other than two, the generating function for the a_n is

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \Big(\sum_{m \geq 0} \frac{u^m}{\gamma_m} \Big)^2,$$

and so

$$a_n = \sum_{i=0}^{n} \frac{\gamma_n}{\gamma_i \gamma_{n-i}}.$$

Solutions of $A^2 = I$

Let a_n be the number of $n \times n$ matrices A over $\mathbb{F}_q$ satisfying $A^2 = I$.

In characteristic other than two, the generating function for the a_n is

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \Big(\sum_{m \geq 0} \frac{u^m}{\gamma_m} \Big)^2,$$

and so

$$a_n = \sum_{i=0}^{n} \frac{\gamma_n}{\gamma_i \gamma_{n-i}}.$$

In characteristic two, $A^2 = I$ does not imply that A is diagonalizable and the above formula does not hold. Here, we have the formula

$$a_n = \sum_{0 \leq i \leq n/2} \frac{\gamma_n}{q^{i(2n-3i)} \gamma_i \gamma_{n-2i}}.$$

Solutions of $A^k = I$

More generally, let k be a positive integer not divisible by p, where q is a power of p. We consider the solutions of $A^k = I$ and let a_n be the number of $n \times n$ solutions with coefficients in $\mathbb{F}_q$. Now $z^k - 1$ factors into a product of distinct irreducible polynomials

$$z^k - 1 = \phi_1(z)\phi_2(z)\dots\phi_r(z).$$

Then the generating function for the a_n is

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{i=1}^{r} \sum_{m \geq 0} \frac{u^{md_i}}{\gamma_m(q^{d_i})},$$

where $\gamma_j(q^d) = |\mathrm{GL}_j(q^d)|$.

Cyclic Matrices

v_d number of irreducible monic polynomials of degree d over $\mathbb{F}_q$

A matrix A is **cyclic** if there exists a vector v such that $\{A^i v \mid i = 0, 1, 2, \ldots\}$ spans the underlying vector space. Equivalently, the minimal and characteristic polynomials of A are the same.

Cyclic Matrices

v_d number of irreducible monic polynomials of degree d over $\mathbb{F}_q$

A matrix A is **cyclic** if there exists a vector v such that $\{A^i v \mid i = 0, 1, 2, \ldots\}$ spans the underlying vector space. Equivalently, the minimal and characteristic polynomials of A are the same.

Let a_n be the number of cyclic matrices over $\mathbb{F}_q$. The generating function factors as

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d \geq 1} \left(1 + \frac{1}{q^d - 1} \frac{u^d}{1 - (u/d)^d}\right)^{v_d}$$

and can be put into the form

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{d \geq 1} \left(1 + \frac{u^d}{q^d(q^d - 1)}\right)^{v_d}.$$

Semi-Simple Matrices

A matrix A is **semi-simple** if it diagonalizes over the algebraic closure of the base field.

Let a_n be the number of semi-simple $n \times n$ matrices over $\mathbb{F}_q$. Then the generating function has a factorization

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d \geq 1} \left(1 + \sum_{j \geq 1} \frac{u^{jd}}{\gamma_j(q^d)}\right)^{v_d}.$$

Separable Matrices

A matrix is **separable** if it is both cyclic and semi-simple, which is equivalent to having a characteristic polynomial that is square-free.

Let a_n be the number of separable $n \times n$ matrices over $\mathbb{F}_q$. Then the generating function factors

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d \geq 1} \left(1 + \frac{u^d}{q^d - 1}\right)^{v_d}.$$

Niloptent Matrices

An $n \times n$ matrix A is **nilpotent** if there exists a positive integer r such that $A^r = 0$.

Equivalently, A is nilpotent if and only if all its eigenvalues are 0.

Niloptent Matrices

An $n \times n$ matrix A is **nilpotent** if there exists a positive integer r such that $A^r = 0$.

Equivalently, A is nilpotent if and only if all its eigenvalues are 0.

(Fine and Herstein) The number of nilpotent $n \times n$ matrices is $q^{n(n-1)}$.

