# Splitting subspaces, Krylov subspaces and polynomial matrices over finite fields

by
Divya Aggarwal
(PhD 19301)

Under the Supervision of Dr. Samrith Ram

Indraprastha Institute of Information Technology Delhi
September, 2024

# Splitting subspaces, Krylov subspaces and polynomial matrices over finite fields

by
Divya Aggarwal
(PhD 19301)

Submitted
in partial fulfilment of the requirements for the degree of
Doctor of Philosophy

to the

Indraprastha Institute of Information Technology Delhi
September, 2024

***Dedicated to my parents***

# Certificate

**This is to certify that the thesis titled "Splitting subspaces, Krylov subspaces and polynomial matrices over finite fields" being submitted by Divya Aggarwal to the Indraprastha Institute of Information Technology Delhi, for the award of the degree of Doctor of Philosophy, is an original research work carried out by her under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.**

**The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree/diploma.**

**Dr. Samrith Ram**

**September, 2024**

**Indraprastha Institute of Information Technology Delhi**

**New Delhi 110020**

# Acknowledgements

I would like to express my deepest gratitude to my advisor, Dr. Samrith Ram, whose expertise, patience, and relentless support have been indispensable throughout my doctoral journey. His invaluable input and dedication to excellence have been instrumental in shaping this thesis. His mentorship and suggestions have significantly enriched the quality of this work.

I extend my sincere gratitude to Prof. Amritanshu Prasad, whose guidance, enthusiastic encouragement and unwavering support have helped me learn and grow. His insights and expertise in the subject have been an inspiration to me. I am profoundly thankful to Dr. Jeetendra Aggarwal and Dr. Surbhi Madan for their continuous motivation and belief in my potential.

I am immensely grateful to Indraprastha Institute of Information Delhi for providing the scholarly environment and resources essential for conducting this research. Special acknowledgement is due to the Council of Scientific and Industrial Research (CSIR) for their generous financial support, which facilitated the realization of this project.

I am indebted to my esteemed committee members, Dr. Sneha Chaubey and Dr. Shilpak Banerjee, for their constructive feedback and scholarly rigour.

My heartfelt appreciation goes to my beloved family for their boundless love, encouragement, and unwavering belief in my abilities. Their persistent support and understanding have been a constant source of strength and motivation.

To my dear friends and colleagues, your friendship and intellectual companionship have made this journey more fulfilling and enjoyable. Your stimulating conversations and shared experiences have enriched my academic journey immeasurably.

Divya Aggarwal

# Abstract

Let $V$ be a vector space of dimension $n$ over the finite field $\mathbb{F}_q$ and $T$ be a linear operator on $V$. Given an integer $m$ that divides $n$, an $m$-dimensional subspace $W$ of $V$ is $T$-splitting if $V = W \oplus TW \oplus \cdots \oplus T^{d-1}W$ where $d = n/m$. Let $\sigma(m, d; T)$ denote the number of $m$-dimensional $T$-splitting subspaces. Determining $\sigma(m, d; T)$ for an arbitrary operator $T$ is an interesting problem. We prove that $\sigma(m, d; T)$ depends only on the similarity class type of $T$ and give an explicit formula in the special case where $T$ is cyclic and nilpotent. Denote by $\sigma(m, d; \tau)$ the number of $m$-dimensional splitting subspaces for a linear operator of similarity class type $\tau$ over an $\mathbb{F}_q$-vector space of dimension $md$. For fixed values of $m, d$ and $\tau$, we show that $\sigma(m, d; \tau)$ is a polynomial in $q$. This problem is closely related to another open problem on Krylov spaces. We discuss this connection and give explicit formulae for $\sigma(m, d; T)$ in the case where the invariant factors of $T$ satisfy certain degree conditions. A connection with another enumeration problem on polynomial matrices is also discussed.

We finally present a brief review of some recent developments in the splitting subspaces problem. In particular, the connection of this problem to the theory of symmetric functions is highlighted. Lastly, we conclude with some future directions for research.

# Contents

# List of Figures

# Notations

| | |
|---|---|
| $q$ | a prime power |
| $\mathbb{F}_q$ | finite field with $q$ elements |
| $\mathbb{F}_q[x]$ | $\mathbb{F}_q$-algebra of polynomials in the indeterminate $x$ |
| $\begin{bmatrix} \cdot \\ \cdot \end{bmatrix}_q$ | $q$-binomial coefficient |
| $n, k, m, d$ | positive integers |
| $R$ | a ring |
| $\mathrm{M}_{n,k}(R)$ | set of $n \times k$ matrices over $R$ |
| $\mathrm{M}_n(R)$ | ring of $n \times n$ matrices over $R$ |
| $\mathrm{GL}_n(\mathbb{F}_q)$ | group of $n \times n$ invertible matrices over $\mathbb{F}_q$ |
| $\gamma_q(n)$ | order of the group $\mathrm{GL}_n(\mathbb{F}_q)$ |
| $\lambda, \mu$ | integer partitions |

# Chapter 1

# Introduction

This thesis comprises a study of some problems in enumerative combinatorics, which have their origin in cryptography and number theory. Let $\mathbb{F}_q$ denote the finite field with $q$ elements where $q$ is a prime power. Throughout the thesis, the variables $m$ and $d$ denote positive integers.

## 1.1 Splitting subspaces and Krylov subspaces

Let $V$ be an $md$-dimensional vector space over the finite field $\mathbb{F}_q$. We begin with a definition.

**Definition 1.1.1.** Let $T$ be a linear operator on $V$. A subspace $W$ of $V$ of dimension $m$ is a *splitting subspace* for $T$ if

$$V = W \oplus TW \oplus \cdots \oplus T^{d-1}W.$$

The above definition was motivated by the following question asked by Niederreiter [31, p. 11]: Let $\alpha \in \mathbb{F}_{q^{md}}$ be such that $\alpha$ is a generator of the cyclic group $\mathbb{F}_{q^{md}}^*$ of nonzero elements in $\mathbb{F}_{q^{md}}$. How many $m$-dimensional $\mathbb{F}_q$-linear subspaces $W$ of $\mathbb{F}_{q^{md}}$ satisfy

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

An example of a subspace which satisfies the above condition is

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

Niederreiter encountered this problem in the context of his work on the multiple-recursive matrix method for pseudorandom number generation. This question was settled by Chen and Tseng [11, Cor. 3.4] who proved a conjecture [18, Conj. 5.5] that the number of such subspaces is

$$\frac{q^{md}-1}{q^m-1} q^{m(m-1)(d-1)}. \tag{1.1}$$

Another proof of the result of Chen and Tseng and some connections with unimodular matrices may be found in [3]. Given a linear operator $T$ on $V$, let $\sigma(m, d; T)$ denote the number of $m$-dimensional $T$-splitting subspaces. Finding a formula for $\sigma(m, d; T)$ for arbitrary $T$ is an interesting problem [19, p. 54]. If $T$ has an irreducible characteristic polynomial, then it follows from the work of Chen and Tseng that $\sigma(m, d; T)$ is given by the expression in (1.1) above.

In fact, splitting subspaces are closely related to anti-invariant subspaces. A subspace $W$ is said to be $k$-fold anti-invariant with respect to $T$ if

$$\dim(W + TW + \cdots + T^k W) = (k+1) \dim W.$$

Barría and Halmos [4] and Sourour [44] determined the maximal dimension of a 1-fold anti-invariant subspace for a given operator $T$. These results were generalized by Knüppel and Nielsen [25] who solved the same problem for $k$-fold anti-invariant subspaces.

The problem of determining $\sigma(m, d; T)$ has connections with an important problem on Krylov subspaces which we now discuss. Let $T$ be a linear operator on an $N$-dimensional vector space $V$ over $\mathbb{F}_q$. Let $S = \{v_1, \ldots, v_m\}$ be a set of $m$ vectors in $V$. The *truncated Krylov subspace* [7, p. 277] of order $d$ generated

by $S$ is defined by

$$\mathrm{Kry}(T, S; d) := \left\{ \sum_{i=1}^{m} f_i(T) v_i : f_i(x) \in \mathbb{F}_q[x] \text{ and } \deg f_i < d \right\}.$$

Define

$$\kappa_{m,d}(T) := \frac{1}{q^{Nm}} |\{(v_1, \ldots, v_m) \in V^m : \mathrm{Kry}(T, \{v_1, \ldots, v_m\}; d) = V\}|. \quad (1.2)$$

The number $\kappa_{m,d}(T)$ may be interpreted as the probability of selecting $m$ vectors $v_1, \ldots, v_m$ uniformly and independently from $V$ such that the truncated Krylov subspace of order $d$ spanned by them is all of $V$. Determining $\kappa_{m,d}(T)$ is useful in solving large sparse linear systems over finite fields which arise frequently in number theory and computer algebra [28, 50]. The Number Field Sieve which is a classical algorithm for factoring large integers relies on Krylov subspace methods [6, p. 24]. Krylov subspace methods are relevant to several areas of mathematics including quadrature methods, the analytic theory of continued fractions, infinite series expansions, orthogonalization algorithms and the mathematical foundations of quantum mechanics [28, p. 8]. Krylov-based methods such as Wiedemann's algorithm are used to compute the minimal polynomials of large matrices over finite fields [28, p. 19]. The probability $\kappa_{m,d}(T)$ is relevant to the analysis of the efficiency of such algorithms and obtaining bounds on $\kappa_{m,d}(T)$ is a difficult and important [7, p. 277] problem. The connection between $\kappa_{m,d}(T)$ and splitting subspaces (see Proposition 3.1.6) is as follows:

$$\kappa_{m,d}(T) = \frac{|\,\mathrm{GL}_m(\mathbb{F}_q)| \cdot \sigma(m, d; T)}{q^{m^2 d}}. \quad (1.3)$$

We are mainly interested in determining $\sigma(m, d; T)$. Building upon earlier work by Chen and Tseng, we give a general recurrence which may be solved to obtain an expression for the number of splitting subspaces. We prove that for fixed values of $m$ and $d$, the number $\sigma(m, d; T)$ depends only on the similarity class type of $T$. A crucial ingredient in the proof is a theorem of Fripertinger [14] on the number of invariant subspaces of a primary transformation. The sim-

ilarity class type of an operator is defined as follows. Denote by $\mathbb{F}_q[x]$ the $\mathbb{F}_q$-algebra of polynomials in the indeterminate $x$. If $T$ is a linear operator on a vector space $V$, then $T$ defines an $\mathbb{F}_q[x]$-module on the vector space $V$, where the action of $x$ is defined by $x \cdot v = Tv$ for $v \in V$. The $\mathbb{F}_q[x]$ module $V$ can be decomposed as a direct sum

$$V \simeq \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{\ell_i} \frac{\mathbb{F}_q[x]}{(\phi_i^{\lambda_{i,j}})},$$

where $\phi_1, \ldots, \phi_t$ are distinct monic irreducible polynomials and, for each $i$, $\lambda_i = (\lambda_{i,1}, \lambda_{i,2}, \ldots, \lambda_{i,\ell_i})$ is an integer partition corresponding to $\phi_i (1 \leq i \leq t)$. The finite set $\{(\phi_1, \lambda_1), \ldots, (\phi_t, \lambda_t)\}$ completely determines the *similarity class* of $T$ and corresponds uniquely to the invariant factors of $T$, i.e., the invariant factors of $xI - A$ where $A$ is the matrix of $T$ with respect to some basis. If $d_i = \deg \phi_i$, then the finite multiset

$$\tau = \{(d_1, \lambda_1), \ldots, (d_t, \lambda_t)\}$$

is the *similarity class type* of the linear operator $T$. For instance, if $\frac{\mathbb{F}_q[x]}{(x+1)^2} \oplus \frac{\mathbb{F}_q[x]}{(x+1)}$ is the module corresponding to the operator $T$, then the similarity class of $T$ is $\{(x+1, (2,1))\}$ while the similarity class type of $T$ is $\{(1, (2,1))\}$. The notion of similarity class type may be traced back to the work of Green [22, p. 405] on the irreducible characters of the finite general linear groups. Let $\sigma(m, d; \tau)$ denote the number of $m$-dimensional splitting subspaces for a linear operator of similarity class type $\tau$ defined over an $\mathbb{F}_q$-vector space of dimension $md$. We prove that for $m, d, \tau$ fixed, the quantity $\sigma(m, d; \tau)$ is a polynomial in $q$. We show that there is a simple formula for the number of splitting subspaces of a cyclic operator that is either nilpotent or unipotent. Finally, we give an application of our results to the enumeration of invertible matrices having a special form. This material is covered in Chapter 2.

## 1.2 Polynomial matrices and their connection to splitting subspaces

We begin by explaining some relevant background and give a brief motivated account of polynomial matrices. In what follows, $n, k$ denote positive integers with $k \leq n$. For any ring $R$, the set of all $n \times k$ matrices over $R$ is denoted by $M_{n,k}(R)$ while $M_n(R)$ indicates the ring of $n \times n$ matrices over $R$. Define

$$\mathrm{M}_q(n,k,d) := \{x^d I + x^{d-1}C_{d-1} + \cdots + C_0 : C_i \in \mathrm{M}_{n,k}(\mathbb{F}_q)\},$$

where $I$ denotes the $n \times k$ matrix whose $(i,j)$-th entry is 1 if $i = j$ and 0 otherwise. Evidently any element of $\mathrm{M}_q(n,k,d)$ is a polynomial with matrix coefficients which may also be viewed as a single $n \times k$ matrix over $\mathbb{F}_q$ whose entries are polynomials in $x$. Given elements $P, Q \in \mathrm{M}_q(n,k,d)$ write $P \sim Q$ ($P$ is equivalent to $Q$) if there exist invertible matrices $A \in M_n(\mathbb{F}_q[x])$ and $B \in M_k(\mathbb{F}_q[x])$ such that $APB = Q$. It can be shown that each $P \in M_q(n,k,d)$ is equivalent to a diagonal matrix

$$P \sim \mathrm{diag}_{n,k}(p_1, \ldots, p_k),$$

where $p_1, \ldots, p_k$ are monic polynomials over $\mathbb{F}_q$ satisfying $p_i \mid p_{i+1}$ for $1 \leq i < k$. This diagonal form is called the Smith Normal Form [24, p. 260] of $P$. By a $k$-tuple of invariant factors, we mean a $k$-tuple $\mathcal{I} = (f_1, \ldots, f_k)$ where each $f_i$ is a monic polynomial over $\mathbb{F}_q$ and $f_i \mid f_{i+1}$ for $1 \leq i \leq k-1$. Given such a $k$-tuple $\mathcal{I} = (p_1, \ldots, p_k)$ of invariant factors, define

$$\mu_q(n,k,d;\mathcal{I}) := |\left\{P \in \mathrm{M}_q(n,k,d) : P \sim \mathrm{diag}_{n,k}(p_1, \ldots, p_k)\right\}|.$$

In other words, $\mu_q(n,k,d;\mathcal{I})$ is the number of elements in $\mathrm{M}_q(n,k,d)$ whose Smith form comprises precisely the polynomials appearing in $\mathcal{I}$ as diagonal entries. Determination of $\mu_q(n,k,d;\mathcal{I})$ given an arbitrary assignment of the parameters in full generality is an open problem. To underscore the significance

of studying $\mu_q$ we briefly mention specific cases in the literature where it has been considered previously in the context of group theory, probability theory, unimodularity and mathematical control theory.

For $d = 1$ and $k = n$, we have

$$\mu_q(n, n, 1; \mathcal{I}) := |\{C_0 \in M_n(\mathbb{F}_q) : xI + C_0 \sim \mathrm{diag}_n(p_1, \ldots, p_k)\}|.$$

Two matrices $A, B \in M_n(\mathbb{F}_q)$ are similar if and only if $xI - A$ and $xI - B$ have the same Smith form. Thus in this setting we have the matrix conjugacy class size problem: How many matrices are similar to a given matrix $A$ with invariant factors $\mathcal{I} = (p_1, \ldots, p_n)$? Denoting by $c(\mathcal{I})$ the size of the centralizer in the general linear group $\mathrm{GL}_n(\mathbb{F}_q)$ corresponding to the conjugacy class indexed by $\mathcal{I}$, we have

$$\mu_q(n, n, 1; \mathcal{I}) = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{c(\mathcal{I})}.$$

According to Stanley [46, p. 108] a precise expression for the size of the centralizer $c(\mathcal{I})$ was first given by Philip Hall based on earlier work by Frobenius.

