Unimodular Polynomial Matrices and Partial Linear Transformations over Finite Fields

by

Akansha Arora

PhD17303

Under the Supervision of Dr. Samrith Ram

Indraprastha Institute of Information Technology Delhi

November 2022

Indraprastha Institute of Information Technology Delhi

Doctoral Thesis

Unimodular Polynomial Matrices and Partial Linear Transformations over Finite Fields

Author:

Akansha Arora

Supervisor:

Dr. Samrith Ram

A thesis submitted in fulfillment of the requirements

for the degree of Doctor of Philosophy

to the

Indraprastha Institute of Information Technology Delhi

November 2022

Dedicated to my teachers, my parents

and my nephew Amaay.

CERTIFICATE

This is to certify that the thesis titled "Unimodular Polynomial Matrices and Partial Linear Transformations over Finite Fields" being submitted by AKANSHA ARORA, 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.

Samrith Ram

November, 2022

Dr. Samrith Ram

Indraprastha Institute of Information Technology Delhi

New Delhi 110020

ACKNOWLEDGEMENTS

Completing this doctoral thesis would not have been possible without the support and guidance of many individuals. Thus before beginning, I would like to express my most profound appreciation to all who, knowingly or unknowingly, directly or indirectly helped me in this thesis.

First and foremost, I thank the Almighty for his kind blessings. I express my sincere gratitude to my supervisor Dr. Samrith Ram, whose expertise, guidance, and support made it possible for me to write this thesis. He has always shared his wisdom and vision. His persistent encouragement and patient attitude were critical to my successful research.

I thank all the faculty members of IIIT-D for their constant support and cooperation. I am highly thankful to my doctoral committee members, Dr. Sankha S Basu and Dr. Sneha Chaubey, for their valuable time and helpful comments throughout this research work. Also, I express my sincere thanks to Dr. Shanta Laisharam, Indian Statistical Institute, New Delhi, India, for being the external examiner on the occasion of my comprehensive exam and fellowship enhancement seminar. I thank my fellow labmates, especially Diksha Bansal and Varsha Chauhan, for providing great company and stimulating discussions during all the years of my Ph.D. life.

Most importantly, I am very grateful to my family for their love, affection, care, and blessings. I am highly indebted to my parents for their countless sacrifices, without which I could not have reached where I am today. I acknowledge my sibling Gaurav, his wife Neha, and my nephew Amaay, for always being with me. I am also thankful to my friends Mahima, Raj, Arpita, Asmita, Isha, Nikita, Sanjana, Komal and many more, for providing me their great company and bearing my Ph.D. frustration.

I gratefully acknowledge the University Grant Commission (UGC) for providing financial support and the Department of Mathematics, IIIT-D, for the necessary facilities, outstanding infrastructure, and working environment. Last but not least, I sincerely thank everyone who helped me with my thesis at any stage.

Akansha Arora

PhD17303

ABSTRACT

This thesis consists of some interesting combinatorial problems on matrix polynomials over finite fields. Using results from control theory, we give a proof of a result of Lieb, Jordan and Helmke (2016) which solves the problem of counting the number of linear unimodular polynomial matrices over a finite field. This problem was essentially considered by Kocięcki and Przyłuski in an attempt to estimate the proportion of reachable linear systems over a finite field. As an application of our results, we give a new proof of a theorem of Chen and Tseng, which answers a question of Niederreiter on splitting subspaces. We use our results to affirmatively resolve a conjecture on the probability that a matrix polynomial is unimodular.

We consider another enumerative problem on the similarity class of an arbitrary linear map defined on a subspace of a vector space over a finite field. Let V be a finite-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements where q is a prime power and suppose W and $\widetilde{W}$ are subspaces of V. Two linear transformations $T : W \to V$ and $\widetilde{T} : \widetilde{W} \to V$ are said to be similar if there exists a linear isomorphism $S : V \to V$ such that the following diagram commutes:

$$\begin{array}{ccc} W & \xrightarrow{T} & V \\ {\scriptstyle S_W}\downarrow & & \simeq\downarrow{\scriptstyle S} \\ \widetilde{W} & \xrightarrow{\widetilde{T}} & V \end{array}.$$

In other words, we must have $S \circ T = \widetilde{T} \circ S_W$ where S_W denotes the restriction of S to W. Given a linear map T defined on a subspace W of V, sometimes referred to as a partial linear map, we discuss the similarity invariants for T. We then give an explicit formula for the number of linear maps that are similar to T. The case where T is a linear operator on V (the case $W = V$) is well-studied and we

extend the result where W is an arbitrary subspace of V. In fact, the problem of counting the similarity class size of a linear operator T is equivalent to counting the number of square matrices over the finite field $\mathbb{F}_q$ in a conjugacy class. This problem has been studied by Kung (1981) and Stong (1988) among others, and an explicit formula due to Philip Hall is known. Our results extend the explicit formula of Philip Hall on matrix conjugacy class size. As a consequence of the results, we provide another proof of a theorem of Lieb, Jordan and Helmke on the number of linear unimodular matrix polynomials.

Contents

List of Figures

Chapter 1

Introduction

We denote by $\mathbb{F}_q$ the finite field with q elements where q is a prime power. Let $\mathbb{F}_q[x]$ denote the ring of polynomials over $\mathbb{F}_q$ in the indeterminate x. Throughout this thesis, n and k denote nonnegative integers. For any ring R, define $M_{n,k}(R)$ to be the set of all $n \times k$ matrices over R. Similarly $M_k(R)$ denotes the ring of $k \times k$ matrices over R. Denote by $I_{n,k}$ the matrix in $M_{n,k}(\mathbb{F}_q)$ whose $(i,j)^{\text{th}}$ entry is zero whenever $i \neq j$ and equal to 1 for $i = j$. We begin by providing a general overview of the problems that we have explained in the thesis.

1.1 Unimodular matrix polynomials over finite fields

This part is devoted to the study of matrix polynomials over finite fields. A matrix polynomial over a field F in the variable x is a sum $\sum_{i=0}^{d} A_i x^i$, where $A_i \in M_{n,k}(F)(0 \leq i \leq d)$ for some fixed positive integers n, k. It is often convenient to view such a matrix polynomial as a single matrix whose entries are polynomials in x (sometimes referred to as a polynomial matrix) and we freely alternate between these two points of view. A matrix polynomial $\mathbf{A} = \sum_{i=0}^{d} A_i x^i \in M_{n,k}(\mathbb{F}_q[x])$ is *unimodular* if the greatest common divisor of all $r \times r$ minors of $\mathbf{A}$ is equal to 1

where $r = \min\{n, k\}$. The notion of unimodularity can be defined more generally for rectangular matrices over an arbitrary integral domain. A landmark result in the setting of unimodularity is the Quillen-Suslin theorem [40, 48] formerly known as Serre's conjecture. We refer to [22, 32, 34, 50] for other contexts where unimodularity is considered. We begin with a combinatorial question concerning matrix polynomials over a finite field.

Question 1.1.1. Given positive integers n, k and a prime power q, determine the number of matrices $A \in M_{n,k}(\mathbb{F}_q)$ for which the matrix polynomial $xI_{n,k} - A$ is unimodular.

This question was essentially considered by Kocięcki and Przyłuski [28] (also see [42, Prob. 1.2]) in an attempt to determine the number of reachable pairs of matrices over a finite field. Reachability is a fundamental notion in the control theory of linear systems. The question was fully answered only recently by Lieb, Jordan and Helmke [33, Thm. 1] who showed that the answer is equal to $\prod_{i=1}^{k}(q^n - q^i)$. In fact, the problem of counting reachable pairs of matrices is equivalent to the problem of determining the number of simple linear transformations (see Definition 3.2.1) and the problem of counting the number of zero kernel pairs of matrices. We briefly state the alternate formulations of the result of Lieb et al in Chapter 2 (see introduction of [42] for more details).