α-Splitting Subspace

- For $V = \mathbb{F}_{q^{md}}$, let $\alpha \in \mathbb{F}_{q^{md}}$ and T is $\mathbb{F}_q$-linear endomorphism of $\mathbb{F}_{q^{md}}$ given by $x \to \alpha x$. Then we call any m-dimensional subspace W of $\mathbb{F}_{q^{md}}$ as **α-splitting** if

$$\mathbb{F}_{q^{md}} = W \oplus \alpha W \oplus \ldots \oplus \alpha^{d-1} W,$$

and denote by $\sigma(m, d; T)$ the number of m-dimensional α-splitting subspaces of $\mathbb{F}_{q^{md}}$.

α-Splitting Subspace

- For $V = \mathbb{F}_{q^{md}}$, let $\alpha \in \mathbb{F}_{q^{md}}$ and T is $\mathbb{F}_q$-linear endomorphism of $\mathbb{F}_{q^{md}}$ given by $x \to \alpha x$. Then we call any m-dimensional subspace W of $\mathbb{F}_{q^{md}}$ as **α-splitting** if

$$\mathbb{F}_{q^{md}} = W \oplus \alpha W \oplus \ldots \oplus \alpha^{d-1} W,$$

and denote by $\sigma(m, d; T)$ the number of m-dimensional α-splitting subspaces of $\mathbb{F}_{q^{md}}$.

Note: For an arbitrary $\alpha \in \mathbb{F}_{q^{md}}$, there may not be any α-splitting subspace; e.g., if $\alpha \in \mathbb{F}_q$ and $d > 1$. However, if $\alpha \in \mathbb{F}_{q^{md}}$ satisfies $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$, then a α-splitting subspace exists, e.g.,

$$W = \text{span}\{1, \alpha^d, \alpha^{2d}, \ldots, \alpha^{(m-1)d}\}.$$

- Let $\alpha \in \mathbb{F}_{q^{md}}$ be such that $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$. Then what is $\sigma(m, d; T)$?

Splitting Subspace Theorem

- Let $\alpha \in \mathbb{F}_{q^{md}}$ be such that $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$. Then what is $\sigma(m, d; T)$?

Splitting Subspace Theorem (E. Chen, D. Tseng; 2013)

Let $\alpha \in \mathbb{F}_{q^{md}}$ satisfy $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$. Then

$$\sigma(m, d; T) = \frac{q^{md} - 1}{q^m - 1} q^{m(m-1)(d-1)}.$$

.

T-Splitting Subspaces

Given an md-dimensional vector space V and any $\mathbb{F}_q$-linear endomorphism $T : V \to V$, we say that an m-dimensional subspace W of V is **T-splitting** if

$$V = W \oplus T(W) \oplus T^2(W) \oplus \cdots \oplus T^{d-1}(W),$$

where T^j denotes the j-fold composite of T with itself $(0 \le j \le d-1)$ and denote by $\sigma(m, d; T)$ the number of m-dimensional T-splitting subspaces of V.

Some Special Cases

- If $d = 1$, then $W = V$ is obviously the only m-dimensional T-splitting subspace, for any $T : V \to V$ and thus $\sigma(m, 1; T) = 1$.

Some Special Cases

- If $d = 1$, then $W = V$ is obviously the only m-dimensional T-splitting subspace, for any $T : V \to V$ and thus $\sigma(m, 1; T) = 1$.
- If $m = 1$, then the existence of m-dimensional T-splitting subspaces of V evidently forces T to be cyclic and the minimal polynomial of T to be the characteristic polynomial of T.

Proposition (S.R. Ghorpade, S. Ram; 2012)

Let $T : V \to V$ be a cyclic $\mathbb{F}_q$-linear endomorphism and let $p_T \in F_q[X]$ be the minimal polynomial of T. Suppose $p_T = f_1^{e_1} \cdots f_k^{e_k}$ is the factorization of p_T into positive powers of distinct monic irreducible polynomials $f_i \in \mathbb{F}_q[X]$ with deg $(f_i) = n_i$ for $i = 1, \ldots, k$. Then

$$\sigma(1, d; q) = \frac{q^d}{q-1} \prod_{i=1}^{k} \Big(1 - \frac{1}{q^{n_i}}\Big).$$

Determination of $\sigma(m, d; T)$

Open Problem

Determine $\sigma(m, d; T)$ for every $\mathbb{F}_q$-linear endomorphism T of V.

Splitting Subspaces for Cyclic Nilpotent Operators

Proposition (A. and S. Ram; 2020)

Let T and T' be similar linear operators on an md-dimensional vector space V. Then $\sigma(m, d; T) = \sigma(m, d; T')$.