The case $k = 1$ is considered in Section 3.3, we must have $\mathcal{I} = (g)$ for some monic polynomial $g$ and in this case it is not difficult to see that $\mu_q(n, 1, d, (g))$ counts the number of $n$-tuples $(g_1, \ldots, g_n)$ of monic polynomials over $\mathbb{F}_q$ of degree $d$ such that $\gcd(g_1, \ldots, g_n) = g$. In particular, for $g = 1$, this problem has been studied by Corteel, Savage, Wilf and Zeilberger [12, Prop. 3] and a nice answer is known in this case.

The case where $\mathcal{I}$ is a $k$-tuple of 1's corresponds to unimodularity. A polynomial matrix is *unimodular* if its maximal minors are coprime. The case $d = 1$ for arbitrary $n, k$ with $k < n$ and $\mathcal{I} = (1, \ldots, 1)$ has been considered, albeit in a slightly different context, by Lieb, Jordan and Helmke [23, Thm. 1] who essentially prove that if $k < n$ are positive integers, then the number of matrices $A \in M_{n,k}(\mathbb{F}_q)$ for which $xI - A$ is unimodular is given by

$$\mu_q(n, k, 1, (1, \ldots, 1)) = \prod_{i=1}^{k} (q^n - q^i).$$

This theorem has connections with mathematical control theory and answers a question of Kociecki and Przyłuski [27] on the number of reachable linear systems over a finite field. We refer to the introduction of [37] for these connections and the link with unimodularity. A recent generalization of this result in the setting of unimodular polynomial matrices appears in [3, Thm. 4.1] and corresponds to the case of general $d$:

$$\mu_q(n,k,d,(1,\ldots,1)) = q^{nk(d-1)}\prod_{i=1}^{k}(q^n - q^i).$$

In Chapter 3, we prove that determining $\mu_q(n,k,d;\mathcal{I})$ for $n=k$ is intimately connected with the problem on splitting subspaces. We show that if $T$ is a linear operator on an $md$ dimensional vector space $V$ over $\mathbb{F}_q$, then $\sigma(m,d;T)>0$ if and only if the number of nonconstant invariant factors of $T$ is at most $m$. It is easily seen that the number $\sigma(m,d;T)$ depends only on the similarity class of $T$ (Proposition 2.2.2) since a subspace $W$ is $T$-splitting if and only if $SW$ is $S\circ T\circ S^{-1}$ splitting for each linear isomorphism $S$ of $V$. Thus, given an $md$-tuple of invariant factors $\mathcal{I}$, one can define

$$\sigma(m,d;\mathcal{I}) = \sigma(m,d;T),$$

where $T$ is any linear operator with invariant factors $\mathcal{I}$. By the positivity criterion for $\sigma(m,d;T)$ above, we may restrict ourselves to the case where the first $m(d-1)$ coordinates of the $md$-tuple $\mathcal{I}$ are equal to 1:

$$\mathcal{I} = (1,1,\ldots,1,p_1,p_2,\ldots,p_m).$$

For $\mathcal{I}$ as above, we prove the following.

**Theorem 1.2.1.** If $\deg p_1 = d$ and $p_1 = g_1^{e_1}\cdots g_t^{e_t}$, where the $g_i$ are distinct irreducible polynomials with $\deg g_i = d_i (1\le i\le t)$, then

$$\sigma(m,d;\mathcal{I}) = \frac{\prod_{i=1}^{t}\prod_{j=1}^{m}(1-q^{-jd_i})}{\prod_{j=1}^{m}(1-q^{-j})}q^{m^2(d-1)}.$$

**Theorem 1.2.2.** If $\deg p_1 = d - 1$, then

$$\sigma(m, d; \mathcal{I}) = \frac{c(\mathcal{I})}{c(\widetilde{\mathcal{I}})},$$

where $\widetilde{\mathcal{I}} = (\tilde{p}_1, \ldots, \tilde{p}_m)$ with $\tilde{p}_i = p_i/p_1$ for $1 \leq i \leq m$.

Note that $c(\mathcal{I})$ corresponds to a centralizer in $\mathrm{GL}_{md}(\mathbb{F}_q)$ while $c(\widetilde{\mathcal{I}})$ is associated with the group $\mathrm{GL}_m(\mathbb{F}_q)$. In conjunction with (1.3), the theorems above can be used to derive precise formulae for the probability $\kappa_{m,d}(T)$ (see (1.2)) for suitable values of $T$. This is the content of Chapter 3.

## 1.3 Future work

We finally discuss some recent developments concerning the enumeration problem of splitting subspaces. The notion of splitting subspaces was generalized by Prasad and Ram [34]. They gave the following definition.

**Definition 1.3.1.** Let $T$ be a linear operator on an $n$-dimensional vector space $V$ over $\mathbb{F}_q$. A subspace $W$ of $V$ has $T$-profile $\mu = (\mu_1, \mu_2, \ldots)$ if

$$\dim(W + TW + \cdots + T^{i-1}W) = \mu_1 + \cdots + \mu_i \quad \text{for all} \quad i \geq 1.$$

The number of subspaces with $T$-profile $\mu$ is denoted by $\sigma(\mu; T)$.

Prasad and Ram posed the problem of determining $\sigma(\mu; T)$ for an arbitrary operator $T$. They solved the problem when the operator is regular and diagonalizable [34] or when the profile $\mu$ has two parts $(\mu_1, \mu_2)$ such that $n = \mu_1 + \mu_2$ for an arbitrary operator using a linear algebraic approach [36]. Subsequently, Ram and Schlosser [40] gave a formula for $\sigma(\mu; T)$ when $T$ is a diagonal operator, extending the earlier work and establishing some connections with the theory of symmetric functions. A complete solution to this problem is given by Ram in [39], where the formula for $\sigma(\mu; T)$ is expressed as the Hall-scalar product of suitably defined symmetric functions. This result also leads to a solution to the problem of enumeration of anti-invariant subspaces and Krylov

subspaces. We briefly mention the applications of the solution to Krylov subspace methods. We conclude with a discussion on some future problems for research on the topic. This is covered in Chapter 4.

# Chapter 2

# Enumeration of splitting subspaces of linear operators

In this chapter, we are mainly interested in determining $\sigma(m, d; T)$ (see Section 1.1 for the definition). In Section 2.1, we give a general recurrence to count a more general class of subspaces that includes splitting subspaces. This recurrence is an extension of the recurrence relation given by Chen and Tseng [11]. We prove, in Section 2.2, that the number of splitting subspaces depends only on the similarity class type of the operator. We further prove some polynomiality results. In Section 2.3, we give precise formulae for the number of splitting subspaces for operators which are either nilpotent or unipotent. We also provide an application of our results to count the number of matrices which have a special form. This is in the spirit of earlier work by Gluesing-Luerssen and Ravagnani [20].

## 2.1 Counting flags of subspaces

To unravel the enumeration problem, we begin with some definitions and notation introduced by Chen and Tseng [11, Sec. 2] to count a more general class of subspaces that includes the $T$-splitting subspaces. In what follows, $V$ denotes a vector space of dimension $N$ over the finite field $\mathbb{F}_q$ and $T$ a linear operator on $V$.

**Definition 2.1.1.** Suppose $S_1, S_2, \ldots, S_k$ are sets of subspaces of $V$. Let $[S_1, S_2, \ldots, S_k]_T$ denote the set of all $k$-tuples $(W_1, W_2, \ldots, W_k)$ such that

$$\begin{aligned} W_i \in S_i \quad &\text{for} \quad 1 \leq i \leq k, \\ W_i \supseteq W_{i+1} + TW_{i+1} \quad &\text{for} \quad 1 \leq i \leq k-1. \end{aligned}$$

If $S_i$ is the set of all subspaces of $V$ of dimension $d_i$ for some $i$, then $S_i$ is denoted within the brackets as $d_i$. For instance, $[5, 3]_T$ denotes the set all tuples $(W_1, W_2)$ such that $\dim(W_1) = 5$, $\dim(W_2) = 3$ and $W_1 \supseteq W_2 + TW_2$.

**Definition 2.1.2.** Let $a$, $b$ be nonnegative integers such that $N \geq a \geq b$. Define

$$(a, b)_T = \left\{ W \subseteq V : \dim(W) = a \text{ and } \dim(W \cap T^{-1}W) = b \right\}.$$

For instance, $(3, 2)_T$ denotes the set of 3-dimensional subspaces $W$ for which $\dim(W \cap T^{-1}W) = 2$. Note that $(a, a)_T$ is the set of all subspaces of dimension $a$ which are invariant under $T$. We will freely use $[S_1, S_2, \ldots, S_k]$ to denote $[S_1, S_2, \ldots, S_k]_T$ and $(a, b)$ to denote $(a, b)_T$ when there is only one operator or when the operator under consideration is clear from the context.

**Definition 2.1.3.** Suppose $[S_{1,1}, S_{1,2}], [S_{2,1}, S_{2,2}], \ldots, [S_{r,1}, S_{r,2}]$ are sets as defined above. Then

$$\langle [S_{1,1}, S_{1,2}], [S_{2,1}, S_{2,2}], \ldots, [S_{r,1}, S_{r,2}] \rangle$$

denotes the set of $2r$-tuples of subspaces $(W_{1,1}, W_{1,2}, W_{2,1}, W_{2,2}, \ldots, W_{r,1}, W_{r,2})$ such that

$$\begin{aligned} (W_{i,1}, W_{i,2}) \in [S_{i,1}, S_{i,2}] \quad &\text{for} \quad 1 \leq i \leq r, \\ W_{i,2} \supseteq W_{i+1,1} \quad &\text{for} \quad 1 \leq i \leq r-1. \end{aligned}$$

For instance, $\langle [5, 4], [3, 2] \rangle$ is the set of all 4-tuples of subspaces

$(W_1, W_2, W_3, W_4)$ such that

$$\dim(W_1) = 5,\ \dim(W_2) = 4,\ \dim(W_3) = 3,\ \dim(W_4) = 2,$$
$$W_1 \supseteq W_2 + TW_2, \quad W_3 \supseteq W_4 + TW_4, \quad W_2 \supseteq W_3.$$

The next definition specifies an ordering on tuples labelling sets of the form

$$[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \ldots, (a_{r,1}, a_{r,2})].$$

**Definition 2.1.4.** Define an ordering on ordered pairs $(a, b)$ such that $(a_1, b_1) \succeq (a_2, b_2)$ if $a_1 > a_2$ or $a_1 = a_2$ and $b_1 \leq b_2$. Extend the ordering to tuples of the form

$$[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \ldots, (a_{r,1}, a_{r,2})]$$

in such a way that the order is lexicographic in terms of the ordered pairs $(a_{i,1}, a_{i,2})$ from left to right.

For instance, $(5, 2) \succ (5, 3) \succ (2, 1)$ while $[(8, 6), (5, 3)] \succ [(8, 6), (5, 4)] \succ [(7, 6), (6, 2)]$.

For fixed $r$, the ordering $\succeq$ is a total order. The following proposition is used repeatedly in constructing the recursion and follows easily from the definitions above.

**Proposition 2.1.5.** For nonnegative integers $N \geq a \geq b$, we have

$$\begin{aligned}[a, b] &= \bigcup_{i=b}^{a} [(a, i), b] \\ &= \bigcup_{j=0}^{b} [a, (b, j)].\end{aligned}$$

The recursion in the next lemma expresses the cardinality of sets of subspaces labelled by a tuple $\nu$ in terms of the cardinality of sets labelled by tuples $\mu \prec \nu$ in the ordering. The base cases are of the form $|[(a_1, a_1), (a_2, a_2), \ldots, (a_r, a_r)]_T|$. The following lemma and Proposition 2.1.7 extend results obtained by Chen and Tseng that hold for invertible operators.

**Lemma 2.1.6.** Let $T$ be a linear operator on an $N$-dimensional vector space. Suppose

$$a_{0,1} = a_{0,2} = N \geq a_{1,1} \geq a_{1,2} \geq a_{2,1} \geq a_{2,2} \geq \dots \geq a_{r,1} \geq a_{r,2} \geq 0 = a_{r+1,1} = a_{r+1,2},$$

$$\text{and } a_{i-1,1} \geq 2a_{i,1} - a_{i,2} \quad \text{for} \quad 1 \leq i \leq r.$$

(If the conditions are not satisfied, then $[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]$ is empty). Further, let

$$A = \{(j_1, \dots, j_r) : \max(a_{i+1,2}, 2a_{i,2} - a_{i,1}) \leq j_i \leq a_{i,2} \text{ and } 1 \leq i \leq r\},$$
$$B = \{(k_1, \dots, k_r) : a_{i,2} \leq k_i \leq a_{i,1} \text{ and } 1 \leq i \leq r\}.$$

Then

$$\begin{aligned}
&|[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]| \\
&= \sum_{(j_1,\dots,j_r)\in A} |[(a_{1,2}, j_1), (a_{2,2}, j_2), \dots, (a_{r,2}, j_r)]| \prod_{i=1}^{r} \begin{bmatrix} a_{i-1,2} - (2a_{i,2} - j_i) \\ a_{i,1} - (2a_{i,2} - j_i) \end{bmatrix}_q \\
&- \sum_{(k_1,\dots,k_r)\in B\setminus(a_{1,2},\dots,a_{r,2})} |[(a_{1,1}, k_1), (a_{2,1}, k_2), \dots, (a_{r,1}, k_r)]| \prod_{i=1}^{r} \begin{bmatrix} k_i - a_{i+1,1} \\ a_{i,2} - a_{i+1,1} \end{bmatrix}_q.
\end{aligned}$$

*Proof.* The proof is along the lines of [11, Lem. 2.7]. The size of $[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \dots, (a_{r,1}, a_{r,2})]$ is computed by applying Proposition 2.1.5. Consider

$$\begin{aligned}
&| \langle [a_{1,1}, a_{1,2}], [a_{2,1}, a_{2,2}], \dots, [a_{r,1}, a_{r,2}] \rangle | \\
&= \sum_{(k_1,\dots,k_r)\in B} | \langle [(a_{1,1}, k_1), a_{1,2}], [(a_{2,1}, k_2), a_{2,2}], \dots, [(a_{r,1}, k_r), a_{r,2}] \rangle | \\
&= \sum_{(k_1,\dots,k_r)\in B} |[(a_{1,1}, k_1), (a_{2,1}, k_2), \dots, (a_{r,1}, k_r)]| \prod_{i=1}^{r} \begin{bmatrix} k_i - a_{i+1,1} \\ a_{i,2} - a_{i+1,1} \end{bmatrix}_q. \qquad \text{(R)}
\end{aligned}$$

Using Proposition 2.1.5 again, we have

$$\begin{aligned}
&|\,\langle [a_{1,1},a_{1,2}],[a_{2,1},a_{2,2}],\dots,[a_{r,1},a_{r,2}]\rangle\,| \\
&= \sum_{(j_1,\dots,j_r)\in A} |\,\langle [a_{1,1},(a_{1,2},j_1)],[a_{2,1},(a_{2,2},j_2)],\dots,[a_{r,1},(a_{r,2},j_r)]\rangle\,| \\
&= \sum_{(j_1,\dots,j_r)\in A} |[(a_{1,2},j_1),(a_{2,2},j_2),\dots,(a_{r,2},j_r)]| \prod_{i=1}^{r} \begin{bmatrix} a_{i-1,2}-(2a_{i,2}-j_i) \\ a_{i,1}-(2a_{i,2}-j_i) \end{bmatrix}_q ,
\end{aligned} \tag{L}$$

where the last two equalities follow from the fact that

$$\dim(W+TW) = 2\dim W - \dim(W\cap T^{-1}W)$$

for every subspace $W$. Then (L) $-$ (R) $=0$. Adding

$$|[(a_{1,1},a_{1,2}),(a_{2,1},a_{2,2}),\dots,(a_{r,1},a_{r,2})]|$$

to both sides of this equality, we obtain the lemma. □

**Proposition 2.1.7.** Let $T$ be any linear operator on an $md$-dimensional vector space $V$. Then

$$\begin{aligned}
&[((d-1)m,(d-2)m),((d-2)m,(d-3)m),\dots,(2m,m),(m,0)]_T \\
&\qquad = \left\{ (\bigoplus_{i=0}^{d-2} T^iW,\ \bigoplus_{i=0}^{d-3} T^iW,\ \dots,\ W\oplus TW,\ W) \ :\ \bigoplus_{i=0}^{d-1} T^iW = V \right\}.
\end{aligned}$$

In particular,

$$\sigma(m,d;T) = |[((d-1)m,(d-2)m),((d-2)m,(d-3)m),\dots,(2m,m),(m,0)]_T|.$$

*Proof.* If $W$ is an $m$-dimensional subspace of $V$ such that $\dim(\bigoplus_{i=0}^{d-1} T^iW) = md$, then

$$(\bigoplus_{i=0}^{d-2} T^iW, \bigoplus_{i=0}^{d-3} T^iW, \dots, W\oplus TW, W)$$

$$\in [((d-1)m,(d-2)m),((d-2)m,(d-3)m),\ldots,(2m,m),(m,0)].$$

Conversely, suppose

$$(W_{d-1},W_{d-2},\ldots,W_2,W_1)$$
$$\in [((d-1)m,(d-2)m),((d-2)m,(d-3)m),\ldots,(2m,m),(m,0)].$$

Let $W_0=\{0\}$ and $W_d=W_{d-1}+TW_{d-1}$. We claim that

$$W_n=\bigoplus_{i=1}^{n}T^{i-1}W_1 \quad \text{for } 1\le n\le d.$$

We induct on $n$. The base case $n=1$ is evident. Now fix $1\le k\le d-1$ and suppose $W_j=\bigoplus_{i=1}^{j}T^{i-1}W_1$ for $j\le k$. By comparing dimensions, we must have $\dim T^{i-1}W_1=m$ for $i\le k$. We claim that $W_k\cap T^kW_1=\{0\}$. Suppose there is a nonzero vector $\beta\in W_k\cap T^kW_1$. Then $\beta=T\alpha$ for some $\alpha\in T^{k-1}W_1$ and consequently $\alpha\in W_k\cap T^{-1}W_k=W_{k-1}$, which contradicts the fact that $W_{k-1}\cap T^{k-1}W_1=\{0\}$. This proves the claim.