One of our main result is Lemma 3.2.9. This lemma allows us to give a new proof (Corollary 3.2.12) of the theorem of Lieb et al. An essential ingredient in our main lemma is a control theoretic result of Brunovský on completely controllable pairs.

Further applications of our results appear in Chapter 4. In Section 4.2 we consider splitting subspaces (defined below) which were introduced by Niederreiter [36, Def. 1] in the context of his work on the multiple recursive matrix method for pseudorandom number generation. Here is the definition of a splitting subspace.

Definition 1.1.2. Let d, m be positive integers and consider the vector space $\mathbb{F}_{q^{md}}$ over $\mathbb{F}_q$. For any element $\alpha \in \mathbb{F}_{q^{md}}$ an m-dimensional subspace W of $\mathbb{F}_{q^{md}}$ is α-*splitting* if

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

Niederreiter was interested in the following question on splitting subspaces.

Question 1.1.3. Given $\alpha \in \mathbb{F}_{q^{md}}$ such that $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$, what is the number of α-splitting subspaces of $\mathbb{F}_{q^{md}}$ of dimension m?

It may be noted that the same question was also considered by Goresky and Klapper (see the remark in [21, p. 1653] and [21, Thm. 3(4)]). In addition to the evident cryptographic aspect, Niederreiter's question also has interesting connections with group theory and finite projective geometry via block companion Singer cycles. We refer to [17, 18] for more on this topic. The case $m = 2$ of Niederreiter's question was settled in [18] using a result that answers the following question: What is the probability that two randomly chosen polynomials of a fixed positive degree over a finite field are coprime? This question on the probability of coprime polynomials goes back to an exercise in Knuth [27, §4.6.1, Ex. 5] and has subsequently been considered by Corteel, Savage, Wilf and Zeilberger [10] in the more general setting of combinatorial prefabs. Further results on the degree distribution of the greatest common divisor of random polynomials over a finite field appear in [15]. In fact, our main result relies on Lemma 3.2.3 which may be viewed as a probabilistic result on coprime polynomials. Chen and Tseng [8, Cor. 3.4] eventually answered Niederreiter's question on splitting subspaces by proving the following theorem which was initially conjectured in [18, Conj. 5.5].

Theorem 1.1.4 (Splitting Subspace Theorem)**.** For any $\alpha \in \mathbb{F}_{q^{md}}$ such that $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$, the number of α-splitting subspaces of $\mathbb{F}_{q^{md}}$ of dimension m is

precisely

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

In Chapter 4, a control-theoretic result of Wimmer (Theorem 4.2.7) is used to prove Theorem 4.2.8 from which the Splitting Subspace Theorem follows as a corollary.

In Section 4.3, a generalization of Question 1.1.1 is considered. The answer to this question which was stated earlier can be given a probabilistic flavour as follows.

Theorem 1.1.5. If a matrix A is selected uniformly at random from $M_{n,k}(\mathbb{F}_q)$, then the probability that $xI_{n,k} - A$ is unimodular is given by $\prod_{i=1}^{k}(1-q^{i-n})$.

Using results in Section 3.2, we prove a conjecture (Theorem 4.3.1) proposed in [42] on the proportion of unimodular polynomial matrices which generalizes Theorem 1.1.5.

1.2 Enumerating partial linear transformations in a similarity class

We now consider the similarity of linear transformations defined on a subspace of a vector space over the field $\mathbb{F}_q$. Let V be an n dimensional vector space over the field $\mathbb{F}_q$ with q elements and let W be a subspace of V. Let $L(W,V)$ denote the vector space of all $\mathbb{F}_q$-linear transformations from W to V. Two linear transformations $T \in L(W,V)$ and $\widetilde{T} \in L(\widetilde{W},V)$ defined on subspaces W and $\widetilde{W}$ of V respectively are similar if there exists a linear isomorphism $S : V \to V$ such that the following diagram commutes:

$$\begin{array}{ccc} W & \xrightarrow{T} & V \\ {\scriptstyle S_W}\downarrow & & \simeq\downarrow{\scriptstyle S} \\ \widetilde{W} & \xrightarrow{\widetilde{T}} & V \end{array}.$$

In other words, we must have $S \circ T = \widetilde{T} \circ S_W$ where S_W denotes the restriction of S to W. Let $\mathcal{L}(V)$ denote the union of the vector spaces $L(W, V)$ as W varies over all possible subspaces of V. Given $T \in \mathcal{L}(V)$ define $\mathcal{C}(T)$, the conjugacy class of T, by

$$\mathcal{C}(T) := \{\widetilde{T} : \widetilde{T} \in \mathcal{L}(V),\ \widetilde{T} \text{ is similar to } T\}.$$

We are interested in determining the cardinality of $\mathcal{C}(T)$ for an arbitrary linear map T. The case where T is a linear operator on V is well-studied. Given such a linear operator T, one can view V as an $\mathbb{F}_q[x]$-module where the element x acts on V as the linear transformation T. By the structure theorem for modules over a principal ideal domain [25, p. 86], V is isomorphic to a direct sum

$$V \simeq \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[x]}{(p_i)}$$

of cyclic modules where $p_1, p_2, \ldots, p_r$ are monic polynomials of degree at least one over $\mathbb{F}_q$ with p_i dividing p_{i+1} for $1 \leq i \leq r-1$. The p_i are known as the invariant factors of T and uniquely determine T up to similarity; two linear operators T and $\widetilde{T}$ on V are similar if and only if they have the same invariant factors. In this case the problem of determining $|\mathcal{C}(T)|$ is equivalent to counting the number of square matrices over $\mathbb{F}_q$ in a conjugacy class. An explicit formula [45, Eq. 1.107] for the size of $\mathcal{C}(T)$ for a linear operator T was given by Philip Hall based on earlier work by Frobenius. This problem has also been studied by Kung [30] and Stong [46] who employ a generating function approach. In particular, Kung introduced a vector space cycle index which is an analog of the Pólya cycle index and can be used to enumerate many classes of square matrices over a finite field. We refer to the survey article of Morrison [35] for more on this topic. The invariant factors p_i of a linear operator T appear as the nonunit diagonal entries in the Smith Normal Form [24, p. 257] of $xI - A$ where A is the matrix of T with respect to some ordered basis for V. For more details, we refer Section 2.2.