Proposition (A. and S. Ram; 2020)

Let T and T' be similar linear operators on an md-dimensional vector space V. Then $\sigma(m, d; T) = \sigma(m, d; T')$.

Sketch of the proof : There exists a linear isomorphism S of V such that $T' = S \circ T \circ S^{-1}$.

Then W is a splitting subspace for T if and only if SW is a splitting subspace for T'.

Splitting Subspaces for Cyclic Nilpotent Operators

Proposition (A. and S. Ram; 2020)

Let T and T' be similar linear operators on an md-dimensional vector space V. Then $\sigma(m, d; T) = \sigma(m, d; T')$.

Sketch of the proof : There exists a linear isomorphism S of V such that $T' = S \circ T \circ S^{-1}$.
Then W is a splitting subspace for T if and only if SW is a splitting subspace for T'.

Theorem (A. and S. Ram; 2020)

Let T be a cyclic nilpotent operator over $\mathbb{F}_q$. Then

$$\sigma(m, d; T) = q^{m^2(d-1)}.$$

.

Similarity class type and Splitting subspaces

Theorem (A. and S. Ram; 2020)

Suppose T and T' are two operators of the same similarity class type defined on an md-dimensional vector space over $\mathbb{F}_q$.Then $\sigma(m, d; T) = \sigma(m, d; T')$.

Similarity class type and Splitting subspaces

Theorem (A. and S. Ram; 2020)

Suppose T and T' are two operators of the same similarity class type defined on an md-dimensional vector space over $\mathbb{F}_q$.Then $\sigma(m, d; T) = \sigma(m, d; T')$.

Define $\sigma_q(m, d; \tau)$ to be the number of m-dimensional splitting subspaces for a linear operator of similarity class type τ defined over an $\mathbb{F}_q$-vector space of dimension md.

Similarity class type and Splitting subspaces

Theorem (A. and S. Ram; 2020)

Suppose T and T' are two operators of the same similarity class type defined on an md-dimensional vector space over $\mathbb{F}_q$.Then $\sigma(m, d; T) = \sigma(m, d; T')$.

Define $\sigma_q(m, d; \tau)$ to be the number of m-dimensional splitting subspaces for a linear operator of similarity class type τ defined over an $\mathbb{F}_q$-vector space of dimension md.

Theorem (A. and S. Ram; 2020)

If m, d, τ are fixed, then $\sigma_q(m, d; \tau)$ is a polynomial in q.

Future Directions

- *Conjecture:* $\sigma_q(m, d; \tau)$ is a polynomial in q of degree $m^2(d-1)$.

Future Directions

- *Conjecture:* $\sigma_q(m, d; \tau)$ is a polynomial in q of degree $m^2(d-1)$.
- Determine $\sigma(m, d; T)$ for every $\mathbb{F}_q$-linear endomorphism T of V.

References

1. Divya Aggarwal, Samrith Ram, Splitting Subspaces of Linear Operators over Finite Fields. arXiv:2012.08411
2. E. Chen, D. Tseng, The splitting subspace conjecture, Finite Fields Appl. 24 (2013) 15-28.
3. M. Gerstenhaber, On the number of nilpotent matrices with coefficients in a finite field, Illinois J. Math. 5 (1961), 330-333.
4. S.R. Ghorpade, S. Ram, Enumeration of splitting subspaces over finite fields, in: Y. Aubry, C. Ritzenthaler, A. Zykin (Eds.), Arithmetic, Geometry, and Coding Theory, Luminy, France, March 2011, in:Contemp.Math., vol.574, American Mathematical Society, Providence, RI, 2012, pp.49-58.
5. S.R. Ghorpade, S. Ram, Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields, Finite Fields Appl. 17 (2011) 461-472.
6. R. Lidl, H. Niederreiter, Finite Fields, 2nd edition, Cambridge University Press, Cambridge, 1997.
7. K. Morrison, Integer sequences and matrices over finite fields, J. Integer Seq. 9 (2006), Article 06.2.1.
8. R. P. Stanley, Enumerative Combinatorics, vol.1, second edition, Cambridge Stud. Adv. Math., vol.49, Cambridge University Press, Cambridge, 2012.
9. J. H. van Lint, R. M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, 1992.

Thank you for your attention!