In fact, the restriction of $T$ to $T^{k-1}W_1$ is injective. For if $T\alpha=0$ for some nonzero $\alpha\in T^{k-1}W_1$, then $\alpha\in W_k\cap T^{-1}W_k=W_{k-1}$, contradicting the fact that $W_{k-1}\cap T^{k-1}W_1=\{0\}$. Injectivity of the restriction implies that $\dim T^kW_1=\dim T^{k-1}W_1=m$.

Now $W_k+TW_k\subseteq W_{k+1}$ and

$$\dim(W_k+TW_k)=\dim\bigoplus_{i=1}^{k+1}T^{i-1}W_1=(k+1)m=\dim W_{k+1}.$$

It follows that $W_{k+1}=W_k+TW_k=\bigoplus_{i=1}^{k+1}T^{i-1}W_1$, completing the proof by induction. Since $\dim W_d=\dim V$, it follows that $W_1$ is $T$-splitting. $\square$

## 2.2 Similarity class type and polynomiality of $\sigma(m, d; \tau)$

The similarity class of an operator $T$ is determined by the isomorphism type of the associated $\mathbb{F}_q[x]$-module on the vector space $V$ in which the action of $x$ is that of $T$. This module is isomorphic to a direct sum

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbb{F}_q[x]/(p_i^{\lambda_{i,j}}),$$

where $p_1, \ldots, p_k$ are distinct monic irreducible polynomials and, for each $1 \leq i \leq k$, the sequence $\lambda_{i,1} \geq \lambda_{i,2} \geq \cdots \geq \lambda_{i,l_i}$ is an integer partition of $n_i = \sum_j \lambda_{i,j}$. Let $\lambda_i$ denote the partition of $n_i$ given by the $\lambda_{i,j}$. The similarity class of $T$ is completely determined by the finite set of distinct monic irreducible polynomials $p_1, \ldots, p_k$ and the corresponding partitions $\lambda_1, \ldots, \lambda_k$.

**Definition 2.2.1.** If $d_i$ denotes the degree of $p_i$ for $1 \leq i \leq k$ in the decomposition above, then the *similarity class type* of $T$ is the finite multiset $\{(d_1, \lambda_1), \ldots, (d_k, \lambda_k)\}$.

Thus, the similarity class type of $T$ keeps track of only the degrees of the polynomials and the corresponding partitions in the decomposition above. The *size* of a similarity class type is the dimension of the vector space on which a corresponding operator is defined. The notion of similarity class type goes back to the work of Green [22, p. 405] on the characters of the finite general linear groups. One of the main reasons for considering the similarity class type is that many combinatorial invariants associated with $T$ often depend only on the partitions $\lambda_i$ and the degrees of the polynomials $\phi_i$ (and not the polynomials themselves). We begin by showing that the number of splitting subspaces depends only on the similarity class of $T$.

**Proposition 2.2.2.** Let $T$ and $T'$ be similar linear operators on an $md$-dimensional vector space $V$. Then $\sigma(m, d; T) = \sigma(m, d; T')$.

*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 $T'$. It follows that $\sigma(m,d;T) = \sigma(m,d;T')$. □

In fact Corollary 2.2.5 asserts that for fixed integers $m$ and $d$, the number $\sigma(m,d;T)$ depends only on the similarity class type of $T$.

Given a positive integer $n$, let $\beta(q,n)$ denote the number of irreducible polynomials of degree $n$ over $\mathbb{F}_q$. It is well known that

$$\beta(q,n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

where $\mu$ denotes the classical Möbius function. In fact $\beta(q,n)$ also counts the number of so called primitive necklaces of length $n$ over a $q$-ary alphabet [42, Thm. 7.1]. This interpretation entails the fact that, for $n$ fixed, the number $\beta(q,n)$ is strictly increasing as a function of $q$. Given a similarity class type $\tau$, let $q_0(\tau)$ denote the smallest prime power $\tilde{q}$ for which there exists a linear operator of type $\tau$ over the field $\mathbb{F}_{\tilde{q}}$. If $q \geq q_0(\tau)$ is a prime power then it follows from the property of $\beta(q,n)$ mentioned above that there exists a linear operator of type $\tau$ over $\mathbb{F}_q$.

**Theorem 2.2.3.** Fix a similarity class type $\tau$ and nonnegative integers $a_{i,j} (1 \leq i \leq r; 1 \leq j \leq 2)$. For each prime power $q \geq q_0(\tau)$, let $T_q$ be an operator of type $\tau$ defined over some $\mathbb{F}_q$ vector space. Then the quantity

$$\left|[(a_{1,1},a_{1,2}),\ldots,(a_{r,1},a_{r,2})]_{T_q}\right|$$

depends solely on $q$ and is in fact a polynomial in $q$ for $q \geq q_0(\tau)$.

*Proof.* As the $q$-binomial coefficients are polynomials in $q$, it suffices to show that the base cases

$$|[(a_1,a_1),\ldots,(a_r,a_r)]|$$

in the recursion of Lemma 2.1.6 coincide for each operator of type $\tau$ over $\mathbb{F}_q$ and are polynomials in $q$. Given an operator $T$, define

$$\phi(a_1,\ldots,a_r;T) := |[(a_1,a_1),\ldots,(a_r,a_r)]_T|.$$

We first prove the result when $\tau$ is primary by induction on $r$. Suppose $\tau = \{(d, \lambda)\}$ for some partition $\lambda$ and let $T$ be an operator of type $\tau$. The base case is $r = 1$. Now $\phi(a_1; T)$ is the number of $T$-invariant subspaces of dimension $a_1$. It follows from the work of Fripertinger [14, Thm. 2] that the number of invariant subspaces of a given dimension for operators of a fixed primary similarity class type on an $\mathbb{F}_q$-vector space is a rational function of $q$. Such a function is necessarily a polynomial in $q$ since it takes integer values at infinitely many integers [10, Prop. X.1.1]. This settles the base case.

For the inductive step, let $\tau$ be a primary similarity class type and suppose $r > 1$. Let $a_1, \ldots, a_r$ be given. For each prime power $q \geq q_0(\tau)$, let $T_q$ be an operator of type $\tau$ defined over $\mathbb{F}_q$. For each partition $\mu$ whose Young diagram is contained in that of $\lambda$ (denoted $\mu \subseteq \lambda$), let $g_q(\lambda, \mu, d)$ denote the number of $T_q$-invariant subspaces $W$ for which the similarity class type of the restriction of $T_q$ to $W$ is $\{(d, \mu)\}$. For $\lambda$ and $\mu$ fixed, the quantity $g_q(\lambda, \mu, d)$ is independent of the choice of the operator over $\mathbb{F}_q$ and is a rational function of $q^d$ [14, Thm. 1] and, therefore, a polynomial in $q$. For each positive integer $k$, define

$$D_\tau(k) := \{\mu : \mu \subseteq \lambda \text{ and } |\mu| = k/d\},$$

and set $\delta_\tau(k) = |D_\tau(k)|$. If we write $D_\tau(a_1) = \{\mu_i\}_{1 \leq i \leq \delta_\tau(a_1)}$ then, by considering restrictions of $T_q$ to invariant subspaces of dimension $a_1$, it follows that

$$\phi(a_1, \ldots, a_r; T_q) = \sum_{j=1}^{\delta_\tau(a_1)} g_q(\lambda, \mu_j, d)\ \phi(a_2, \ldots, a_r; T_q^{(j)}),$$

where $T_q^{(j)}$ is a primary operator of similarity class type $\{(d, \mu_j)\}$ for each $j \leq \delta_\tau(a_1)$. Moreover, the partitions $\mu_j$ are uniquely determined by $\tau = \{(d, \lambda)\}$. By the inductive hypothesis, each $\phi(a_2, \ldots, a_r; T_q^{(j)})$ depends only on $q$ and is a polynomial in $q$ for $q \geq q_0(\tau)$. Therefore $\phi(a_1, \ldots, a_r; T_q)$ is a polynomial in $q$ too, proving our claim for primary similarity class types. Thus we may assign an obvious meaning to $\phi_q(a_1, \ldots, a_r; \tau)$ for each primary similarity class type $\tau$ and $\phi_q(a_1, \ldots, a_r; \tau)$ is a polynomial in $q$ for a given type $\tau$.

Now suppose $\tau$ is an arbitrary similarity class type and let $q \geq q_0(\tau)$ be a prime power. Let $T(= T_q)$ be an operator of similarity class type $\tau$ defined on some vector space $V$ over $\mathbb{F}_q$. Let $V = V_1 \oplus \cdots \oplus V_s$ denote the decomposition of $V$ into primary parts $V_i$ with $\dim V_i = d_i$ for each $i$. Suppose $T_i$ denotes the restriction of $T$ to $V_i$ for $1 \leq i \leq s$. Given any flag $W_1 \supseteq \cdots \supseteq W_r$ of $T$-invariant subspaces with $\dim W_i = a_i$, write $W_i = U_{i1} \oplus \cdots \oplus U_{is}$ with $U_{ij} \subseteq V_j$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. If $\dim U_{ij} = d_{ij}$, then it follows that

$$a_i = \sum_{j=1}^{s} d_{ij} \ (1 \leq i \leq r) \quad \text{and} \quad d_j \geq d_{1j} \geq \cdots \geq d_{rj} \ (1 \leq j \leq s).$$

Counting flags within the primary parts and summing up, we obtain

$$\phi(a_1, \ldots, a_r; T_q) = \sum_{\substack{\sum_{j=1}^{s} d_{ij} = a_i \\ d_{1j} \leq d_j}} \prod_{j=1}^{s} \phi(d_{1j}, \ldots, d_{rj}; T_j),$$

where the $d_{ij}$'s vary over nonnegative integers. If $\tau_j$ denotes the similarity class type of $T_j (1 \leq j \leq s)$, then the $\tau_j$'s as well as the $d_j$'s and $d_{ij}$'s are determined uniquely by $\tau$. Moreover, since the $\tau_j$'s are primary, it follows that

$$\phi(a_1, \ldots, a_r; T_q) = \sum_{\substack{\sum_{j=1}^{s} d_{ij} = a_i \\ d_{1j} \leq d_j}} \prod_{j=1}^{s} \phi_q(d_{1j}, \ldots, d_{rj}; \tau_j),$$

whenever $q \geq q_0(\tau)$. The theorem now follows since each $\phi_q(d_{1j}, \ldots, d_{rj}; \tau_j)$ is a polynomial in $q$. □

**Remark 2.2.4.** Delsarte [13] proved that the number of subgroups of type $\mu$ in a finite abelian $p$-group of type $\lambda$, denoted $\alpha_\lambda(\mu; p)$ is a polynomial in $p$. We refer to the expository account of Butler [9, Lem. 1.4.1] for the details. It can be shown that the expression $g_q(\lambda, \mu, d)$ defined above may be recovered from $\alpha_\lambda(\mu; p)$ by replacing $p$ by $q^d$.

**Corollary 2.2.5.** 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 $\sigma(m, d; T) = \sigma(m, d; T')$.

*Proof.* The result follows from Theorem 2.2.3 and Proposition 2.1.7. □

For another proof of Corollary 2.2.5 using lattice theory, see Appendix A.

**Corollary 2.2.6.** Let $T$ be a linear operator on an $md$-dimensional vector space $V$ over $\mathbb{F}_q$ and suppose $c \in \mathbb{F}_q$. If $I$ denotes the identity on $V$, then $\sigma(m, d; T) = \sigma(m, d; T + cI)$.

*Proof.* This follows from Corollary 2.2.5 as $T$ and $T+cI$ have the same similarity class type. □

**Definition 2.2.7.** If $\tau$ is a similarity class type of size $md$ and $q \geq q_0(\tau)$, then $\sigma(m, d; \tau)$ denotes the number of $m$-dimensional splitting subspaces for a linear operator of similarity class type $\tau$ defined over an $\mathbb{F}_q$-vector space of dimension $md$.

By Corollary 2.2.5, the quantity $\sigma(m, d; \tau)$ is well-defined.

**Corollary 2.2.8.** If $m, d, \tau$ are fixed, then $\sigma(m, d; \tau)$ is a polynomial in $q$.

*Proof.* Follows from Theorem 2.2.3 and Proposition 2.1.7. □

The values of $\sigma(m, d; \tau)$ for $m = 2$ and $d = 2$ are shown in Figure 2.1.

## 2.3 Cyclic nilpotent operators

In this section, we determine the number of splitting subspaces of a cyclic nilpotent operator by guessing a formula that satisfies the recursion in Lemma 2.1.6. The following proposition will prove useful in the computation of base cases.

**Proposition 2.3.1.** [8, Lem. 2] Let $T$ be a cyclic $p$-primary operator on a vector space $U$ of dimension $ad$ where $d = \deg p$. Then the lattice of invariant subspaces of $T$ is given by

$$L(T) = \left\{ \ker\ p(T)^j : 0 \leq j \leq a \right\}.$$

| $\tau$ | $\sigma(2,2;\tau)$ |
|---|---|
| {(1, 1), (1, 1), (1, 1), (1, 1)} | $q \cdot (q+2) \cdot (q-1)^2$ |
| {(1, 1), (1, 1), (1, 2)} | $(q-1) \cdot q \cdot (q^2+q-1)$ |
| {(1, 1), (1, 1), (1, 11)} | $q \cdot (q+1) \cdot (q-1)^2$ |
| {(1, 1), (1, 1), (2, 1)} | $(q-1) \cdot (q+1) \cdot q^2$ |
| {(1, 1), (1, 3)} | $(q-1) \cdot (q+1) \cdot q^2$ |
| {(1, 1), (1, 21)} | $(q-1) \cdot q^3$ |
| {(1, 1), (1, 111)} | $0$ |
| {(1, 1), (3, 1)} | $(q-1) \cdot q \cdot (q^2+q+1)$ |
| {(1, 2), (1, 2)} | $q \cdot (q^3-q+1)$ |
| {(1, 11), (1, 2)} | $q \cdot (q+1) \cdot (q-1)^2$ |
| {(1, 2), (2, 1)} | $q \cdot (q+1) \cdot (q^2-q+1)$ |
| {(1, 11), (1, 11)} | $q \cdot (q+1) \cdot (q-1)^2$ |
| {(1, 11), (2, 1)} | $q \cdot (q+1) \cdot (q-1)^2$ |
| {(2, 1), (2, 1)} | $q \cdot (q+1) \cdot (q^2-q+2)$ |
| {(1, 4)} | $q^4$ |
| {(1, 31)} | $(q-1) \cdot q^3$ |
| {(1, 22)} | $q^4$ |
| {(1, 211)} | $0$ |
| {(1, 1111)} | $0$ |
| {(2, 2)} | $q \cdot (q^3+q+1)$ |
| {(2, 11)} | $q \cdot (q+1) \cdot (q^2+1)$ |
| {(4, 1)} | $q^2 \cdot (q^2+1)$ |

Figure 2.1: $\sigma(2,2;\tau)$ as a polynomial in $q$.

Suppose $T$ is a cyclic nilpotent operator on $V$ and $\dim V = N$. By Proposition 2.3.1, there is precisely one $T$-invariant subspace of dimension $k$ for each integer $0 \leq k \leq \dim V$, namely, the kernel of $T^k$. As restrictions of cyclic operators to invariant subspaces are cyclic as well, it follows that

$$|[(a_1, a_1), (a_2, a_2), \ldots, (a_r, a_r)]_T| = 1 \qquad (N \geq a_1 \geq a_2 \geq \ldots \geq a_r \geq 0).$$

We require a few lemmas before we proceed to solve the recursion. In what follows, the notation $\sum_s$ signifies a sum taken as $s$ varies over all integers with the convention that the $q$-binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is zero whenever either $n$ or $k$ is negative, or when $k$ does not lie between 0 and $n$.