In this part we determine the size of the similarity class $\mathcal{C}(T)$ for an arbitrary transformation $T \in \mathcal{L}(V)$. Our methods are mostly combinatorial and we use ideas from the theory of integer partitions. We first recall the definition of a partition. A partition of a nonnegative integer n is a sequence $\lambda = (\lambda_1, \lambda_2, \ldots)$ of nonnegative integers with $\lambda_i \geq \lambda_{i+1}$ for $i \geq 1$ and $\sum_i \lambda_i = n$. If $\lambda_{\ell+1} = 0$ for some integer ℓ, we also write $\lambda = (\lambda_1, \ldots, \lambda_\ell)$. The notation $\lambda \vdash n$ or $|\lambda| = n$ will mean that λ is a partition of the integer n. The first step is to characterize the similarity invariants for a linear transformation T defined only on a subspace W of an n-dimensional vector space V (such linear transformation could be referred to as a partial linear transformation). Accordingly, let $T \in \mathcal{L}(V)$ be a linear transformation and let U denote the maximal T-invariant subspace, and suppose $\dim U = d$. Interestingly, in this case the similarity classes are indexed by pairs $(\lambda, \mathcal{I})$ where λ is an integer partition of $n - d$ and $\mathcal{I}$ is an ordered set of monic polynomials corresponding to the invariant factors of the restriction of T to U. The precise details are in Chapter 5. When the domain of T is all of V, the partition λ above is empty and the similarity class $\mathcal{C}(T)$ is completely determined by the invariant factors of T. We prove (Corollary 5.4.8) that the size of the conjugacy class corresponding to the pair $(\lambda, \mathcal{I})$ is given by

$$|\mathcal{C}(\lambda, \mathcal{I})| = q^{d(k-d)+\sum_{i\geq 2}\lambda_i^2} \, |\mathcal{C}(\mathcal{I})| \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} k \\ d \end{bmatrix}_q \prod_{i\geq 1} \begin{bmatrix} \lambda_i \\ \lambda_{i+1} \end{bmatrix}_q \prod_{i=0}^{k-d-1} (q^{k-d} - q^i),$$

where $k = n - \lambda_1$ and $\begin{bmatrix} \cdot \\ \cdot \end{bmatrix}_q$ denotes a q-binomial coefficient while $|\mathcal{C}(\mathcal{I})|$ denotes the number of square matrices in the conjugacy class specified by $\mathcal{I}$. In fact Hall's result on matrix conjugacy class size may be recovered from Theorem 5.4.6 as well as Corollaries 5.4.7 and 5.4.8 by setting λ to be the empty partition.

While the problem of estimating similarity class sizes in $\mathcal{L}(V)$ seems quite natural and is an interesting combinatorial problem in its own right, it also has some connections with mathematical control theory. As a consequence of our

results we give another proof of a theorem of Lieb et al mentioned in the beginning on reachable linear systems over a finite field. Reachability also arises in the context of discrete automata theory, convolutional error correcting codes and linear sequential machines [12, 23, 44] among others. We refer to [31, 47] for some recent papers where reachability is considered in the setting of finite fields and to the book by Fuhrmann and Helmke [13] for more on this topic. It is worth noting that reachability has also been considered [6] in the setting of linear systems over commutative rings.

1.3 Organization of the thesis

Chapter 1 provides a general introduction and overview of the problems explored in the thesis. Chapter 2 is essential for the thesis as it briefly explains the background details and the concepts used throughout the thesis. Chapter 3 focuses on the results of unimodular matrix polynomials, and Chapter 4 contains applications of our results. The work of Chapters 3 and 4 is contained in our paper published in the Journal of Algebraic Combinatorics [5]. In Chapter 5, we study the similarity of partial linear transformations, and this work appears in Linear Algebra and its Applications [4]. In Chapter 6, we briefly discuss some interesting problems in this direction.

Chapter 2

Some Preliminaries

2.1 Introduction

This chapter contains related background information and well-known facts that will be employed later. To begin with, we give a definition of invariant factors in Section 2.2. We then introduce the notion of similar matrices and provide an explicit formula due to Philip Hall on the number of square matrices in a conjugacy class. In the next section, we briefly discuss the connection of the problem of determining the number of linear unimodular matrix polynomials (Question 1.1.1) with other equivalent problems.

2.2 Similarity

A polynomial matrix $P \in M_n(\mathbb{F}_q[x])$ is invertible if and only if the determinant of P is a nonzero element of $\mathbb{F}_q$. Let $A, B \in M_{n,k}(\mathbb{F}_q[x])$. Then A is equivalent to B (written $A \sim B$) over $\mathbb{F}_q[x]$ if there exist invertible matrices $P \in M_n(\mathbb{F}_q[x])$ and $Q \in M_k(\mathbb{F}_q[x])$ such that

$$PAQ = B.$$

For $1 \leq i \leq \min(n,k)$, we define i^{th} determinantal divisor of A (denoted by $\delta_i(A)$) to be the greatest common divisor of all $i \times i$ minors of the matrix A. It can be shown that if $A \sim B$, then

$$\delta_i(A) = \delta_i(B), \text{ for } 1 \leq i \leq \min(n,k).$$

Every nonzero polynomial matrix $A \in M_{n,k}(\mathbb{F}_q[x])$ is equivalent to a diagonal matrix of the form

$$\begin{bmatrix} p_1 & 0 & 0 & & \cdots & & 0 \\ 0 & p_2 & 0 & & \cdots & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ \vdots & & & p_t & & & \vdots \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & \cdots & & & 0 \end{bmatrix},$$

where the nonzero entries on the diagonal are monic polynomials p_i $(1 \leq i \leq t)$ satisfying $p_i \mid p_{i+1}$ for $1 \leq i < t$. This diagonal form is known as the Smith normal form of A. We express this in brief by writing $A \sim \text{diag}_{n,k}(p_1, \ldots, p_t)$. The polynomials $p_1, p_2, \ldots, p_t$ are called the invariant factors of A. It is easy to see that p_i are uniquely determined by

$$p_i = \frac{\delta_i(A)}{\delta_{i-1}(A)}.$$

We now consider the notion of similarity for square matrices. Let A and A' be $n \times n$ matrices over $\mathbb{F}_q$. We say that A' is similar to A over $\mathbb{F}_q$ if there is an invertible $n \times n$ matrix P over $\mathbb{F}_q$ such that $A' = P^{-1}AP$. It is well known fact that two square matrices $A, A' \in M_n(\mathbb{F}_q)$ are similar if and only if $xI_n - A$ and $xI_n - A'$ are equivalent over $\mathbb{F}_q[x]$, i.e., if and only if they have same invariant

factors (see [24, Sec. 7.2] for more details). More precisely, if $xI_n - A$ and $xI_n - A'$ have the Smith normal form as $\mathrm{diag}_{n,n}(p_1, \ldots, p_n)$ and $\mathrm{diag}_{n,n}(p'_1, \ldots, p'_n)$ respectively, then A, A' are similar if and only if $p_i = p'_i$ for $1 \leq i \leq n$. Thus the similarity class of A containing all matrices similar to A is characterized by the ordered set $\mathcal{I} = \{p_1, \ldots, p_n\}$ of invariant factors of A. It is reasonable to ask the following question: if we are given any matrix $A \in M_n(\mathbb{F}_q)$ with ordered set $\mathcal{I} = \{p_1, \ldots, p_n\}$ of invariant factors, how many matrices are in the conjugacy class of A? The explicit answer (see Theorem 2.2.1) to this question can be found in Stanley [45, Sec. 1.10]. We denote by $\mathcal{C}(\mathcal{I})$ the conjugacy class characterized by the ordered set $\mathcal{I} = \{p_1, \ldots, p_n\}$ of invariant factors with $\deg(p_1 \cdots p_n) = n$.