**Lemma 2.3.2.** [1, p. 42] For integers $a, b, c$, we have

$$\begin{bmatrix} a \\ b \end{bmatrix}_q \begin{bmatrix} b \\ c \end{bmatrix}_q = \begin{bmatrix} a \\ c \end{bmatrix}_q \begin{bmatrix} a-c \\ b-c \end{bmatrix}_q.$$

**Lemma 2.3.3.** For nonnegative integers $a, b, r$, the $q$-Vandermonde identity [2, Thm. 3.4] holds:

$$\begin{bmatrix} a+b \\ r \end{bmatrix}_q = \sum_s \begin{bmatrix} a \\ s \end{bmatrix}_q \begin{bmatrix} b \\ r-s \end{bmatrix}_q q^{s(b-r+s)}.$$

**Lemma 2.3.4.** For nonnegative integers $a \geq d \geq b \geq c$, we have

$$\sum_s \begin{bmatrix} a-b \\ b-s \end{bmatrix}_q \begin{bmatrix} b-c \\ s-c \end{bmatrix}_q \begin{bmatrix} a-2b+s \\ d-2b+s \end{bmatrix}_q q^{(b-s)^2} = \begin{bmatrix} a-b \\ d-b \end{bmatrix}_q \begin{bmatrix} d-c \\ b-c \end{bmatrix}_q.$$

*Proof.* By the $q$-Vandermonde identity,

$$\sum_s \begin{bmatrix} d \\ d-s \end{bmatrix}_q \begin{bmatrix} b-c \\ s \end{bmatrix}_q q^{s^2} = \begin{bmatrix} d+b-c \\ d \end{bmatrix}_q.$$
$$\therefore \sum_s \begin{bmatrix} a \\ d \end{bmatrix}_q \begin{bmatrix} d \\ s \end{bmatrix}_q \begin{bmatrix} b-c \\ s \end{bmatrix}_q q^{s^2} = \begin{bmatrix} a \\ d \end{bmatrix}_q \begin{bmatrix} d+b-c \\ d \end{bmatrix}_q.$$

Now apply Lemma 2.3.2 and replace $s$ by $b-s$ to obtain

$$\sum_s \begin{bmatrix} a \\ s \end{bmatrix}_q \begin{bmatrix} a-s \\ d-s \end{bmatrix}_q \begin{bmatrix} b-c \\ s \end{bmatrix}_q q^{s^2} = \begin{bmatrix} a \\ d \end{bmatrix}_q \begin{bmatrix} d+b-c \\ d \end{bmatrix}_q.$$

$$\therefore \sum_s \begin{bmatrix} a \\ b-s \end{bmatrix}_q \begin{bmatrix} a-b+s \\ d-b+s \end{bmatrix}_q \begin{bmatrix} b-c \\ s-c \end{bmatrix}_q q^{(b-s)^2} = \begin{bmatrix} a \\ d \end{bmatrix}_q \begin{bmatrix} d+b-c \\ d \end{bmatrix}_q.$$

Replacing $a$ by $a-b$ and $d$ by $d-b$ results in the statement of the lemma. □

**Lemma 2.3.5.** For nonnegative integers $a \geq b \geq d \geq c$,

$$\sum_s \begin{bmatrix} a-b \\ b-s \end{bmatrix}_q \begin{bmatrix} b-c \\ s-c \end{bmatrix}_q \begin{bmatrix} s-c \\ d-c \end{bmatrix}_q q^{(b-s)^2} = \begin{bmatrix} b-c \\ d-c \end{bmatrix}_q \begin{bmatrix} a-d \\ b-d \end{bmatrix}_q.$$

*Proof.* By the $q$-Vandermonde identity, we have

$$\sum_s \begin{bmatrix} a-b \\ b-s \end{bmatrix}_q \begin{bmatrix} b-d \\ s-d \end{bmatrix}_q q^{(b-s)^2} = \begin{bmatrix} a-d \\ b-d \end{bmatrix}_q.$$
$$\therefore \sum_s \begin{bmatrix} a-b \\ b-s \end{bmatrix}_q \begin{bmatrix} b-c \\ d-c \end{bmatrix}_q \begin{bmatrix} b-d \\ s-d \end{bmatrix}_q q^{(b-s)^2} = \begin{bmatrix} b-c \\ d-c \end{bmatrix}_q \begin{bmatrix} a-d \\ b-d \end{bmatrix}_q.$$

The result follows from Lemma 2.3.2 since

$$\begin{bmatrix} b-c \\ d-c \end{bmatrix}_q \begin{bmatrix} b-d \\ s-d \end{bmatrix}_q = \begin{bmatrix} b-c \\ s-c \end{bmatrix}_q \begin{bmatrix} s-c \\ d-c \end{bmatrix}_q.$$ □

We now solve the recursion stated in Lemma 2.1.6 for a cyclic nilpotent operator.

**Theorem 2.3.6.** Let $T$ be a cyclic nilpotent operator on $V$ with $\dim V = N$ and suppose

$$N \geq a_{1,1} \geq a_{1,2} \geq a_{2,1} \geq a_{2,2} \geq \cdots \geq a_{r,1} \geq a_{r,2} \geq 0,$$
$$a_{0,1} = a_{0,2} = N, \quad a_{r+1,1} = a_{r+1,2} = 0.$$

Then

$$|[(a_{1,1}, a_{1,2}), \ldots, (a_{r,1}, a_{r,2})]| = \prod_{i=1}^{r} \begin{bmatrix} a_{i-1,1} - a_{i,1} \\ a_{i,1} - a_{i,2} \end{bmatrix}_q \begin{bmatrix} a_{i,1} - a_{i+1,1} \\ a_{i,2} - a_{i+1,1} \end{bmatrix}_q q^{(a_{i,1}-a_{i,2})^2}. \tag{2.1}$$

*Proof.* We show that the formula stated above satisfies the recursion of Lemma 2.1.6 by computing separately the sums over the sets $A$ and $B$ defined

there. Substitute the expression for $|[(a_{1,1},a_{1,2}),\ldots,(a_{r,1},a_{r,2})]|$ given by (2.1) into the recursion to obtain

$$\begin{aligned} L &= \sum_{(j_1,\ldots,j_r)\in A} |[(a_{1,2},j_1),(a_{2,2},j_2),\ldots,(a_{r,2},j_r)]| \prod_{i=1}^{r} \begin{bmatrix} a_{i-1,2}-(2a_{i,2}-j_i) \\ a_{i,1}-(2a_{i,2}-j_i) \end{bmatrix}_q \\ &= \prod_{i=1}^{r} \sum_{j_i} \begin{bmatrix} a_{i-1,2}-a_{i,2} \\ a_{i,2}-j_i \end{bmatrix}_q \begin{bmatrix} a_{i,2}-a_{i+1,2} \\ j_i-a_{i+1,2} \end{bmatrix}_q \begin{bmatrix} a_{i-1,2}-(2a_{i,2}-j_i) \\ a_{i,1}-(2a_{i,2}-j_i) \end{bmatrix}_q q^{(a_{i,2}-j_i)^2}. \end{aligned}$$

Apply Lemma 2.3.4 to each sum in the above expression, followed by Lemma 2.3.2 to obtain

$$\begin{aligned} L = \prod_{i=1}^{r} \begin{bmatrix} a_{i-1,2}-a_{i,2} \\ a_{i,1}-a_{i,2} \end{bmatrix}_q \begin{bmatrix} a_{i,1}-a_{i+1,2} \\ a_{i,2}-a_{i+1,2} \end{bmatrix}_q &= \prod_{i=1}^{r} \frac{\begin{bmatrix} a_{i-1,2} \\ a_{i,1} \end{bmatrix}_q \begin{bmatrix} a_{i,1} \\ a_{i,2} \end{bmatrix}_q}{\begin{bmatrix} a_{i-1,2} \\ a_{i,2} \end{bmatrix}_q} \frac{\begin{bmatrix} a_{i,1} \\ a_{i,2} \end{bmatrix}_q \begin{bmatrix} a_{i,2} \\ a_{i+1,2} \end{bmatrix}_q}{\begin{bmatrix} a_{i,1} \\ a_{i+1,2} \end{bmatrix}_q} \\ &= \frac{1}{\begin{bmatrix} N \\ a_{1,2} \end{bmatrix}_q} \prod_{i=1}^{r} \frac{\begin{bmatrix} a_{i,1} \\ a_{i,2} \end{bmatrix}_q^2 \begin{bmatrix} a_{i-1,2} \\ a_{i,1} \end{bmatrix}_q}{\begin{bmatrix} a_{i,1} \\ a_{i+1,2} \end{bmatrix}_q}. \end{aligned}$$

On the other hand,

$$\begin{aligned} R &= \sum_{(k_1,\ldots,k_r)\in B} |[(a_{1,1},k_1),(a_{2,1},k_2),\ldots,(a_{r,1},k_r)]| \prod_{i=1}^{r} \begin{bmatrix} k_i-a_{i+1,1} \\ a_{i,2}-a_{i+1,1} \end{bmatrix}_q \\ &= \prod_{i=1}^{r} \sum_{k_i} \begin{bmatrix} a_{i-1,1}-a_{i,1} \\ a_{i,1}-k_i \end{bmatrix}_q \begin{bmatrix} a_{i,1}-a_{i+1,1} \\ k_i-a_{i+1,1} \end{bmatrix}_q \begin{bmatrix} k_i-a_{i+1,1} \\ a_{i,2}-a_{i+1,1} \end{bmatrix}_q q^{(a_{i,1}-k_i)^2}. \end{aligned}$$

Apply Lemma 2.3.5 to each sum in the above expression, followed by Lemma 2.3.2 to obtain

$$\begin{aligned} R = \prod_{i=1}^{r} \begin{bmatrix} a_{i,1}-a_{i+1,1} \\ a_{i,2}-a_{i+1,1} \end{bmatrix}_q \begin{bmatrix} a_{i-1,1}-a_{i,2} \\ a_{i,1}-a_{i,2} \end{bmatrix}_q &= \prod_{i=1}^{r} \frac{\begin{bmatrix} a_{i,1} \\ a_{i,2} \end{bmatrix}_q \begin{bmatrix} a_{i,2} \\ a_{i+1,1} \end{bmatrix}_q}{\begin{bmatrix} a_{i,1} \\ a_{i+1,1} \end{bmatrix}_q} \frac{\begin{bmatrix} a_{i-1,1} \\ a_{i,1} \end{bmatrix}_q \begin{bmatrix} a_{i,1} \\ a_{i,2} \end{bmatrix}_q}{\begin{bmatrix} a_{i-1,1} \\ a_{i,2} \end{bmatrix}_q} \\ &= \begin{bmatrix} N \\ a_{1,1} \end{bmatrix}_q \prod_{i=1}^{r} \frac{\begin{bmatrix} a_{i,1} \\ a_{i,2} \end{bmatrix}_q^2 \begin{bmatrix} a_{i,2} \\ a_{i+1,1} \end{bmatrix}_q}{\begin{bmatrix} a_{i-1,1} \\ a_{i,2} \end{bmatrix}_q}. \end{aligned}$$

Therefore

$$\frac{L}{R} = \frac{1}{\begin{bmatrix} N \\ a_{1,2} \end{bmatrix}_q \begin{bmatrix} N \\ a_{1,1} \end{bmatrix}_q} \begin{bmatrix} N \\ a_{1,1} \end{bmatrix}_q \begin{bmatrix} N \\ a_{1,2} \end{bmatrix}_q = 1.$$

Hence $L = R$, proving that the given expression satisfies the recurrence. The expression in (2.1) satisfies the base cases since

$$\begin{aligned}|[(a_1,a_1),(a_2,a_2),\ldots,(a_r,a_r)]| &= \prod_{i=1}^{r} \begin{bmatrix} a_{i-1}-a_i \\ 0 \end{bmatrix}_q \begin{bmatrix} a_i - a_{i+1} \\ a_i - a_{i+1} \end{bmatrix}_q q^{(a_i-a_i)^2} \\ &= 1.\end{aligned}$$

This completes the proof. □

The following result gives the number of splitting subspaces for cyclic nilpotent operators.

**Corollary 2.3.7.** When $N \geq md$, we have the equality

$$|[((d-1)m,(d-2)m),\ldots,(2m,m),(m,0)]| = \begin{bmatrix} N-md+m \\ m \end{bmatrix}_q q^{m^2(d-1)}.$$

In particular, when $N = md$,

$$|[((d-1)m,(d-2)m),\ldots,(2m,m),(m,0)]| = q^{m^2(d-1)}.$$

*Proof.* By Theorem 2.3.6, we have

$$\begin{aligned}&|[((d-1)m,(d-2)m),((d-2)m,(d-3)m),\ldots,(2m,m),(m,0)]| \\ &= \begin{bmatrix} N-(d-1)m \\ m \end{bmatrix}_q q^{m^2} \prod_{i=2}^{d-1} \left( \begin{bmatrix} m \\ m \end{bmatrix}_q \begin{bmatrix} m \\ 0 \end{bmatrix}_q q^{m^2} \right) \\ &= \begin{bmatrix} N-md+m \\ m \end{bmatrix}_q q^{m^2(d-1)}.\end{aligned}$$

□

Note that for $d = 1$ the final expression above reduces to $\begin{bmatrix} N \\ m \end{bmatrix}_q$ which is simply the total number of $m$-dimensional subspaces of an $N$-dimensional vector space over $\mathbb{F}_q$. Combining the above corollary with Corollary 2.2.6, we obtain the following result.

**Corollary 2.3.8.** Let $T$ be a linear operator on an $md$-dimensional vector space over $\mathbb{F}_q$. If $T$ is cyclic and $p$-primary for some linear polynomial $p$, then $\sigma(m,d;T) = q^{m^2(d-1)}$.

**Remark 2.3.9.** One of the main results of Chen and Tseng [11, Cor. 3.4] is the computation of $\sigma(m, d; T)$ when the similarity class type of $T$ is $\{(md, (1))\}$. The above corollary corresponds to the similarity class type $\{(1, (md))\}$.

Our results may be used to enumerate invertible matrices of a special form. Recall that the number of ordered bases for an $m$-dimensional vector space over $\mathbb{F}_q$ is given by $\gamma_q(m) := (q^m - 1)\dots(q^m - q^{m-1})$.

**Corollary 2.3.10.** The number of invertible $md \times md$ matrices over $\mathbb{F}_q$ of the form

$$\begin{bmatrix}
a_{1,1} & \cdots & a_{1,m} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
a_{2,1} & \cdots & a_{2,m} & a_{1,1} & \cdots & a_{1,m} & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
a_{d,1} & \cdots & a_{d,m} & a_{d-1,1} & \cdots & a_{d-1,m} & \cdots & a_{1,1} & \cdots & a_{1,m} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
a_{md,1} & \cdots & a_{md,m} & a_{md-1,1} & \cdots & a_{md-1,m} & \cdots & a_{md-d+1,1} & \cdots & a_{md-d+1,m}
\end{bmatrix} \tag{2.2}$$

equals $\gamma_q(m) \cdot q^{m^2(d-1)}$.

*Proof.* Let $V = \mathbb{F}_q^{md}$ viewed as a vector space over $\mathbb{F}_q$. Let $T$ denote the right shift operator $T(x_1, \dots, x_{md}) = (0, x_1, \dots, x_{md-1})$. Then $T$ is cyclic and nilpotent. If $\alpha_1, \dots, \alpha_m$ denote the first $m$ columns of the matrix (2.2) above, then the matrix is nonsingular if and only if the set

$$\{\alpha_1, \dots, \alpha_m, T\alpha_1, \dots, T\alpha_m, \dots, T^{d-1}\alpha_1, \dots, T^{d-1}\alpha_m\}$$

is linearly independent. In other words $\{\alpha_1, \dots, \alpha_m\}$ may be characterized as an ordered basis for some $m$-dimensional $T$-splitting subspace. Since number of such bases is $\gamma_q(m) \cdot \sigma(m, d; T)$, the result now follows from Corollary 2.3.8. □

A result in a similar vein to the above corollary is proved by Gluesing-Luerssen and Ravagnani [20, Cor. 7.2] who find an expression for the number of nonsingular matrices over $\mathbb{F}_q$ whose nonzero entries lie within a Ferrers shape.

# Chapter 3

# Polynomial matrices and splitting subspaces over finite fields

In this chapter, we obtain an existence criterion for splitting subspaces and give precise formulae for the number of splitting subspaces for operators whose invariant factors satisfy certain degree conditions.

The chapter is organized as follows. In Section 3.1, we obtain an existence criterion for splitting subspaces using the result of Knüppel and Nielsen [25] on anti-invariant subspaces and discuss the connection between Krylov subspaces and splitting subspaces. In Section 3.2, we show an equivalence between the problem of counting polynomial matrices (see Section 1.2) when $n = k$ and the problem of determination of $\sigma(m, d; T)$. We also prove a formula for the number of splitting subspaces for operators whose smallest invariant factor has degree $d$. In Section 3.3, we give a formula for $\sigma(m, d; T)$ for all operators $T$ whose smallest invariant factor has degree $d - 1$.

## 3.1 Existence of splitting subspaces

Recall from Section 1.2, a $k$-tuple of invariant factors is a $k$-tuple $\mathcal{I} = (f_1, \ldots, f_k)$ where each $f_i$ is a monic polynomial over $\mathbb{F}_q$ such that

$f_i \mid f_{i+1}$ for $1 \leq i \leq k-1$. For any $k$-tuple of invariant factors $\mathcal{I} = (p_1, \ldots, p_k)$, define

$$\deg \mathcal{I} := \deg(p_1 \cdots p_k).$$

By Proposition 2.2.2, the number of splitting subspaces $\sigma(m, d; T)$ depends only on the similarity class of $T$. Here is a precise definition.

**Definition 3.1.1.** Let $\mathcal{I}$ be an $md$-tuple of invariant factors with $\deg \mathcal{I} = md$. Then

$$\sigma(m, d; \mathcal{I}) := \sigma(m, d; T),$$

where $T$ is any linear operator on an $md$-dimensional vector space over $\mathbb{F}_q$ with invariant factors $\mathcal{I}$.

More generally, by Corollary 2.2.5, we know that the number of splitting subspaces $\sigma(m, d; T)$ depends only on the similarity class type of $T$. In other words, whenever there exists a linear transformation over $\mathbb{F}_q$ of similarity class type $\tau$, one can define

$$\sigma(m, d; \tau) := \sigma(m, d; T),$$

where $T$ is any linear operator of type $\tau$ defined on an $md$-dimensional vector space over $\mathbb{F}_q$. For our purposes it will be more convenient to work with $\sigma(m, d; \mathcal{I})$ but it is worth emphasizing that all results involving $\sigma(m, d; \mathcal{I})$ may be reformulated in terms of similarity class type and we will include such examples.

Splitting subspaces are closely related to anti-invariant subspaces.

**Definition 3.1.2.** Given a non-negative integer $\ell$, a subspace $W$ of $V$ is called *$\ell$-fold $T$-anti-invariant* if

$$\dim(W + TW + \cdots + T^{\ell}W) = (\ell + 1) \cdot \dim W.$$

If $\dim V = md$, then every $m$-dimensional $T$-splitting subspace is $(d-1)$-fold $T$-anti-invariant. Barría and Halmos [4] and Sourour [44] studied 1-fold anti-invariant subspaces and determined the maximum possible dimension of

such a subspace. Knüppel and Nielsen (2003) extended their work to $\ell$-fold anti-invariant subspaces for arbitrary $\ell$. In particular, they gave the following existence criterion.

**Proposition 3.1.3.** [25, Cor. 2.2] Let $T$ be a linear operator on an $N$-dimensional vector space over $\mathbb{F}_q$ where $N = (\ell+1)m$. Suppose $(p_1, \ldots, p_N)$ is the $N$-tuple of invariant factors of $T$. Then an $\ell$-fold $T$-anti-invariant subspace of dimension $m$ exists if and only if $p_i = 1$ for $1 \leq i \leq \ell m$.

It is important to note that [25, Cor. 2.2] is stated only for invertible operators. However, the proof [25, Lem 3.1, Lem 3.2] does not require the hypothesis that $T$ is invertible.

Proposition 3.1.3 yields a criterion for the existence of splitting subspaces.

**Corollary 3.1.4.** Let $\mathcal{I} = (p_1, \ldots, p_{md})$ with $\deg \mathcal{I} = md$. Then $\sigma(m, d; \mathcal{I}) > 0$ if and only if $p_i = 1$ for $1 \leq i \leq m(d-1)$.

**Corollary 3.1.5.** If $\tau = \{(d_1, \lambda_1), \ldots, (d_t, \lambda_t)\}$, then $\sigma(m, d; \tau) > 0$ if and only if each partition $\lambda_i (1 \leq i \leq t)$ has at most $m$ parts.

Recall the probability

$$\kappa_{m,d}(T) := \frac{1}{q^{Nm}} |\{(v_1, \ldots, v_m) \in V^m : \mathrm{Kry}(T, \{v_1, \ldots, v_m\}; d) = V\}|$$

defined in Section 1.1. The next proposition gives the connection between $\kappa_{m,d}(T)$ and $\sigma(m, d; T)$. In what follows we will denote the order of the general linear group $\mathrm{GL}_m(\mathbb{F}_q)$ by $\gamma_q(m) = (q^m - 1)(q^m - q) \ldots (q^m - q^{m-1})$.

**Proposition 3.1.6.** Let $T$ be a linear operator on an $md$-dimensional vector space over $\mathbb{F}_q$. Then

$$\kappa_{m,d}(T) = \frac{\gamma_q(m) \cdot \sigma(m, d; T)}{q^{m^2 d}}.$$

*Proof.* Let $S = \{v_1, \ldots, v_m\} \subseteq V$. By the definition of truncated Krylov subspace, we have $\mathrm{Kry}(T, S; d) = V$ if and only if $W = \mathrm{span}(S)$ is an $m$ dimensional $T$-splitting subspace. Since each $m$-dimensional subspace has precisely $\gamma_q(m)$ ordered bases, the proposition follows. □

## 3.2 Splitting subspaces and polynomial matrices

In this section we show that $\sigma(m,d;\mathcal{I})$ may be recovered from $\mu_q(m,m,d;\mathcal{I})$, where $\mu_q$ is as defined in Section 1.2. We begin with the following lemma concerning the equivalence of matrices.

**Lemma 3.2.1.** [21, Thm. 1.1] Let $P = x^dI + x^{d-1}C_{d-1} + \cdots + C_0 \in \mathrm{M}_q(m,m,d)$. Consider the $md \times md$ block matrix

$$A = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & -C_0 \\ I & \mathbf{0} & \dots & \mathbf{0} & -C_1 \\ \mathbf{0} & I & \dots & \mathbf{0} & -C_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & I & -C_{d-1} \end{bmatrix}.$$

Then

$$xI - A \sim \begin{bmatrix} I & \mathbf{0} \\ \mathbf{0} & P \end{bmatrix},$$

where $I$ and $\mathbf{0}$ denote the identity and zero matrices of appropriate sizes. In particular, if $P$ has invariant factors $(p_1,\dots,p_m)$, then $xI - A$ has invariant factors $(1,\dots,1,p_1,\dots,p_m)$.

Given $\mathcal{I} = (p_1,\dots,p_m)$, the above lemma implies that $\mu_q(m,m,d;\mathcal{I})$ is equal to the number of matrices $A$ of the block form above whose invariant factors are $\mathcal{I} = (1,\dots,1,p_1,\dots,p_m)$. In view of Corollary 3.1.4, given any $m$-tuple $\mathcal{I} = (p_1,\dots,p_m)$ we interpret $\sigma(m,d;\mathcal{I})$ to mean $\sigma(m,d;\mathcal{I}')$ where $\mathcal{I}' = (1,\dots,1,p_1,\dots,p_m)$ is the $md$-tuple obtained from $\mathcal{I}$ by padding $m(d-1)$ ones. As a natural extension we will write $c(\mathcal{I})$ to mean $c(\mathcal{I}')$ hereafter.

**Theorem 3.2.2.** Let $\mathcal{I} = (p_1,\dots,p_m)$ be an $m$-tuple of invariant factors with $\deg \mathcal{I} = md$. Then

$$\sigma(m,d;\mathcal{I}) = \frac{c(\mathcal{I})}{\gamma_q(m)}\mu_q(m,m,d;\mathcal{I}).$$

*Proof.* Let $T$ be a linear operator on an $md$-dimensional vector space with in-

variant factors $\mathcal{I}$ and let $W$ be an $m$-dimensional $T$-splitting subspace. Suppose $\mathcal{B}_W = \{v_1, \ldots, v_m\}$ is an ordered basis for $W$. Then an ordered basis for $V$ is given by

$$\mathcal{B}_V = \{v_1, \ldots, v_m, Tv_1, \ldots, Tv_m, \ldots, T^{d-1}v_1, \ldots, T^{d-1}v_m\}.$$

The matrix of $T$ with respect to the basis $\mathcal{B}_V$ has the block form

$$\begin{bmatrix} \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & -C_0 \\ I & \mathbf{0} & \ldots & \mathbf{0} & -C_1 \\ \mathbf{0} & I & \ldots & \mathbf{0} & -C_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & I & -C_{d-1} \end{bmatrix}, \tag{3.1}$$

for some matrices $C_0, C_1, \ldots, C_{d-1} \in \mathrm{M}_m(\mathbb{F}_q)$. Conversely, if $\{\alpha_1, \ldots, \alpha_{md}\}$ is an ordered basis for $V$ with respect to which the matrix of $T$ is in the above block form, then span $\{\alpha_1, \ldots, \alpha_m\}$ forms a $T$-splitting subspace for $V$. Since there are $\sigma(m, d; \mathcal{I})$ splitting subspaces of dimension $m$ and each such subspace has $\gamma_q(m)$ bases, it follows that $V$ has $\sigma(m, d; \mathcal{I}) \cdot \gamma_q(m)$ bases with respect to which the matrix of $T$ has the above block form. Different bases for $V$ may yield the same matrix for $T$. If $A$ denotes the matrix of $T$ with respect to the basis $\mathcal{B}_V$, then the number of different bases $\mathcal{B}$ for $V$ such that the matrix of $T$ with respect to $\mathcal{B}$ is $A$ is precisely

$$|\{P \in \mathrm{GL}_{md}(\mathbb{F}_q) : P^{-1}AP = A\}| = c(\mathcal{I}).$$

By Lemma 3.2.1, $\mu_q(m, m, d; \mathcal{I})$ is equal to the number of matrices of the block form (3.1) whose invariant factors are $\mathcal{I}$. Thus

$$\mu_q(m, m, d; \mathcal{I}) = \frac{\sigma(m, d; \mathcal{I}) \cdot \gamma_q(m)}{c(\mathcal{I})},$$

which proves the theorem. □

**Definition 3.2.3.** Let $P \in \mathrm{M}_q(n, k, d)$ and suppose $1 \leq i \leq k$. The $i^{\text{th}}$ deter-

minantal divisor of $P$, denoted $\delta_i(P)$, is the greatest common divisor of all $i \times i$ minors of $P$.

The invariant factors of $P$ can be recovered from the determinantal divisors; if $P \in \mathrm{M}_q(n,k,d;(p_1,\ldots,p_k))$, then [24, p. 260]

$$p_i = \frac{\delta_i(P)}{\delta_{i-1}(P)} \quad (1 \le i \le k),$$

where $\delta_0(P) = 1$. In what follows, $\mathrm{M}_q(n,k,d;\mathcal{I})$ denotes all elements $P \in \mathrm{M}_q(n,k,d)$ which have invariant factors $\mathcal{I}$. By definition, we have $\mu_q(n,k,d;\mathcal{I}) = |M_q(n,k,d;\mathcal{I})|$.

**Remark 3.2.4.** If $P \in \mathrm{M}_q(n,k,d;\mathcal{I})$, then

$$\deg \mathcal{I} = \deg \prod_{i=1}^{k} p_i = \deg \delta_k(P) \le kd,$$

since the maximum possible degree of a minor of $P$ is precisely $kd$. In view of this degree constraint above we will implicitly assume that $\deg \mathcal{I} \le kd$ whenever $\mu_q(n,k,d;\mathcal{I})$ is considered.

The following reduction lemma will prove very useful.

**Lemma 3.2.5.** We have

$$\mu_q(n,k,d;(p_1,\ldots,p_k)) = \mu_q(n,k,d-d_1;(\tilde{p}_1,\ldots,\tilde{p}_k)),$$

where $d_1 = \deg p_1$ and $\tilde{p}_i = p_i/p_1$ for $1 \le i \le k$.

*Proof.* Let $\mathcal{I} = (p_1,\ldots,p_k)$ and suppose $P \in \mathrm{M}_q(n,k,d;\mathcal{I})$. Since $\delta_1(P) = p_1$, it follows that $P = p_1 \cdot Q$ for some $Q \in \mathrm{M}_q(n,k,d-d_1)$. It is easily seen that $\delta_i(Q) = \delta_i(P)/p_1^i$ for $1 \le i \le k$. Therefore the invariant factors for $Q$ are

$$\left(\frac{p_1}{p_1}, \frac{p_2}{p_1}, \ldots, \frac{p_k}{p_1}\right) = (\tilde{p}_1,\ldots,\tilde{p}_k) = \widetilde{\mathcal{I}}.$$

It follows that the map $\mathrm{M}_q(n,k,d;\mathcal{I}) \to \mathrm{M}_q(n,k,d-d_1;\widetilde{\mathcal{I}})$ defined by $P \mapsto P/p_1$ is a bijection. □

**Corollary 3.2.6.** Let $g$ be a monic polynomial of degree $d$ over $\mathbb{F}_q$ and $\mathcal{I} = (g, \ldots, g)$ be a $k$-tuple of invariant factors. Then

$$\mu_q(n, k, d; \mathcal{I}) = 1.$$

*Proof.* By Lemma 3.2.5, $\mu_q(n, k, d; (g, \ldots, g)) = \mu_q(n, k, 0; (1, \ldots, 1))$ and the corollary follows since $\mu_q(n, k, 0; (1, \ldots, 1)) = 1$ by definition. □

A precise expression for the cardinality of the centralizer in $\mathrm{GL}_n(\mathbb{F}_q)$ of a matrix $A \in \mathrm{M}_n(\mathbb{F}_q)$ is known. As we will require this expression in some calculations, we state it here. Suppose the similarity class of $A$ is given by $\{(\phi_1, \lambda_1), \ldots, (\phi_t, \lambda_t)\}$ for some irreducible polynomials $\phi_i$ and partitions $\lambda_i (1 \leq i \leq t)$. Let the corresponding invariant factors (i.e. those of $xI - A$) be $\mathcal{I} = (p_1, \ldots, p_n)$. For any partition $\lambda$, let $\lambda'$ denote its conjugate partition and let $m_i(\lambda) = \lambda'_i - \lambda'_{i+1}$ denote the number of parts of $\lambda$ of size $i$. Denote by $\langle \lambda, \lambda \rangle$ the sum of squares of the parts of $\lambda$. For an indeterminate $u$ and a non-negative integer $r$, define

$$(u)_r := \prod_{i=1}^{r} (1 - u^i).$$

For any monic irreducible polynomial $\phi$ of degree $d$ and integer partition $\lambda$, let

$$c_d(\lambda) = q^{d\langle \lambda', \lambda' \rangle} \prod_{i \geq 1} \left(q^{-d}\right)_{m_i(\lambda)}.$$

If $d_i = \deg \phi_i$, then the order of the centralizer of $A$ is given by [15, p. 55]

$$c(\mathcal{I}) = \prod_{i=1}^{t} c_{d_i}(\lambda_i). \tag{3.2}$$

For instance, if $\mathcal{I} = (x+1, (x+1)^2)$ then $c(\mathcal{I}) = c_1(2, 1)$. Here, $\lambda = (2, 1), \lambda' = (2, 1), \langle \lambda', \lambda' \rangle = 5, m_1 = 1$, and $m_2 = 1$. Therefore $c_1(2, 1) = q^5(1 - q^{-1})^2$.

**Remark 3.2.7.** Note that the expression for $c(\mathcal{I})$ above involves only the degrees of the polynomials $\phi_i$ and not the polynomials themselves. Thus given

any similarity class type $\tau$, the corresponding centralizer size $c(\tau)$ is given by the product in (3.2).

Corollary 3.2.6 and Theorem 3.2.2 imply a formula for $\sigma(m, d; (p_1, \ldots, p_m))$ in the case where $\deg p_1 = d$. In this case we necessarily have $p_i = p_1$ for each $1 \leq i \leq m$.