Let Par denote the set of all partitions of all non negative integers. We write $\lambda \vdash n$ if λ is a partition of n. Given any partition $\lambda = (\lambda_1, \lambda_2, \ldots) \in \mathrm{Par}$, let $\lambda' = (\lambda'_1, \lambda'_2, \ldots)$ denote the conjugate partition to λ, and let $m_i = m_i(\lambda) = \lambda'_i - \lambda'_{i+1}$ denote the number of parts of λ of size i. Set

$$h_i = \lambda'_1 + \lambda'_2 + \cdots + \lambda'_i.$$

For $\lambda \in \mathrm{Par}$ and any irreducible $f \in \mathbb{F}_q[x]$ of degree d, define

$$c_f(\lambda) = \prod_{i \geq 1} \prod_{j=1}^{m_i} (q^{h_i d} - q^{(h_i - j)d}).$$

For $f, g \in \mathbb{F}_q[x]$ with f irreducible and g nonzero, set

$$\nu_f(g) := \max\{e : f^e \mid g\}.$$

Given an ordered set $\mathcal{I} = \{p_1, \ldots, p_n\}$ of invariant factors, let $S(\mathcal{I})$ denote the set of all monic irreducible polynomials which divide p_n. To each $f \in S(\mathcal{I})$, we

associate a partition $\Phi_{\mathcal{I}}(f) \vdash \nu_f(P)$ by defining

$$\Phi_{\mathcal{I}}(f) := (\nu_f(p_n), \nu_f(p_{n-1}), \ldots, \nu_f(p_r)),$$

where $r = \min\{i : \nu_f(p_i) > 0\}$. Let $\mathrm{GL}_n(\mathbb{F}_q)$ denote the general linear group of $n \times n$ nonsingular matrices over $\mathbb{F}_q$. The following theorem (refer [43, Sec. 2]) gives the size of the conjugacy class corresponding to given ordered set of invariant factors.

Theorem 2.2.1 (P. Hall)**.** Let $\mathcal{I} = \{p_1, \ldots, p_n\}$ be any ordered set of invariant factors with $\deg(p_1 \cdots p_n) = n$. Then size of the conjugacy class corresponding to the ordered set of invariant factors $\mathcal{I}$ is given by

$$\#\mathcal{C}(\mathcal{I}) = \frac{|\,\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{f \in S(\mathcal{I})} c_f(\Phi_{\mathcal{I}}(f))}.$$

In Chapter 5, we extend the above result of Hall to the setting of rectangular matrices.

2.3 Unimodular Matrices And Zero Kernel Pairs

Recalling the definition of unimodularity, a matrix polynomial $\mathbf{A} \in M_{n,k}(\mathbb{F}_q[x])$ is *unimodular* if the greatest common divisor of all $r \times r$ minors of $\mathbf{A}$ is equal to 1 where $r = \min\{n, k\}$, i.e., $\mathbf{A}$ has all invariant factors equal to 1. We are interested in determining the number of matrices $A \in M_{n,k}(\mathbb{F}_q)$ having the property that the linear matrix polynomial $xI_{n,k} - A$ is unimodular (refer Question 1.1.1). This problem is equivalent to the following combinatorial matrix completion problem.

Question 2.3.1. Determine the number of matrices in $M_{n,k}(\mathbb{F}_q)$ that occur as the submatrix formed by the first k columns of some matrix in $M_n(\mathbb{F}_q)$ with irreducible characteristic polynomial.

As a corollary to the result of Wimmer [51] (also see [11, Thm. 15]) for the case of irreducible polynomial, the following proposition ([42, Cor. 2.2]) establishes the equivalence of Question 1.1.1 and Question 2.3.1.

Proposition 2.3.2. Let $A \in M_k(\mathbb{F}_q)$ and $C \in M_{n-k,k}(\mathbb{F}_q)$. The block matrix $\begin{bmatrix} A \\ C \end{bmatrix} \in M_{n,k}(\mathbb{F}_q)$ can be completed to a matrix in $M_n(\mathbb{F}_q)$ with irreducible characteristic polynomial if and only if all the invariant factors of

$$\begin{bmatrix} xI_k - A \\ -C \end{bmatrix}$$

are equal to 1.

Now we consider a sequence $\mathbf{x}_s$ which is widely used in many areas such as control systems, linear sequential machines, discrete automata theory and convolutional error correcting codes (see [12],[23],[44]). For a fixed column vector $\mathbf{x}_0$ in $\mathbb{F}_q$, we define the sequence $\mathbf{x}_s$ in $\mathbb{F}_q^k$ as

$$\mathbf{x}_{s+1} = A\mathbf{x}_s + B\mathbf{u}_s \ (s \geq 0),$$

where $A \in M_k(\mathbb{F}_q), B \in M_{k,n-k}(\mathbb{F}_q)$ are fixed and $\mathbf{u}_s (s \geq 0)$ is some sequence in $\mathbb{F}_q^{n-k}$. By using backward substitution, we can solve the recurrence for $\mathbf{x}_k$ and obtain

$$\mathbf{x}_k = A^k\mathbf{x}_0 + \begin{bmatrix} B & AB & \cdots & A^{k-1}B \end{bmatrix} \begin{bmatrix} \mathbf{u}_{k-1} \\ \mathbf{u}_{k-2} \\ \vdots \\ \mathbf{u}_0 \end{bmatrix}.$$

It is usually needed that $\mathbf{x}_k$ take all possible values in $\mathbb{F}_q^k$ by suitably varying the 'input sequence' $\mathbf{u}_s (0 \leq s \leq k-1)$. This is possible if and only if the

reachability matrix defined by

$$\mathcal{C}(A,B) := \begin{bmatrix} B & AB & \cdots & A^{k-1}B \end{bmatrix}$$

has full rank k. This leads to the definition of a reachable pair of matrices.

Definition 2.3.3. The ordered pair $(A,B) \in M_k(\mathbb{F}_q) \times M_{k,n-k}(\mathbb{F}_q)$ is said to be reachable if

$$\text{rank } \mathcal{C}(A,B) = k.$$

Kocięcki and Przyłuski [28] considered the following problem of counting the number of reachable pairs of matrices over finite fields.

Question 2.3.4. Determine the number of reachable pair of matrices (A,B) lying in $M_k(\mathbb{F}_q) \times M_{k.n-k}(\mathbb{F}_q)$.

This is an interesting problem and is equivalent to the problem of counting the number of zero kernel pairs (also called observable pair in the terminology of linear control theory).

Definition 2.3.5. The ordered pair $(C,A) \in M_{n-k,k}(\mathbb{F}_q) \times M_k(\mathbb{F}_q)$ is zero kernel pair ([42, def. 2.3] or [20, sec. X.1]) if

$$\bigcup_{i=0}^{k-1} \ker\,(CA^i) = \{\mathbf{0}\}.$$

Reachable pairs are related to zero kernel pairs by the following characterizations ([20, Thm. IX.3.3], [44, Thm. 23]) of zero kernel pairs.

Proposition 2.3.6. Let $A \in M_k(\mathbb{F}_q)$ and $C \in M_{n-k,k}(\mathbb{F}_q)$. Then the following statements are equivalent:

1. The pair (C,A) is zero kernel pair.

2. The product of invariant factors of

$$\begin{bmatrix} xI_k - A \\ -C \end{bmatrix}$$

is 1.

3. The block matrix

$$\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{k-1} \end{bmatrix}$$

has rank k.

Proposition 2.3.6 implies that (C, A) is zero kernel pair if and only if (A^T, C^T) is reachable. This shows the duality between reachable and zero kernel pairs of matrices. Proposition 2.3.6 further shows that Question 2.3.4 is equivalent to solving Question 1.1.1 and hence Question 2.3.1.

The above problems are further equivalent to the problem of counting the number of simple linear transformations. We first recall the notion of a simple linear transformation [42, Def. 3.1].

Definition 2.3.7. Let V denote a vector space over a field F and let W be a subspace of V. An F-linear transformation $T : W \to V$ is *simple* if the only T-invariant subspace properly contained in V is the zero subspace.

Remark 2.3.8. Note that the definition requires that there are no T-invariant subspaces properly contained in V rather than in W. The reason being that if W is a proper subspace, then the definition does not allow W itself to be T-invariant. In the case $W = V$ we necessarily have that W is T-invariant. It can be shown that a linear operator T on a finite dimensional vector space V is simple if and only if it has an irreducible characteristic polynomial. In fact simple maps defined

on a proper subspace W of a vector space V are precisely the restrictions to W of simple maps defined on all of V.