**Theorem 3.2.8.** Let $g$ be a monic polynomial of degree $d$ over $\mathbb{F}_q$, and suppose $g = \phi_1^{e_1} \cdots \phi_t^{e_t}$ for distinct irreducible polynomials $\phi_i$ with $\deg \phi_i = d_i$ $(1 \leq i \leq t)$. If $\mathcal{I}$ denotes the $m$-tuple $(g, \ldots, g)$, then

$$\sigma(m, d; \mathcal{I}) = \frac{q^{m^2 d}}{\gamma_q(m)} \prod_{i=1}^{t} \prod_{j=1}^{m} \left(1 - q^{-jd_i}\right).$$

*Proof.* By Corollary 3.2.6, we have $\mu_q(m, m, d, (g, \ldots, g)) = 1$. The conjugacy class data corresponding to $\mathcal{I}$ is $\{(\phi_i, \lambda_i)\}_{1 \leq i \leq t}$ where $\lambda_i$ is the integer partition with $m$ equal parts $e_i$ for each $1 \leq i \leq t$. If $d_i = \deg \phi_i$, then by Theorem 3.2.2 and (3.2), we have

$$\begin{aligned}
\sigma(m, d; \mathcal{I}) = \frac{c(\mathcal{I})}{\gamma_q(m)} &= \frac{\prod_{i=1}^{t} c_{d_i}(\lambda_i)}{\gamma_q(m)} \\
&= \frac{\prod_{i=1}^{t} q^{d_i m^2 e_i} \left(q^{-d_i}\right)_m}{\gamma_q(m)} \\
&= \frac{q^{m^2 \sum d_i e_i}}{\gamma_q(m)} \prod_{i=1}^{t} \left(q^{-d_i}\right)_m,
\end{aligned}$$

and the theorem follows since $\sum d_i e_i = \deg g = d$. □

We may recast Theorem 3.2.8 in terms of similarity class type.

**Theorem 3.2.9.** Let $\tau = \{(d_1, \lambda_1), \ldots, (d_t, \lambda_t)\}$ be a similarity class type of size $md$. If $\sum_{i=1}^{t} d_i \lambda_{i,m} = d$, then

$$\sigma(m, d; \tau) = \frac{q^{m^2 d}}{\gamma_q(m)} \prod_{i=1}^{t} \prod_{j=1}^{m} \left(1 - q^{-jd_i}\right).$$

## 3.3 Splitting subspaces and centralizers

In this section we extend the definition of $c(\mathcal{I})$ to include $k$-tuples of invariant factors $\mathcal{I}$ for which $\deg \mathcal{I}$ is not necessarily equal to $k$ in a natural way. If $\mathcal{I} = (p_1, \ldots, p_k)$ and $\deg \mathcal{I} = \delta > k$, then we set $c(\mathcal{I}) = c(\mathcal{I}')$ where $\mathcal{I}' = (1, \ldots, 1, p_1, \ldots, p_k)$ denotes the $\delta$-tuple obtained by padding $\delta - k$ ones to $\mathcal{I}$. On the other hand, if $\delta < k$, then we set $c(\mathcal{I}) = c(\mathcal{I}')$ where $\mathcal{I}'$ is the $\delta$-tuple $(p_{k-\delta+1}, \ldots, p_k)$. Denote by $\mathbb{I}_q(n, k, d)$ the set of all possible $k$-tuples of invariant factors that arise as the invariant factors of some element $P \in \mathrm{M}_q(n, k, d)$.

For $\mathcal{I} = (p_1, \ldots, p_k)$, the definition of $\mu_q(n, k, d; \mathcal{I})$ states that

$$\mu_q(n, k, 1; \mathcal{I}) = |\left\{A \in \mathrm{M}_{n,k}(\mathbb{F}_q) : xI - A \sim \mathrm{diag}_{n,k}(p_1, \ldots, p_k)\right\}|.$$

A precise formula for $\mu_q(n, k, 1; \mathcal{I})$ was originally given in [38, Thm. 3.8].

**Theorem 3.3.1.** Let $\mathcal{I} \in \mathbb{I}_q(n, k, 1)$ and suppose $\deg \mathcal{I} = \delta$. Then

$$\mu_q(n, k, 1; \mathcal{I}) = \begin{bmatrix} k \\ \delta \end{bmatrix}_q \frac{\gamma_q(\delta)}{c(\mathcal{I})} \prod_{i=\delta+1}^{k} (q^n - q^i),$$

where $\begin{bmatrix} \cdot \\ \cdot \end{bmatrix}_q$ denotes a $q$-binomial coefficient.

The classical result of Philip Hall [46, Thm. 1.10.4] on conjugacy class size in $\mathrm{M}_n(\mathbb{F}_q)$ can be recovered from the above theorem by setting $k = n$; in this case we necessarily have $\delta = n$ and it follows that $\mu_q(n, n, 1; \mathcal{I}) = \gamma_q(n)/c(\mathcal{I})$.

A polynomial matrix $P \in \mathrm{M}_q(n, k, d)$ is said to be *unimodular* if the greatest common divisor of all $k \times k$ minors of $P$ is 1, in other words, if and only if $\delta_k(P) = 1$. This corresponds to the case where all invariant factors of $P$ are equal to 1. For $k < n$, a formula for the number of unimodular matrices in $\mathrm{M}_q(n, k, 1)$ was given by Helmke, Jordan, and Lieb [23, Thm. 1]; this formula may be recovered from Theorem 3.3.1 by setting $\mathcal{I} = (1, \ldots, 1)$.

Theorem 3.3.1 can be used to derive an expression for $\sigma(m, d; \mathcal{I})$ when $\mathcal{I} = (p_1, \ldots, p_m)$ with $\deg p_1 = d - 1$ in terms of centralizers in general linear groups.

**Corollary 3.3.2.** Suppose $\mathcal{I} = (p_1, \ldots, p_k) \in \mathbb{I}_q(n, k, d)$ and $\deg p_1 = d - 1$. Then

$$\mu_q(n, k, d; \mathcal{I}) = \begin{bmatrix} k \\ \delta \end{bmatrix}_q \frac{\gamma_q(\delta)}{c(\widetilde{\mathcal{I}})} \prod_{i=\delta+1}^{k} (q^n - q^i),$$

where $\widetilde{\mathcal{I}} = (\tilde{p}_1, \ldots, \tilde{p}_k)$ with $\tilde{p}_i = p_i/p_1$ and $\delta = \deg \widetilde{\mathcal{I}}$.

*Proof.* By Lemma 3.2.5, we have $\mu_q(n, k, d; \mathcal{I}) = \mu_q(n, k, 1; \widetilde{\mathcal{I}})$. The corollary now follows from Theorem 3.3.1. □

**Corollary 3.3.3.** Suppose $\mathcal{I} = (p_1, \ldots, p_m)$ with $\deg \mathcal{I} = md$ and $\deg p_1 = d - 1$. Then

$$\sigma(m, d; \mathcal{I}) = \frac{c(\mathcal{I})}{c(\widetilde{\mathcal{I}})},$$

where $\widetilde{\mathcal{I}} = (\tilde{p}_1, \ldots, \tilde{p}_m)$ and $\tilde{p}_i = p_i/p_1$ for $1 \leq i \leq m$.

*Proof.* Note that $\deg \widetilde{\mathcal{I}} = \deg \mathcal{I} - m \cdot \deg p_1 = m$. By Theorem 3.2.2, we have

$$\begin{aligned} \sigma(m, d; \mathcal{I}) &= \frac{c(\mathcal{I})}{\gamma_q(m)} \mu_q(m, m, d; \mathcal{I}) \\ &= \frac{c(\mathcal{I})}{\gamma_q(m)} \frac{\gamma_q(m)}{c(\widetilde{\mathcal{I}})}, \end{aligned}$$

where the last step follows from Corollary 3.3.2 by setting $n = m$ and $k = m$. □

By considering types we obtain the following generalization of the above corollary. Recall the definition of $c(\tau)$ from Remark 3.2.7.

**Corollary 3.3.4.** Let $\tau = \{(d_1, \lambda_1), \ldots, (d_t, \lambda_t)\}$ be a similarity class type of size $md$. If $\sum_{i=1}^{t} d_i \lambda_{i,m} = d - 1$, then

$$\sigma(m, d; \tau) = \frac{c(\tau)}{c(\widetilde{\tau})},$$

where $\widetilde{\tau} = \{(d_1, \mu_1), \ldots, (d_t, \mu_t)\}$ and $\mu_i$ is given by $\mu_{i,j} = \lambda_{i,j} - \lambda_{i,m}$ for $1 \leq i \leq t$ and $1 \leq j \leq m$.

Corollary 3.3.4 may be reformulated in a more explicit form as follows.

**Corollary 3.3.5.** Let $\tau = \{(d_1, \lambda_1), \ldots, (d_t, \lambda_t)\}$ be a similarity class type of size $md$. Suppose $\sum_{i=1}^{t} d_i \lambda_{i,m} = d - 1$ and let $m_i$ denote the multiplicity of $\lambda_{i,m}$ as a part of $\lambda_i$ for $1 \leq i \leq t$. Then

$$\sigma(m, d; \tau) = q^{m^2(d-1)} \prod_{i=1}^{t} \prod_{j=1}^{m_i} \left(1 - q^{-jd_i}\right).$$

*Proof.* Continuing with the notation of Corollary 3.3.4, we have

$$\begin{aligned}\sigma(m, d; \tau) = \frac{c(\tau)}{c(\widetilde{\tau})} &= \prod_{i=1}^{t} \frac{c_{d_i}(\lambda_i)}{c_{d_i}(\mu_i)} \\ &= \prod_{i=1}^{t} \frac{q^{d_i \langle \lambda_i', \lambda_i' \rangle} \prod_{j \geq 1} \left(q^{-d_i}\right)_{m_j(\lambda_i)}}{q^{d_i \langle \mu_i', \mu_i' \rangle} \prod_{j \geq 1} \left(q^{-d_i}\right)_{m_j(\mu_i)}}.\end{aligned}$$

Observe that $\lambda_i'$ may be obtained from $\mu_i'$ by adding $\lambda_{i,m}$ new parts, each equal

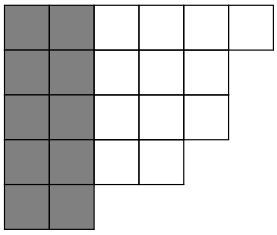

Figure 3.1: If $m = 5$ and $\lambda_i = (6, 5, 5, 4, 2)$, then $\mu_i = (4, 3, 3, 2)$.

to $m$. Therefore, $\langle \lambda_i', \lambda_i' \rangle = m^2 \lambda_{i,m} + \langle \mu_i', \mu_i' \rangle$. If we remove all parts equal to $\lambda_{i,m}$ from $\lambda_i$, then the multiplicities of the remaining parts coincide with the multiplicities of the parts of $\mu_i$. These observations allow us to rewrite the product above as

$$\begin{aligned}\sigma(m, d; \tau) &= \prod_{i=1}^{t} q^{d_i m^2 \lambda_{i,m}} \left(q^{-d_i}\right)_{m_i} \\ &= q^{m^2(d-1)} \prod_{i=1}^{t} \left(q^{-d_i}\right)_{m_i}.\end{aligned}$$

□

We conclude by considering $\mu_q(n, k, d; \mathcal{I})$ for $k = 1$. In this case the problem is equivalent to counting $n$-tuples of coprime monic polynomials of a given degree over a finite field, a question that appears as an exercise in Knuth [26,

Exer. 5 of §4.6.1]. An answer was given by Corteel, Savage, Wilf and Zeilberger [12, Prop. 3] (also see [16, Thm. 4.1]).

**Proposition 3.3.6.** The number of coprime $n$-tuples of monic polynomials of degree $d$ over $\mathbb{F}_q$ is $q^{nd} - q^{n(d-1)+1}$. Equivalently, if $n$ monic polynomials of degree $d$ over $\mathbb{F}_q$ are chosen independently and uniformly at random, then the probability that they are coprime is $1 - 1/q^{n-1}$.

**Corollary 3.3.7.** Let $g \in \mathbb{F}_q[x]$ be a monic polynomial of degree $\delta \leq d$. Then

$$\mu_q(n, 1, d; (g)) = \begin{cases} q^{n(d-\delta)} \left(1 - q^{1-n}\right) & \delta < d, \\ 1 & \delta = d. \end{cases}$$

*Proof.* By Lemma 3.2.5, we have $\mu_q(n, 1, d; (g)) = \mu_q(n, 1, d - \delta; (1))$. If $\delta = d$, then by definition we have $\mu_q(n, 1, d - \delta; (1)) = 1$. If $\delta < d$, then set $d' = d - \delta$ and note that $\mu_q(n, 1, d'; (1))$ equals the number of polynomial matrices

$$\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix} \tag{3.3}$$

such that $\deg g_1 = d'$, $\deg g_i < d'$ for $2 \leq i \leq n$ and $\gcd(g_1, \ldots, g_n) = 1$. Since

$$\gcd(g_1, g_2, \ldots, g_n) = \gcd(g_1, g_2 + g_1 \ldots, g_n + g_1),$$

it follows that $\mu_q(n, 1, d'; (1))$ is equal to the number of coprime $n$-tuples of monic polynomials of degree $d'$. Therefore $\mu_q(n, 1, d'; (1)) = q^{nd'}(1 - q^{1-n})$. □

# Chapter 4

# Conclusion and future work

In Section 4.1, we present a brief review of the literature regarding some recent developments in the splitting subspace problem. We conclude with some future problems for research in Section 4.2.

## 4.1 Subspace profiles

In 2022, Prasad and Ram [33,34] gave a formula for $\sigma(m, d; T)$ when $T$ is a regular diagonalizable operator. Their solution also gave a method of construction of splitting subspaces recursively [33, Thm. 4.17]. In fact, they solved a more general problem, which extended the counting problem on splitting subspaces. It is defined as follows.

**Definition 4.1.1.** Let $T$ be a linear operator on an $n$-dimensional vector space $V$ over $\mathbb{F}_q$. A subspace $W$ of $V$ has $T$-profile $\mu = (\mu_1, \mu_2, \ldots)$ if

$$\dim(W + TW + \cdots + T^{i-1}W) = \mu_1 + \cdots + \mu_i \quad \text{for all} \quad i \geq 1.$$

Denote by $\sigma(\mu; T)$, the number of subspaces with $T$-profile $\mu$. Prasad and Ram asked the following question.

**Problem 4.1.2.** What is the number of subspaces with $T$-profile $\mu$ for an arbitrary linear operator $T$?

The above problem has been studied earlier by Bender, Coley, Robbins, and Rumsey [5]. Prasad and Ram went on to solve Problem 4.1.2 when $\mu$ consists of two parts and $T$ is arbitrary [36]. Here is their precise formula.

**Theorem 4.1.3.** Let $\mu = (m, l)$ such that $n = m + l$. Then

$$\sigma(\mu; T) = q^{\binom{l}{2}} \sum_{j=0}^{l} (-1)^j (X_j^T - X_{j-1}^T) \begin{bmatrix} n-l-j \\ n-2l \end{bmatrix}_q q^{\binom{l-j+1}{2}},$$

where $X_j^T$ is the number of $j$-dimensional $T$-invariant subspaces of $V$.

When $m = l$, the above formula gives an expression for $\sigma(m, 2; T)$ for an arbitrary linear operator $T$. The proof of Theorem 4.1.3 uses a linear algebraic approach where they set up a system of equations and solve them. Their results also give a new proof of the Touchard-Riordan formula, which enumerates chord diagrams according to their number of crossings. When $T$ is regular diagonalizable and $n = 2m$, then [35, p. 2]

$$X_j^T = \binom{2m}{j}.$$

Therefore, in this case,

$$\sigma(m, 2; T) = q^{\binom{m}{2}} \sum_{j=0}^{m} (-1)^j \left[ \binom{2m}{j} - \binom{2m}{j-1} \right] q^{\binom{m-j+1}{2}}.$$

The above sum is the right-hand side of the Touchard-Riordan formula [43],

$$(q-1)^m T_m(q) = \sum_{j=0}^{m} (-1)^j \left[ \binom{2m}{j} - \binom{2m}{j-1} \right] q^{\binom{m-j+1}{2}},$$

where $T_m(q)$ is the polynomial that enumerates chord diagrams on $2m$ points according to their number of crossings [47–49]. Penaud [32] gave a bijective proof, and Read [41] gave a proof using the theory of continued fractions. See Aigner [1, p. 337] for a nice exposition on the Touchard-Riordan formula.

Ram and Schlosser, in 2023, extended the earlier work to diagonalizable operators [40]. They gave a combinatorial formula for $\sigma(\mu; T)$ when $T$ is di-

agonalizable and presented some connections with the theory of symmetric functions. In particular, they expressed the polynomials $T_m(q)$ in terms of $q$-Whittaker functions [17], which are specializations of the Macdonald polynomials [40, Thm. 5.6]. See [30] for an introduction to Macdonald polynomials.