Question 2.3.9. Let V be an n-dimensional vector space over $\mathbb{F}_q$ and suppose W is a fixed k-dimensional subspace of V. Determine the number of simple linear transformations T defined on the subspace W of V.

The following proposition [42, Prop. 3.2] facilitates the connection between simple linear transformations and zero kernel pairs.

Proposition 2.3.10. Let W be a k-dimensional subspace of an n-dimensional vector space over $\mathbb{F}_q$. Let $\mathcal{B}_k$ be a fixed ordered basis for W and let $\mathcal{B}_n$ be an extension of the basis $\mathcal{B}_k$ to an ordered basis of V. Then, a linear transformation $T : W \to V$ is simple if and only if the matrix of T with respect to the bases $\mathcal{B}_k$ and $\mathcal{B}_n$ is of the form $\begin{bmatrix} A \\ C \end{bmatrix}$ for some zero kernel pair (C, A).

Proposition 2.3.10 shows that counting zero kernel pair is equivalent to counting simple maps and establishes the equivalence of Question 2.3.4 and 2.3.9. Thus Questions 1.1.1, 2.3.1, 2.3.4 and 2.3.9 are equivalent and have the same answer given by $\prod_{i=1}^{k}(q^n - q^i)$. By applying our results, we give two different solutions of Question 1.1.1 in Chapter 3 and Chapter 5.

Chapter 3

Unimodular Polynomial Matrices over Finite Fields

3.1 Introduction

As discussed in the introduction to this thesis, the notion of unimodularity has been well studied during the last decade. In Chapter 2, we discussed the connection of Question 1.1.1 of determining the number of linear unimodular matrix polynomials with other interesting enumeration problems. The question was fully answered only recently by Lieb, Jordan and Helmke [33, Thm. 1] who showed that the answer is equal to $\prod_{i=1}^{k}(q^n - q^i)$. The objective of this chapter is to give a new proof of Question 1.1.1 by first proving our main result Lemma 3.2.9. The proof of our main lemma relies on a control theoretic result of Brunovský on completely controllable pairs and uses some elementary methods in linear algebra.

3.2 Simple Linear Transformations

We begin by recalling the notion of a simple linear transformation.

Definition 3.2.1. Let V denote a vector space over a field F and let W be a

subspace of V. An F-linear transformation $T : W \to V$ is *simple* if the only T-invariant subspace properly contained in V is the zero subspace.

The following proposition elucidates the connection between simple linear transformations and unimodularity.

Proposition 3.2.2. Let V be an n-dimensional vector space over F with ordered basis $\mathcal{B}_n = \{v_1, \ldots, v_n\}$. Let $\mathcal{B}_k = \{v_1, \ldots, v_k\}$ denote the ordered basis for the subspace W spanned by $v_1, \ldots, v_k$. Let $T : W \to V$ be a linear transformation and let $Y \in M_{n,k}(F)$ denote the matrix of T with respect to $\mathcal{B}_k$ and $\mathcal{B}_n$. Then T is simple if and only if $xI_{n,k} - Y$ is unimodular.

Proof. See [42, Prop. 2.5] and [42, Prop. 3.2]. □

Let m be a positive integer and let $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ be an arbitrary but fixed nonzero vector. Let t be the largest index such that $a_t \neq 0$. Let $d_1 \geq d_2 \geq \cdots \geq d_m$ be a nonincreasing sequence of integers with $d_t \geq -1$. Let $N_{\mathbf{a}}(d_1, \ldots d_m)$ denote the number of m-tuples $(f_1, \ldots, f_m)$ of polynomials over $\mathbb{F}_q$ such that $f_i = a_i x^{d_i+1} + h_i$ and $\deg h_i \leq d_i$ for $1 \leq i \leq m$ with $\gcd(f_1, \ldots, f_m) = 1$. Here we interpret negative powers of x to be zero. Since $a_t \neq 0$, we necessarily have $\deg f_t = d_t + 1$ for any tuple $(f_1, \ldots, f_m) \in N_{\mathbf{a}}(d_1, \ldots, d_m)$. We adopt the convention that the degree of the zero polynomial is $-\infty$. Note that if there is some $s \geq t$ such that $d_i < 0$ for each $s < i \leq m$, then $N_{\mathbf{a}}(d_1, \ldots, d_m) = N_{\mathbf{a}'}(d_1, \ldots, d_s)$ where $\mathbf{a}' = (a_1, \ldots, a_s)$.

We adapt an argument in the proof of [16, Thm. 4.1] to prove the following lemma which is central to our main result.

Lemma 3.2.3. Let m be a positive integer and let $d_1 \geq d_2 \geq \cdots \geq d_m \geq 0$ be a sequence of integers. Let $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ be a fixed nonzero vector. We have

$$N_{\mathbf{a}}(d_1, \ldots, d_m) = q^{k+m} - q^{k+1},$$

where $k = d_1 + \cdots + d_m$.

Proof. Fix a positive integer m. Let $S(d_1, \ldots, d_m)$ denote the set of ordered m-tuples $(f_1, \ldots, f_m)$ where $f_i = a_i x^{d_i+1} + h_i$ for some h_i with $\deg h_i \leq d_i$ for $1 \leq i \leq m$. Let t be the largest index such that $a_t \neq 0$. We partition $S(d_1, \ldots, d_m)$ into disjoint subsets $S_0, S_1, \ldots, S_{d_t+1}$ where the set S_d $(0 \leq d \leq d_t + 1)$ denotes the set of m-tuples in $S(d_1, \ldots, d_m)$ whose GCD is a monic polynomial of degree d. For each monic polynomial h over $\mathbb{F}_q$ of degree d and any coprime m-tuple $(g_1, \ldots, g_m)$ of polynomials in $S(d_1 - d, \ldots, d_m - d)$, it is easy to see that $(g_1 h, g_2 h, \ldots, g_m h) \in S_d$. Conversely, for any tuple $(f_1, \ldots, f_m) \in S_d$, the polynomial $h = \gcd(f_1, \ldots, f_m)$ is monic of degree d and $(f_1/h, \ldots, f_m/h)$ is an ordered m-tuple of coprime polynomials in $S(d_1 - d, \ldots, d_m - d)$. As a result, we have $|S_d| = q^d N_{\mathbf{a}}(d_1 - d, \ldots, d_m - d)$ for $0 \leq d \leq d_t + 1$. For $k = d_1 + \cdots + d_m$, we have

$$q^{k+m} = \sum_{d=0}^{d_t+1} |S_d| = \sum_{d=0}^{d_t+1} q^d N_{\mathbf{a}}(d_1 - d, \ldots, d_m - d). \tag{3.1}$$

Replacing d_i by $d_i + 1$ for each $1 \leq i \leq m$, we obtain

$$\begin{aligned} q^{k+2m} &= \sum_{d=0}^{d_t+2} q^d N_{\mathbf{a}}(d_1 + 1 - d, \ldots, d_m + 1 - d) \\ &= \sum_{d=-1}^{d_t+1} q^{d+1} N_{\mathbf{a}}(d_1 - d, \ldots, d_m - d) \\ &= N_{\mathbf{a}}(d_1 + 1, \ldots, d_m + 1) + q \sum_{d=0}^{d_t+1} q^d N_{\mathbf{a}}(d_1 - d, \ldots, d_m - d) \\ &= N_{\mathbf{a}}(d_1 + 1, \ldots, d_m + 1) + q(q^{k+m}), \end{aligned}$$

where the last equality follows from (3.1). It follows that $N_{\mathbf{a}}(d_1+1, \ldots, d_m+1) = q^{k+2m}(1 - q^{1-m})$, or equivalently, $N_{\mathbf{a}}(d_1, \ldots, d_m) = q^{k+m} - q^{k+1}$ as desired. □

As the language of control theory is used in the proof of our main result we collate here a few definitions [20, IX.2] and results that are referred to later on. In what follows, F denotes an arbitrary field and k, ℓ are fixed positive integers.