A complete solution to Problem 4.1.2 is given by Ram in [39]. The expression for $\sigma(\mu; T)$ is expressed as a Hall-scalar product of symmetric functions. To state the result, let us recall some basic facts about symmetric functions.

Let $x = (x_1, x_2, \ldots)$ be an infinite set of determinates. A *symmetric function* over a commutative ring $R$ is a formal power series

$$f(x) = \sum_{\alpha} c_\alpha x^\alpha,$$

where the sum runs over all weak compositions $\alpha = (\alpha_1, \alpha_2, \ldots)$, $c_\alpha \in R$, $x^\alpha$ denotes the monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots$, and $f(x_{w(1)}, x_{w(2)}, \ldots) = f(x_1, x_2, \ldots)$ for every permutation $w$ of the positive integers. Given a partition $\lambda = (\lambda_1, \lambda_2, \ldots)$ of $n$, define the *monomial symmetric function* $m_\lambda$ as

$$m_\lambda = \sum_{\alpha} x^\alpha,$$

where $\alpha = (\alpha_1, \alpha_2, \ldots)$ runs over all distinct permutations of the vector $\lambda = (\lambda_1, \lambda_2, \ldots)$. For instance, $m_2 = \sum_i x_i^2$ and $m_{11} = \sum_{i<j} x_i x_j$. The *elementary symmetric function* $e_\lambda$ is defined as

$$e_n = m_{1^n} = \sum_{i_1 < \cdots < i_n} x_{i_1} \cdots x_{i_n} \quad (n \geq 1),$$

where $e_0 = m_\phi = 1$ and

$$e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots, \text{ if } \lambda = (\lambda_1, \lambda_2, \ldots).$$

For example, $e_2 = \sum_{i<j} x_i x_j$. The *complete homogeneous symmetric function*

$h_\lambda$ is defined by the formulas

$$h_n = \sum_{\lambda \vdash n} m_\lambda = \sum_{i_1 \leq \cdots \leq i_n} x_{i_1} \cdots x_{i_n} \quad (n \geq 1) \quad \text{with } h_0 = m_\phi = 1,$$

$$h_\lambda = h_{\lambda_1} h_{\lambda_2} \cdots, \text{ if } \lambda = (\lambda_1, \lambda_2, \ldots).$$

For instance, $h_2 = \sum_i x_i^2 + \sum_{i<j} x_i x_j$. We define the *power sum symmetric function* $p_\lambda$ as follows:

$$p_n = m_n = \sum_i x_i^n \quad (n \geq 1) \quad \text{with } p_0 = m_\phi = 1,$$

$$p_\lambda = p_{\lambda_1} p_{\lambda_2} \cdots, \text{ if } \lambda = (\lambda_1, \lambda_2, \ldots).$$

Symmetric functions are equipped with the Hall-scalar product, denoted by $\langle \cdot, \cdot \rangle$, with respect to which the monomial symmetric function, $m_\lambda$, and the complete homogeneous symmetric function, $h_\lambda$, are dual to each other [29, p. 23], i.e.,

$$\langle m_\lambda, h_\mu \rangle = \delta_{\lambda\mu},$$

where $\delta_{\lambda\mu}$ is the Kronecker delta function. The $q$-Whittaker function $W_\lambda(x; q)$ is a specialization of the Macdonald polynomial. The $q = 0$ and $q = 1$ specializations of the $q$-Whittaker function give us the Schur function (see [45, p. 309] for the definition) and the elementary symmetric function, respectively, as follows:

$$W_\lambda(x; 0) = s_\lambda(x), \qquad W_\lambda(x; 1) = e_{\lambda'}(x).$$

Here $\lambda'$ denotes the conjugate partition to $\lambda$. Let $\widetilde{W}_\lambda(x; q)$ and $P_\lambda(x; q)$ denote the Hall-dual $q$-Whittaker function and the Hall-Littlewood polynomial, respectively. Then

$$\omega P_{\lambda'}(x; q) = \widetilde{W}_\lambda(x; q),$$

where $\omega$ is the involutory automorphism defined on the ring of symmetric func-

tions, with respect to which

$$\omega e_\lambda = h_\lambda, \quad \omega h_\lambda = e_\lambda, \quad \text{and} \quad \omega s_\lambda = s_{\lambda'}.$$

We now define a symmetric function which depends on the operator $T$ and is useful for the main result.

**Definition 4.1.4.** Let $T$ be a linear operator defined on an $n$-dimensional vector space $V$ over $\mathbb{F}_q$ and let $\alpha = (\alpha_1, \ldots, \alpha_r)$ be a weak composition of $n$. We denote by $X_\alpha(T)$, the number of flags

$$(0) = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_r = V$$

of $T$-invariant subspaces such that $\dim(W_i/W_{i-1}) = \alpha_i$ for all $1 \leq i \leq r$.

Define the invariant flag-generating function $F_T(x)$ as follows

$$F_T(x) = \sum_\alpha X_\alpha(T) x^\alpha,$$

where the sum runs over all weak compositions $\alpha$ of $n$ and $x^\alpha$ denotes the product $x_1^{\alpha_1} x_2^{\alpha_2} \ldots$.

For example, when $T$ is an operator with an irreducible characteristic polynomial, then $T$ has only two invariant subspaces: the zero subspace, (0) and the whole space $V$. Consequently, $F_T = p_n$, where $p_n$ is the power-sum symmetric function of degree $n$. If $T$ is a cyclic nilpotent operator on $V$, it has precisely one invariant subspace of dimension $i$ for each $0 \leq i \leq n$. In this case, $F_T = h_n$, the complete homogeneous symmetric function of degree $n$.

The length of a partition $\lambda$ is the number of non-zero parts of $\lambda$. For each partition $\lambda$, let $l(\lambda)$ denote the length of $\lambda$ and $|\lambda|$ denote the size of $\lambda$. Moreover, define $\epsilon_\lambda = (-1)^{|\lambda| - l(\lambda)}$. The following is the main result of [39].

**Theorem 4.1.5.** [39, Thm. 5.3] For every linear operator $T$ on $V$ and every partition $\mu$,

$$\sigma(\mu; T) = \epsilon_{\mu'} q^{\sum_{j \geq 2} \binom{\mu_j}{2}} \langle F_T, \widetilde{W}_\mu(x; q) h_{n-|\mu|} \rangle$$

$$= \epsilon_{\mu'} q^{\sum_{j\geq 2}\binom{\mu_j}{2}} \langle \omega F_T, P_{\mu'}(x;q) e_{n-|\mu|} \rangle. \tag{4.1}$$

Recall the Krylov subspaces defined in Section 1.1. Let $T$ be a linear operator on an $n$-dimensional vector space $V$ over $\mathbb{F}_q$. Let $S = \{v_1, \ldots, v_m\}$ be a set of $m$ vectors in $V$. The *truncated Krylov subspace* of order $d$ generated by $S$ is defined by

$$\mathrm{Kry}(T, S; d) := \left\{ \sum_{i=1}^{m} f_i(T) v_i : f_i(x) \in \mathbb{F}_q[x] \text{ and } \deg f_i < d \right\}.$$

Define

$$\kappa_{m,d}(T) := \frac{1}{q^{nm}} |\{(v_1, \ldots, v_m) \in V^m : \mathrm{Kry}(T, \{v_1, \ldots, v_m\}; d) = V\}|.$$

Krylov subspaces have several applications, as discussed in Section 1.1, and obtaining bounds on $\kappa_{m,d}(T)$ is an important problem for analyzing the efficiency of Krylov-based methods [7, p. 277]. The following theorem provides an expression for $\kappa_{m,d}(T)$ in terms of the Hall-scalar product of the invariant flag-generating function with another symmetric function defined below.

**Theorem 4.1.6.** [39, Thm. 7.1] Let $T$ be a linear operator on $V$. Then $\kappa_{m,d}(T) = \langle F_T, G(n, m, d) \rangle$, where

$$G(n, m, d) = q^{-nm} \sum_{\substack{\mu \vdash n \\ l(\mu) \leq d}} (-1)^{n-\mu_1} (q-1)^{\mu_1} q^{\sum_{j\geq 1}\binom{\mu_j}{2}} \begin{bmatrix} m \\ \mu_1 \end{bmatrix}_q [\mu_1]_q! \widetilde{W}_\mu(x;q).$$

## 4.2 Future directions

Finally, we discuss some future research problems. These are listed as follows.

*I. Combinatorial interpretation of the formula 4.1.*

A combinatorial formula for diagonal operators appears in [40], where a formula for $\sigma(\mu; T)$ is expressed as a summation over semi-standard Young tableaux. For a general operator, we do not have a combinatorial description for the number of subspaces with a given profile.

*II. Construction of splitting subspaces.*

It is an interesting project to provide a method of construction of splitting subspaces or, more generally, subspaces with a given profile. A recursive formula for constructing such subspaces is known for diagonalizable operators [40]. However, for a general operator, the problem seems to be open.

*III. Enumeration of polynomial matrices.*

The problem of determination of $\mu_q(n, k, d; \mathcal{I})$ (see Section 1.2 for the definition) is open for an arbitrary assignment of the parameters $n$, $k$, $d$, and $\mathcal{I}$. When $n = k$, the problem boils down to counting the number of splitting subspaces (Theorem 3.2.2), which is given by Theorem 4.1.5. However, when $n \neq k$, further work is required to have a complete solution.

# Appendices

# Appendix A

# Similarity class types and splitting subspaces

We give an alternate proof of Corollary 2.2.5 here using the theory of lattices. We prove that if two operators have the same similarity class type, then the number of splitting subspaces for both the operators coincide. To prove this we begin by recalling some basic facts about lattices. A partially ordered set $P$ is called a *lattice* if any two elements $a, b \in P$ have a meet (greatest lower bound), denoted by $a \wedge b$, and a join (least upper bound), denoted $a \vee b$. We denote by $L(T)$, the set of all $T$-invariant subspaces of $V$. Clearly, $L(T)$ is a lattice with subspaces ordered by inclusion, with intersection as meet and linear sum as join. A *lattice homomorphism* is a mapping between lattices that preserves meets and joins. Two lattices are *isomorphic* if there exists a bijective lattice homomorphism between them.

Let $p = \prod_{i=1}^{k} {p_i}^{n_i}$ denote the canonical factorization of the minimal polynomial $p$ of an operator $T$ into distinct irreducible factors $p_i (1 \leq i \leq k)$. Let $V_i = \{\alpha \in V : p_i(T)^{n_i}\alpha = 0\}$. Then $V_i$ is a $T$-invariant subspace of $V$ and

$$V = \bigoplus_{i=1}^{k} V_i.$$

This is the primary decomposition of $V$. We call an operator *primary* or *p-primary* if its minimal polynomial is a power of the irreducible polynomial $p$.

Denote by $T_i$ the restriction of $T$ to $V_i$. Then $T_i$ is a linear operator on $V_i$. It is known [8, Thm. 1] that the lattice $L(T)$ is the direct product of the lattices $L(T_i)$, i.e.,

$$L(T) = \prod_{i=1}^{k} L(T_i).$$

Thus, for each $U \in L(T)$, there exists precisely one sequence $(U_1, \ldots, U_k) \in \prod_{i=1}^{k} L(T_i)$ such that $U = U_1 \oplus \cdots \oplus U_k$. Consequently, it suffices to study the lattices $L(T_i)$ corresponding to the primary components $V_i, 1 \leq i \leq k$.

**Proposition A.1.** If $T$ and $T'$ are similar then there exists a dimension preserving isomorphism between $L(T)$ and $L(T')$.

*Proof.* Let $S$ be an invertible transformation such that $T' = S \circ T \circ S^{-1}$. Then $W$ is $T$-invariant if and only if $SW$ is $T'$-invariant. Therefore the map $W \mapsto SW$ is a dimension preserving lattice isomorphism from $L(T)$ to $L(T')$. □

**Theorem A.2.** Let $T$ be a linear operator on a vector space $V$ over a field $F$ such that $T$ is $p$-primary with $p$ separable. Let $T = S + Q$ denote the Jordan-Chevalley decomposition of $T$ into its semi-simple part $S$ and nilpotent part $Q$. Let $K$ be the algebra of polynomials in $S$ over $F$. Then $K$ is a field isomorphic to $F[x]/(p(x))$, $V$ is naturally a $K$-vector space, $T$ is $K$-linear, and $L_F(T) = L_K(T) = L_K(Q)$.

*Proof.* See [8, Thm. 6]. □

The above theorem applies to every primary operator defined over a finite field since irreducible polynomials in this setting are separable.

**Theorem A.3.** Let $T$ and $T'$ be linear operators of the same similarity class type defined on a vector space $V$ over $\mathbb{F}_q$. Then there exists a dimension preserving isomorphism between $L(T)$ and $L(T')$.

*Proof.* It suffices to prove the result when $T$ and $T'$ are primary operators. Let $T$ be $p$-primary and $T'$ be $p'$-primary. Let $T = S + Q$ and $T' = S' + Q'$ where $S$ and $S'$ are semi-simple while $Q$ and $Q'$ are nilpotent. Further, let

$K$ and $K'$ be the algebras of polynomials in $S$ and $S'$ respectively over $\mathbb{F}_q$. Theorem A.2 implies that the fields $K$ and $K'$ are isomorphic since $p$ and $p'$ are irreducible polynomials over $\mathbb{F}_q$ of the same degree. Further, $L_{\mathbb{F}_q}(T) = L_K(Q)$ and $L_{\mathbb{F}_q}(T') = L_{K'}(Q')$. Since $T$ and $T'$ are of same similarity class type, it follows that their nilpotent parts $Q$ and $Q'$ are also of the same type. Thus $Q$ and $Q'$ are similar. By Proposition A.1 and the fact that $K \cong K'$, we obtain a dimension preserving isomorphism between $L_K(Q)$ and $L_{K'}(Q')$. □

**Remark A.4.** In light of the above theorem, given $q$, we may define the number of invariant subspaces of dimension $k$ of a similarity class type $\tau$ to be the number of invariant subspaces of dimension $k$ of some operator $T$ of type $\tau$ over $\mathbb{F}_q$.

**Corollary A.5.** 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 $\sigma(m, d; T) = \sigma(m, d; T')$.

*Proof.* The sets $[(a_1, a_1), (a_2, a_2), \ldots, (a_r, a_r)]_T$ corresponding to base cases in the recursion of Lemma 2.1.6 consist of flags of invariant subspaces $(W_1, \ldots, W_r)$ such that $\dim W_i = a_i$ and $W_i \supseteq W_{i+1}$ for $1 \leq i \leq r-1$. The existence of a dimension preserving isomorphism between $L(T)$ and $L(T')$ ensures that the base cases coincide:

$$|[(a_1, a_1), (a_2, a_2), \ldots, (a_r, a_r)]_T| = |[(a_1, a_1), (a_2, a_2), \ldots, (a_r, a_r)]_{T'}|.$$

Therefore

$$|[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \ldots, (a_{r,1}, a_{r,2})]_T| =$$

$$|[(a_{1,1}, a_{1,2}), (a_{2,1}, a_{2,2}), \ldots, (a_{r,1}, a_{r,2})]_{T'}|,$$

whenever the two quantities are defined. In particular, by Proposition 2.1.7, we must have $\sigma(m, d; T) = \sigma(m, d; T')$. □

# Bibliography


[1] Martin Aigner. *A course in enumeration*, volume 238 of *Graduate Texts in Mathematics*. Springer, Berlin, 2007.

[2] George E. Andrews. *The theory of partitions*, volume Vol. 2 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976.

[3] Akansha Arora, Samrith Ram, and Ayineedi Venkateswarlu. Unimodular polynomial matrices over finite fields. *J. Algebraic Combin.*, 53(4):1299–1312, 2021.

[4] José Barría and P. R. Halmos. Weakly transitive matrices. *Illinois J. Math.*, 28(3):370–378, 1984.

[5] Edward A. Bender, Raymond Coley, David P. Robbins, and Howard Rumsey, Jr. Enumeration of subspaces by dimension sequence. *J. Combin. Theory Ser. A*, 59(1):1–11, 1992.

[6] Charles Bouillaguet and Paul Zimmermann. Parallel structured gaussian elimination for the number field sieve. *Mathematical Cryptology*, (1):22–39, 2021.

[7] Richard P. Brent, Shuhong Gao, and Alan G. B. Lauder. Random Krylov spaces over finite fields. *SIAM J. Discrete Math.*, 16(2):276–287, 2003.

[8] L. Brickman and P. A. Fillmore. The invariant subspace lattice of a linear transformation. *Canadian J. Math.*, 19:810–822, 1967.

[9] Lynne M. Butler. Subgroup lattices and symmetric functions. *Mem. Amer. Math. Soc.*, 112(539):vi+160, 1994.

[10] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[11] Eric Chen and Dennis Tseng. The splitting subspace conjecture. *Finite Fields Appl.*, 24:15–28, 2013.

[12] Sylvie Corteel, Carla D. Savage, Herbert S. Wilf, and Doron Zeilberger. A pentagonal number sieve. *J. Combin. Theory Ser. A*, 82(2):186–192, 1998.

[13] S. Delsarte. Fonctions de Möbius sur les groupes abeliens finis. *Ann. of Math. (2)*, 49:600–609, 1948.

[14] Harald Fripertinger. The number of invariant subspaces under a linear operator on finite vector spaces. *Adv. Math. Commun.*, 5(2):407–416, 2011.

[15] Jason Fulman. Random matrix theory over finite fields. *Bull. Amer. Math. Soc. (N.S.)*, 39(1):51–85, 2002.

[16] Mario García-Armas, Sudhir R. Ghorpade, and Samrith Ram. Relatively prime polynomials and nonsingular Hankel matrices over finite fields. *J. Combin. Theory Ser. A*, 118(3):819–828, 2011.

[17] Anton Gerasimov, Dimitri Lebedev, and Sergey Oblezin. On q-deformed-whittaker function i. *Communications in Mathematical Physics*, 294(1):97–119, 2010.

[18] Sudhir R. Ghorpade and Samrith Ram. Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields. *Finite Fields Appl.*, 17(5):461–472, 2011.

[19] Sudhir R. Ghorpade and Samrith Ram. Enumeration of splitting subspaces over finite fields. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 49–58. Amer. Math. Soc., Providence, RI, 2012.

[20] Heide Gluesing-Luerssen and Alberto Ravagnani. Partitions of matrix spaces with an application to $q$-rook polynomials. *European J. Combin.*, 89:103120, 28, 2020.

[21] I. Gohberg, P. Lancaster, and L. Rodman. *Matrix polynomials*, volume 58 of *Classics in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2009.

[22] J. A. Green. The characters of the finite general linear groups. *Trans. Amer. Math. Soc.*, 80:402–447, 1955.

[23] Uwe Helmke, Jens Jordan, and Julia Lieb. Probability estimates for reachability of linear systems defined over finite fields. *Adv. Math. Commun.*, 10(1):63–78, 2016.

[24] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Second edition. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1971.

[25] Frieder Knüppel and Klaus Nielsen. $k$-fold anti-invariant subspaces of a linear mapping. *Linear Algebra Appl.*, 375:13–19, 2003.

[26] Donald E. Knuth. *The art of computer programming. Vol. 2: Seminumerical algorithms*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont, 1969.

[27] M. Kociecki and K. M. Przyluski. On the number of controllable linear systems over a finite field. *Linear Algebra Appl.*, 122/123/124:115–122, 1989.

[28] Jörg Liesen and Zdeněk Strakoš. *Krylov subspace methods*. Numerical Mathematics and Scientific Computation. Oxford University Press, Oxford, 2013. Principles and analysis.

[29] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford Classic Texts in the Physical Sciences. The Clarendon Press, Oxford University Press, New York, second edition, 2015. With contribution by A. V. Zelevinsky and a foreword by Richard Stanley.

[30] Ian G Macdonald. A new class of symmetric functions. *Séminaire Lotharingien de Combinatoire [electronic only]*, 20:B20a–41, 1988.

[31] Harald Niederreiter. The multiple-recursive matrix method for pseudorandom number generation. *Finite Fields Appl.*, 1(1):3–30, 1995.

[32] Jean-Guy Penaud. Une preuve bijective d'une formule de Touchard-Riordan. volume 139, pages 347–360. 1995. Formal power series and algebraic combinatorics (Montreal, PQ, 1992).

[33] Amritanshu Prasad and Samrith Ram. Set partitions, tableaux, and subspace profiles under regular split semisimple matrices. *arXiv preprint arXiv:2112.00479*, 2021.

[34] Amritanshu Prasad and Samrith Ram. Set partitions, tableaux, and subspace profiles of regular diagonal operators. *Sém. Lothar. Combin.*, 86B:Art. 35, 12, 2022.

[35] Amritanshu Prasad and Samrith Ram. Splitting subspaces and a finite field interpretation of the Touchard-Riordan formula. *European J. Combin.*, 110:Paper No. 103705, 11, 2023.

[36] Amritanshu Prasad and Samrith Ram. Enumeration of anti-invariant subspaces and Touchard's formula for the entries of the $q$-Hermite Catalan matrix. *Adv. in Appl. Math.*, 154:Paper No. 102654, 18, 2024.

[37] Samrith Ram. Counting zero kernel pairs over a finite field. *Linear Algebra Appl.*, 495:1–10, 2016.

[38] Samrith Ram. The number of linear transformations defined on a subspace with given invariant factors. *Linear Algebra Appl.*, 532:146–161, 2017.

[39] Samrith Ram. Subspace profiles over finite fields and $q$-Whittaker expansions of symmetric functions. *arXiv preprint arXiv:2309.16607*, 2023.

[40] Samrith Ram and Michael J Schlosser. Diagonal operators, $q$-Whittaker functions and rook theory. *arXiv preprint arXiv:2309.06401*, 2023.

[41] Ronald C. Read. The chord intersection problem. In *Second International Conference on Combinatorial Mathematics (New York, 1978)*, volume 319 of *Ann. New York Acad. Sci.*, pages 444–454. New York Acad. Sci., New York, 1979.

[42] Christophe Reutenauer. *Free Lie algebras*, volume 7 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1993. Oxford Science Publications.

[43] John Riordan. The distribution of crossings of chords joining pairs of $2n$ points on a circle. *Math. Comp.*, 29:215–222, 1975.

[44] A. R. Sourour. Anti-invariant subspaces of maximum dimension. *Linear Algebra Appl.*, 74:39–45, 1986.

[45] Richard P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

[46] Richard P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.

[47] Jacques Touchard. Contribution à l'étude du problème des timbres poste. *Canad. J. Math.*, 2:385–398, 1950.

[48] Jacques Touchard. Sur un problème de configurations. *C. R. Acad. Sci. Paris*, 230:1997–1998, 1950.

[49] Jacques Touchard. Sur un problème de configurations et sur les fractions continues. *Canad. J. Math.*, 4:2–25, 1952.

[50] David S. Watkins. *The matrix eigenvalue problem*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2007. *GR* and Krylov subspace methods.

# List of Publications

## Published articles

1. Divya Aggarwal and Samrith Ram. Splitting subspaces of linear operators over finite fields. *Finite Fields Appl.*, 78:Paper No. 101982, 17, 2022.

2. Divya Aggarwal and Samrith Ram. Polynomial matrices, splitting subspaces and Krylov subspaces over finite fields. *Finite Fields Appl.*, 83:Paper No. 102081, 16, 2022.

## Communicated article

1. Divya Aggarwal. Enumeration of splitting subsets of endofunctions on finite sets. arXiv./abs/2306.04256, 2023.

# DIVYA AGGARWAL

Indraprastha Institute of Information Technology
New Delhi, India

divyaa@iiitd.ac.in (91)9650919527

## EDUCATION

**Ph.D. in Mathematics**
*Indraprastha Institute of Information Technology Delhi* *Thesis Submitted: 31st May 2024*
Advisor: Dr. Samrith Ram
CGPA: 9.73/10

**M.Sc. Mathematics**
*Ramjas College, University of Delhi* *2018*
70.31%

**Bachelor with Honours in Mathematics**
*Shivaji College, University of Delhi* *2016*
88.58%

## ACADEMIC VISITS

- **Visiting Scholar** *April 2023 - May 2023*
  Host: Prof. Manoj K. Yadav
  Harish-Chandra Research Institute (HRI)
  Allahabad, India
- **Visiting Scholar** *July 2022 - Feb. 2023*
  Host: Prof. Amritanshu Prasad
  The Institute of Mathematical Sciences (IMSc)
  Chennai, India

## RESEARCH INTERESTS

Enumerative and Algebraic Combinatorics, Linear Algebra, Finite Fields, Theory of Partitions, Graph Theory, and Representation Theory of Finite Groups

## PUBLISHED/COMMUNICATED PAPERS

- **Enumeration of Splitting Subsets of Endofunctions on Finite Sets** *June 2023*
  https://arxiv.org/abs/2306.04256
- **Polynomial Matrices, Splitting Subspaces and Krylov Subspaces over Finite Fields** *Oct. 2022*
  (with Samrith Ram)
  Finite Fields and their Applications
  https://doi.org/10.1016/j.ffa.2022.102081
- **Splitting Subspaces of Linear Operators over Finite Fields** *Feb. 2022*
  (with Samrith Ram)
  Finite Fields and their Applications
  https://doi.org/10.1016/j.ffa.2021.101982

## INVITED/CONFERENCE TALKS

- **Splitting Subspaces of Linear Operators over Finite Fields** *June 2023*
  International Conference on Finite Fields and their Applications (Fq15)
  Campus Condorcet, Paris-Aubervilliers, France
- **Splitting Subspaces, Krylov Subspaces and Polynomial Matrices over Finite Fields** *May 2023*
  Meru Combinatorics Conference 2023
  Department of Mathematics, Pondicherry University, India
- **Enumeration of Splitting Subspaces and Krylov Subspaces over Finite Fields** *April 2023*
  Harish-Chandra Research Institute (HRI), Allahabad, India
- **Counting splitting subspaces of linear operators over finite fields** *Dec. 2022*
  National Symposium on Mathematics and Applications (NSMA-2022)
  Department of Mathematics, Indian Institute of Technology (IIT) Madras
- **Wilf and Zeilberger's algorithm for proving hypergeometric identities** *Oct. 2022*
  Algebraic Combinatorics Seminar Series
  The Institute of Mathematical Sciences (IMSc), Chennai
- **Cyclic Sieving Phenomenon** *Aug. 2022*
  Algebraic Combinatorics Seminar Series
  The Institute of Mathematical Sciences (IMSc), Chennai
- **Splitting subspaces of linear operators over finite fields** *July 2022*
  Short Communication Satellite (SCS 2022)
  International Congress of Mathematics (ICM)
- **Splitting subspaces, Krylov subspaces and polynomial matrices over finite fields** *June 2022*
  5th International Conference on Recent Advances in Mathematical Sciences with Applications in Engineering and Technology (IC-RA-MSA-ET-2022)
  Jawaharlal Nehru University (JNU), New Delhi
- **Enumeration of splitting subspaces of linear operators over finite fields** *April 2022*
  1st International Conference on Recent Researches in Mathematics (FICRRM-22)
  Department of Mathematics, College of Natural and Computational Science, Mizan-Tepi University, Tepi Campus, Ethiopia
- **Enumeration of Matrices and Splitting Subspaces over Finite Fields** *Feb. 2021*
  Online Research Seminar for Early Career Mathematicians
  Slides of the talk: `https://manjilsaikia.in/seminar/Divya_Aggarwal.pdf`
- **Topics in Matrix Enumeration over Finite Fields** *Dec. 2020*
  Ph.D. Math Seminar Series, IIIT Delhi
- **Mathematics and Society** *July 2018*
  Graduation Ceremony, Department of Mathematics, University of Delhi
- **Applications of Group Theory** *Feb. 2016*
  Infinity, Annual Fest of Mathematics, Shivaji College, University of Delhi
- **Fibonacci Numbers in Nature** *Feb. 2015*
  Infinity, Annual Fest of Mathematics, Shivaji College, University of Delhi

## POSTER PRESENTATIONS

- **Splitting Subspaces of Linear Operators and their q = 1 Analogues** *June 2024*
  Algebraic Combinatorics Virtual Expedition (AlCoVE)

- **Subset Profiles of Endofunctions on Finite Sets** *June 2024*
  Second Meru Combinatorics Conference 2024
  Graphic Era Hill University, Bhimtal, India
- **Polynomial Matrices, Splitting Subspaces and Krylov Subspaces over Finite Fields** *December 2023*
  International Conference on Algebraic Geometry, Coding Theory and Combinatorics
  Indian Institute of Technology, Hyderabad, India
- **Splitting Subspaces of Linear Operators over Finite Fields** *August 2023*
  Summer School in Algebraic, Asymptotic and Enumerative Combinatorics
  The Mathematical Research and Conference Center, Bedlewo, Poland
- **Enumeration of Splitting Subsets of Endofunctions on Finite Sets** *May 2023*
  Research Innovation & Incubation Showcase (RIISE)
  IIIT Delhi, India

## REVIEWER

- **Short Communication Satellite** *July 2022*
  International Congress of Mathematics (ICM)

## AWARDS AND FELLOWSHIPS

- **Senior Research Fellowship** *2021*
  Council of Scientific and Industrial Research, India
- **Junior Research Fellowship and NET** *2018*
  Council of Scientific and Industrial Research, India
  All India Rank: 93
- **GATE in Mathematics** *2018*
  NCB-GATE, Government of India
- **First Prize in Mathematical Extempore** *2015*
  University of Delhi
- **Second Prize in Mathematics Art** *2015*
  University of Delhi
- **CSSS Scholarship** *2013-2014*
  Government of India
- **Indira Award** *2011*
  Presented by Delhi's Chief Minister Smt. Sheela Dixit
  Government of India

## TEACHING ASSISTANCE

- **Advanced Topics in Finite Fields** *July 2023*
  National Centre for Mathematics - Advanced Instructional School (AIS)
  The Institute of Mathematical Sciences (IMSc), Chennai, India
- **Linear Algebra** *Winter 2022*
  Instructor: Dr. Samaresh Chatterji, IIIT Delhi
  Electronics and Communications Engineering (ECE)
- **Combinatorics and its Applications** *Winter 2021*
  Instructor: Dr. Samrith Ram, IIIT Delhi
  B.Tech. Computer Science and Applied Mathematics (CSAM)

- **Discrete Mathematics** *Monsoon 2020, 2021*
  Instructor: Dr. Samrith Ram, IIIT Delhi
  B.Tech. Computer Science and Design (CSD)
- **Real Analysis** *Monsoon 2019*
  Instructor: Dr. Sankha S Basu, IIIT Delhi
  B.Tech. Computer Science and Engineering (CSE)

## PARTICIPATION IN SCHOOLS/ WORKSHOPS

- **CIMPA-NCM School on Finite Geometry and Coding Theory** *November-December 2023*
  Indian Institute of Technology (IIT)
  Hyderabad, India
- **Summer School in Algebraic, Asymptotic and Enumerative Combinatorics** *July-August 2023*
  The Mathematical Research and Conference Center
  Institute of Mathematics of the Polish Academy of Science
  Bedlewo, Poland
- **Advanced Topics in Finite Fields** *July 2023*
  National Centre for Mathematics - AIS
  The Institute of Mathematical Sciences (IMSc)
  Chennai, India
- **Linear Algebra and Discrete Mathematics** *Jan. 2023*
  National Centre for Mathematics
  The Institute of Mathematical Sciences (IMSc)
  Chennai, India
- **Sage Days 114** *July 2022*
  The Institute of Mathematical Sciences (IMSc)
  Chennai, India
- **Representation Theory** *June-July 2022*
  National Centre for Mathematics - AIS
  Chennai Mathematical Institute (CMI)
  Chennai, India
- **Annual Foundation School -I** *April-May 2020*
  National Centre for Mathematics
  Online Session
- **Combinatorial Models in Representation Theory** *November 2019*
  National Centre for Mathematics
  The Institute of Mathematical Sciences (IMSc)
  Chennai, India
- **Training Programme in Mathematics** *May-June 2017*
  Centre for Fundamental Studies
  National Institue of Science Education and Research (NISER)
  Bhubaneswar, India
- **Theory of Equations** *October 2014*
  Science Academies' Lecture Workshop
  Shivaji College, University of Delhi
  New Delhi, India

## SKILLS

- **Programming** SageMath, C$^{++}$, Mathematica
- **Presentation** LaTeX, MS Office
- **Languages** English, Hindi

## EXTRACURRICULAR ACTIVITIES

- Volunteered for FACETS 2022 at the Institute of Mathematical Sciences, Chennai.
- Volunteered for Kanita Kanakam 2022 at the Institute of Mathematical Sciences, Chennai.
- Organized Departmental Fest Infinity with the Mathematics Department at Shivaji College from 2013 - 2016.
- Anchored several events during B.Sc. and M.Sc.
- Participated in various Mathematical activities like Quizzes, Extempores, Debates and Discussions.

## PERSONAL DETAILS

- **Nationality** Indian
- **Date of Birth** $16^{th}$ April 1996
- **Marital Status** Unmarried
- **Permanent Address** 12, Top Floor, Pocket-1, Sector-A9, Narela, Delhi-110040