Definition 3.2.4. A matrix pair $(A, B) \in M_{k,k}(F) \times M_{k,\ell}(F)$ is a *reachable pair* if the $k \times k\ell$ matrix $S(A,B) := \begin{bmatrix} B & AB & \cdots & A^{k-1}B \end{bmatrix}$ has rank equal to k.

Remark 3.2.5. A pair (A, B) is reachable if and only if the polynomial matrix $[xI_k - A \; B]$ is unimodular.

Definition 3.2.6. Associate with each pair $(A, B) \in M_{k,k}(F) \times M_{k,\ell}(F)$ a sequence of integers $p_i (i \geq 1)$ by defining $p_1 := \text{rank } B$ and for $i \geq 2$,

$$p_i := \text{rank} \begin{bmatrix} B & AB & \cdots & A^{i-1}B \end{bmatrix} - \text{rank} \begin{bmatrix} B & AB & \cdots & A^{i-2}B \end{bmatrix}.$$

Consider the dual sequence $k_j (j \geq 1)$ defined by $k_j = \#\{r : p_r \geq j\}$. The numbers $k_1, \ldots, k_\ell$ are called the *controllability indices* of the pair (A, B).

For any positive integer m, denote by $\text{GL}_m(F)$ the general linear group of $m \times m$ nonsingular matrices over F. Define [52, P. 3]

$$\Gamma_{k,\ell} := \left\{ \begin{bmatrix} P & \mathbf{0} \\ R & Q \end{bmatrix} \in \text{GL}_{k+\ell}(F) : P \in \text{GL}_k(F), Q \in \text{GL}_\ell(F), R \in M_{\ell,k}(F) \right\}.$$

Definition 3.2.7. Two pairs (A_1, B_1) and (A_2, B_2) in $M_{k,k}(F) \times M_{k,\ell}(F)$ are said to be $\Gamma_{k,\ell}$-equivalent [52, Def. 2.1] if there exists a matrix $P \in \Gamma_{k,\ell}$ such that for each pair of matrices $C_1 \in M_{\ell,k}(F)$ and $D_1 \in M_\ell(F)$, there exist matrices $C_2 \in M_{\ell,k}(F)$ and $D_2 \in M_\ell(F)$ such that

$$P \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix} P^{-1} = \begin{bmatrix} A_2 & B_2 \\ C_2 & D_2 \end{bmatrix}.$$

When the values of k, ℓ are clear from the context, we refer to $\Gamma_{k,\ell}$-equivalence simply as Γ-equivalence. The following result ([7], [52, Lem. 2.7]) is due to Brunovsky.

Theorem 3.2.8. Let $(A, B) \in M_{k,k}(F) \times M_{k,\ell}(F)$. Suppose (A, B) is a reachable pair with $\operatorname{rank} B = r$ and $k_1 \geq \cdots \geq k_r > k_{r+1} = \cdots = k_\ell (= 0)$ are the controllability indices of (A, B). Then (A, B) is Γ-equivalent to a pair $(A_c, B_c) \in M_{k,k}(F) \times M_{k,\ell}(F)$ of the following form:

i) A_c is the block diagonal matrix $\operatorname{diag}(A_1, \ldots, A_r)$ where A_i is the $k_i \times k_i$ matrix

$$\begin{bmatrix} \mathbf{0} & I_{k_i-1} \\ 0 & \mathbf{0} \end{bmatrix};$$

ii) B_c is of the block form $[B' \; \mathbf{0}]$, where B' denotes the $k \times r$ matrix

$$B' = \begin{bmatrix} E_1 \\ \vdots \\ E_r \end{bmatrix}; \text{ where } E_i = \begin{bmatrix} \mathbf{0} \\ e_i \end{bmatrix} \in M_{k_i \times r}(F),$$

and e_i denotes the i^{th} row of the $r \times r$ identity matrix.

The following lemma is our main result.

Lemma 3.2.9. Let n, k be integers with $0 \leq k < n - 1$. Let V be an n-dimensional vector space over $\mathbb{F}_q$ and let W, W' be fixed subspaces of V of dimensions k and $k + 1$ respectively with $W \subset W'$. Suppose $T : W \to V$ is a simple linear transformation. Then the number of simple linear transformations $T' : W' \to V$ such that $T'_{|W} = T$ (the restriction of T' to W is T) is equal to $q^n - q^{k+1}$.

Proof. First suppose $k = 0$. In this case W' is spanned by some nonzero vector $w \in V$. Then T' is simple precisely when $T'(w)$ does not lie in the span of w. So the number of such linear transformations is clearly $q^n - q$.

Suppose $k \geq 1$. Let $\mathcal{B}_k = \{v_1, \ldots, v_k\}$ be an ordered basis for W and $\mathcal{B}_n = \{v_1, \ldots, v_n\}$ be an ordered basis for V obtained by extending $\mathcal{B}_k$. Let Y be the matrix of T with respect to $\mathcal{B}_k$ and $\mathcal{B}_n$. Since T is simple, $\mathbf{Y} = xI_{n,k} - Y$

is unimodular by Proposition 3.2.2. Suppose that $Y = \begin{bmatrix} A \\ C \end{bmatrix}$ for some $A \in M_{k,k}(\mathbb{F}_q)$ and $C \in M_{n-k,k}(\mathbb{F}_q)$. Since $\mathbf{Y} = xI_{n,k} - Y$ is unimodular, it follows by Remark 3.2.5 that (A^t, C^t) is a reachable pair. Suppose that $\operatorname{rank}(C) = r$, and $k_1 \geq k_2 \geq \cdots \geq k_r > k_{r+1} = \cdots = k_{n-k} = 0$ are the controllability indices of the pair (A^t, C^t). We have $k_1 + \cdots + k_r = k$. By Theorem 3.2.8 we may assume that A and C are of the following form:

$A = \operatorname{diag}(A_1, A_2, \ldots, A_r)$, where A_i is the $k_i \times k_i$ matrix $\begin{bmatrix} \mathbf{0} & 0 \\ I_{k_i-1} & \mathbf{0} \end{bmatrix}$;

$C = \begin{bmatrix} C' \\ \mathbf{0} \end{bmatrix}$, where $C' = [E_1 \cdots E_r] \in M_{r,k}(\mathbb{F}_q)$ with $E_i = [\mathbf{0}\, e_i] \in M_{r,k_i}(\mathbb{F}_q)$, and e_i denotes the i^{th} column of the $r \times r$ identity matrix for $1 \leq i \leq r$. Let $\lambda_s = \sum_{i=1}^{s} k_i$ for $1 \leq s \leq r$ and set $\lambda_0 = 0$. Then the linear transformation T can be described by

$$T(v_j) = \begin{cases} v_{k+s} & \text{if } j = \lambda_s \text{ for some } s,\ 1 \leq s \leq r; \\ v_{j+1} & \text{otherwise,} \end{cases} \tag{3.2}$$

where $1 \leq j \leq k$. Also the matrix Y can be described by

$$Y = [\mathbf{e}_{\lambda_0+2}, \ldots, \mathbf{e}_{\lambda_1}, \mathbf{e}_{k+1}, \mathbf{e}_{\lambda_1+2}, \ldots, \mathbf{e}_{\lambda_2}, \mathbf{e}_{k+2}, \ldots, \mathbf{e}_{\lambda_{r-1}+2}, \ldots, \mathbf{e}_{\lambda_r}, \mathbf{e}_{k+r}],$$

where $\mathbf{e}_i$ is the i^{th} column of the identity matrix I_n. Let $U = \operatorname{span}(\mathcal{B}_n \setminus \mathcal{B}_k)$ be the subspace of V spanned by $\{v_{k+1}, \ldots, v_n\}$. We have $V = W \oplus U$.

Now $W \subset W'$ and W' is of dimension $k+1$. Since $V = W \oplus U$, there is a nonzero vector $w \in W' \cap U$. Let $\{v'_{k+1} = w, v'_{k+2}, \ldots, v'_n\}$ be an ordered basis for U. Since $V = W \oplus U$, we have $\mathcal{B}'_n = \{v_1, \ldots, v_k, v'_{k+1}, \ldots, v'_n\}$ is an ordered basis for V. Let R be the matrix of the identity map 1_V on V with respect to

the bases $\mathcal{B}'_n$ and $\mathcal{B}_n$. Note that the matrix R can be expressed as

$$\begin{bmatrix} I_k & \mathbf{0} \\ \mathbf{0} & S \end{bmatrix},$$

where S is the matrix of the identity map 1_U on U with respect to the bases $\mathcal{B}'_n \setminus \mathcal{B}_k$ and $\mathcal{B}_n \setminus \mathcal{B}_k$. Let $v'_{k+1} = \sum_{j=k+1}^{n} c_j v_j$ for some scalars c_j. Then the first column of S is given by $(c_{k+1}, \ldots, c_n)^t \in \mathbb{F}_q^{n-k}$. The matrix $\tilde{Y}$ of T with respect to $\mathcal{B}_k$ and $\mathcal{B}'_n$ is given by $\tilde{Y} = R^{-1}Y$. Define $\mathcal{B}'_{k+1} = \{v_1, \ldots, v_k, v'_{k+1}\}$ and let Y' be the matrix of T' with respect to the bases $\mathcal{B}'_{k+1}$ and $\mathcal{B}'_n$. Since $T'_{|W} = T$ we have $Y' = R^{-1}[Y\ \mathbf{b}]$ for some column vector $\mathbf{b} \in \mathbb{F}_q^n$. By Proposition 3.2.2, T' is simple if and only if $\mathbf{Y}' = xI_{n,k+1} - Y'$ is unimodular. Let $\mathbf{Y_b} = R\mathbf{Y}' = R(xI_{n,k+1} - R^{-1}[Y\ \mathbf{b}]) = xR_{k+1} - [Y\ \mathbf{b}]$, where R_{k+1} is the submatrix formed by the first $(k+1)$ columns of R. We have $\mathbf{Y_b} = [\mathbf{Y}\ x\mathbf{c} - \mathbf{b}]$, where $\mathbf{c} = (0, \ldots, 0, c_{k+1}, \ldots, c_n)^t \in \mathbb{F}_q^n$.

Suppose $\mathbf{b} = (b_1, b_2, \ldots, b_n)^t \in \mathbb{F}_q^n$. Then the matrix $Y_\mathbf{b} = [Y\ \mathbf{b}]$ is of the form

$$Y_\mathbf{b} = \begin{bmatrix} A_1 & \mathbf{0} & \ldots & \mathbf{0} & \mathbf{b}_1 \\ \mathbf{0} & A_2 & \ldots & \mathbf{0} & \mathbf{b}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & A_r & \mathbf{b}_r \\ E_1 & E_2 & \ldots & E_r & \tilde{\mathbf{b}} \\ \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & \hat{\mathbf{b}} \end{bmatrix}, \tag{3.3}$$

where $\mathbf{b}_i = (b_{\lambda_{i-1}+1}, \ldots, b_{\lambda_i})^t \in \mathbb{F}_q^{k_i}$ for $1 \leq i \leq r$, $\tilde{\mathbf{b}} = (b_{k+1}, \ldots, b_{k+r})^t \in \mathbb{F}_q^r$, and $\hat{\mathbf{b}} = (b_{k+r+1}, \ldots, b_n)^t \in \mathbb{F}_q^{n-k-r}$.

Now consider the polynomial matrix $\mathbf{Y_b} = [\mathbf{Y}\ x\mathbf{c} - \mathbf{b}]$. We permute the rows of $\mathbf{Y_b}$ in the following way: for each $1 \leq i \leq r-1$, arrange the $(k+i)^{\text{th}}$ row of $\mathbf{Y_b}$ in between the i^{th} and $(i+1)^{\text{th}}$ block rows appearing in (3.3). The resulting

matrix $\mathbf{Z}$ is of the following form:

$$\mathbf{Z} = \begin{bmatrix} \mathbf{Z}_1 & \mathbf{0} & \dots & \mathbf{0} & \mathbf{b}'_1 \\ \mathbf{0} & \mathbf{Z}_2 & \dots & \mathbf{0} & \mathbf{b}'_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{Z}_r & \mathbf{b}'_r \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{b}' \end{bmatrix}, \tag{3.4}$$

where $\mathbf{Z}_i = x \begin{bmatrix} I_{k_i} \\ \mathbf{0} \end{bmatrix} - \begin{bmatrix} \mathbf{0} \\ I_{k_i} \end{bmatrix}$, $\mathbf{b}'_i = \begin{bmatrix} -\mathbf{b}_i \\ c_{k+i}x - b_{k+i} \end{bmatrix}$ for $1 \leq i \leq r$ and $\mathbf{b}' = (c_{k+r+1}x - b_{k+r+1}, \dots, c_n x - b_n)^t$. Now we apply the following sequence of elementary row operations to $\mathbf{Z}$ to eliminate x in the first k columns: in the first block row appearing in (3.4), add x times the $(i+1)^{\text{th}}$ row to the i^{th} row successively for $i = k_1, k_1 - 1, \dots, 1$ in that order. Similarly we apply elementary row operations to the other block rows. By appropriate elementary column operations, the entries in the last column can be made zero at suitable positions. Eventually we can transform the matrix to the following form:

$$\mathbf{Z}' = \begin{bmatrix} \mathbf{Z}'_1 & \mathbf{0} & \dots & \mathbf{0} & \mathbf{b}''_1 \\ \mathbf{0} & \mathbf{Z}'_2 & \dots & \mathbf{0} & \mathbf{b}''_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{Z}'_r & \mathbf{b}''_r \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{b}' \end{bmatrix}, \tag{3.5}$$

where $\mathbf{Z}'_i = -\begin{bmatrix} \mathbf{0} \\ I_{k_i} \end{bmatrix}$, $\mathbf{b}''_i = \begin{bmatrix} f_i \\ \mathbf{0} \end{bmatrix}$ with $f_i(x) = c_{k+i}x^{k_i+1} - b_{k+i}x^{k_i} - \sum_{j=1}^{k_i} b_{\lambda_{i-1}+j}x^{j-1}$ for $1 \leq i \leq r$ and $\mathbf{b}' = (c_{k+r+1}x - b_{k+r+1}, \dots, c_n x - b_n)^t$.

Let $g = \gcd(f_1, f_2, \dots, f_r, c_{k+r+1}x - b_{k+r+1}, \dots, c_n x - b_n)$. The matrix $\mathbf{Z}'$ is unimodular if and only if $g = 1$. By Lemma 3.2.3 it follows that the number of vectors $\mathbf{b} \in \mathbb{F}_q^n$ such that $g = 1$ is given by $q^n - q^{k+1}$. As $\mathbf{Y}'$ and $\mathbf{Z}'$ are equivalent,

the result follows.

□

The lemma can be recast in the setting of matrices as follows.

Corollary 3.2.10. Let $Y \in M_{n,k}(\mathbb{F}_q)$ be such that the linear matrix polynomial $xI_{n,k} - Y$ is unimodular. For each column vector $\mathbf{b} \in \mathbb{F}_q^n$ let $Y_{\mathbf{b}} = [Y \ \mathbf{b}] \in M_{n,k+1}(\mathbb{F}_q)$. Then the number of column vectors $\mathbf{b} \in \mathbb{F}_q^n$ for which $xI_{n,k+1} - Y_{\mathbf{b}}$ is unimodular equals $q^n - q^{k+1}$.

We can now give an alternate proof of [42, Thm. 3.8] concerning the number of simple linear transformations with a fixed domain.

Corollary 3.2.11. Let V be an n-dimensional vector space over $\mathbb{F}_q$ and W be a proper k-dimensional subspace of V. The number of simple linear transformations $T : W \to V$ equals

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

We may use Proposition 3.2.2 to reformulate the corollary in terms of matrices. This allows us to answer Question 1.1.1 stated in the introduction.

Corollary 3.2.12. Let n, k be positive integers with $k < n$. The number of matrices $A \in M_{n,k}(\mathbb{F}_q)$ such that $xI_{n,k} - A$ is unimodular equals

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

By repeated application of Corollary 3.2.10 we obtain the following extension which is used later on in Sections 4.2 and 4.3.

Lemma 3.2.13. Let n, k, t be positive integers such that $k + t < n$. Suppose that the matrix polynomial $xI_{n,k} - Y$ is unimodular for some $Y \in M_{n,k}(\mathbb{F}_q)$. The number of matrices $A \in M_{n,t}(\mathbb{F}_q)$ such that the matrix polynomial

$$xI_{n,k+t} - [Y \ A]$$

is unimodular is equal to $\prod_{i=1}^{t}(q^n - q^{k+i})$.

Chapter 4

Unimodular Polynomial Matrices and Splitting Subspaces

4.1 Introduction

It is a well-known property of the finite field that finite dimensional vector spaces over them naturally possess a canonical and compatible field structure. More precisely, we can write $\mathbb{F}_q^n \simeq \mathbb{F}_{q^n}$. This leads to interesting concepts connecting the field structure and the linear structure, that of which is of *splitting subspace* stemming from the work of Niederreiter (1995) [36] on pseudorandom number generation. Recall the definition of splitting subspace given earlier in the Chapter 1.

Definition 4.1.1. Let d, m be positive integers and consider the vector space $\mathbb{F}_{q^{md}}$ over $\mathbb{F}_q$. For any element $\alpha \in \mathbb{F}_{q^{md}}$ an m-dimensional subspace W of $\mathbb{F}_{q^{md}}$ is α-*splitting* if

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

For example, for any $\alpha \in \mathbb{F}_{q^{md}}$ such that $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$, $\{1, \alpha^d, \alpha^{2d}, \ldots, \alpha^{(m-1)d}\}$

spans an m-dimensional α-splitting subspace. If $d = 1$, then $\mathbb{F}_{q^{md}} = \mathbb{F}_{q^m}$ is the only α-splitting subspace; and if $m = 1$ with $\alpha \in \mathbb{F}_{q^{md}} = \mathbb{F}_{q^d}$ such that $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$, then every 1-dimensional subspace is α-splitting.

In this chapter, we provide an alternate proof of the Splitting Subspace Theorem (stated below) which answers a question considered by Niederreiter [36, p.11], stated and conjectured by Ghorpade and Ram [18, Conj. 5.5] and originally resolved by Chen and Tseng [8, Cor. 3.4].

Theorem 4.1.2 (Splitting Subspace Theorem)**.** For any $\alpha \in \mathbb{F}_{q^{md}}$ such that $\mathbb{F}_{q^{md}} = \mathbb{F}_q(\alpha)$, the number of α-splitting subspaces of $\mathbb{F}_{q^{md}}$ of dimension m is precisely

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

Using a control-theoretic result of Wimmer (Theorem 4.2.7) and results on unimodular matrix polynomials in Chapter 3, we prove Theorem 4.2.8 from which the Splitting Subspace Theorem follows as a corollary.

In the last section, we consider a generalization of Question 1.1.1 which shows that for a uniformly random matrix $A \in M_{n,k}(\mathbb{F}_q)$, the probability that $xI_{n,k} - A$ is unimodular is given by $\prod_{i=1}^{k}(1-q^{i-n})$. Using results from Chapter 3, we prove a more general result Theorem 4.3.1 on the density of unimodular polynomial matrices which was earlier conjectured in [42].

4.2 The Splitting Subspace Theorem

We first define the notion of block companion matrices which are closely related to splitting subspaces.

Definition 4.2.1. For positive integers m, d, an (m, d)-block companion matrix

over $\mathbb{F}_q$ is a matrix in $M_{md}(\mathbb{F}_q)$ of the form

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & C_0 \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & C_1 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & C_{d-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & C_{d-1} \end{pmatrix}, \tag{4.1}$$

where $C_0, C_1, \ldots, C_{d-1} \in M_m(\mathbb{F}_q)$ and I_m denotes the $m \times m$ identity matrix over $\mathbb{F}_q$ while $\mathbf{0}$ denotes the zero matrix in $M_m(\mathbb{F}_q)$.

Remark 4.2.2. It was shown (see the discussion after Conjecture 5.5 in [18] or Appendix A in [19] for an overview) that the Splitting Subspace Theorem is in fact equivalent to the following theorem on block companion matrices.

Theorem 4.2.3. For any irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree md, the number of (m, d)-block companion matrices over $\mathbb{F}_q$ having f as their characteristic polynomial equals

$$q^{m(m-1)(d-1)} \prod_{i=1}^{m-1} (q^m - q^i).$$

It is noteworthy that the problem of counting specific types of block companion matrices having irreducible characteristic polynomial has been considered in other contexts [9, 26, 41] where pseudorandom number generation is of interest. We now deduce Theorem 4.2.3 as a special case of Theorem 4.2.8 which we prove below, thereby providing an alternate proof of the Splitting Subspace Theorem.

Definition 4.2.4. For positive integers k, ℓ with $k < \ell$, let $J^{\ell,k}$ denote the $\ell \times k$ matrix given by

$$J^{\ell,k} := \begin{bmatrix} \mathbf{0} \\ I_k \end{bmatrix}.$$

Lemma 4.2.5. The linear matrix polynomial

$$x \begin{bmatrix} I_k \\ \mathbf{0} \end{bmatrix} - J^{\ell,k}$$

is unimodular.

Proof. Since the $k \times k$ minor formed by the last k rows of the above matrix polynomial equals $(-1)^k$ it follows that the GCD of all $k \times k$ minors is 1. □

Definition 4.2.6. Let m, ℓ be positive integers such that $m < \ell$. An m-companion matrix of order ℓ over $\mathbb{F}_q$ is a square matrix C of the form

$$C = [J^{\ell,\ell-m} \; A]$$

for some $A \in M_{\ell,m}(\mathbb{F}_q)$. We denote the set of all m-companion matrices of order ℓ over $\mathbb{F}_q$ by $\mathcal{C}(\ell, m; q)$. Note that $|\mathcal{C}(\ell, m; q)| = q^{\ell m}$.

Let $\mathcal{P}(\ell, \mathbb{F}_q)$ denote the set of all monic polynomials of degree ℓ over $\mathbb{F}_q$. Now consider the map $\Phi : \mathcal{C}(\ell, m; q) \to \mathcal{P}(\ell, \mathbb{F}_q)$ given by

$$\Phi(C) := \det(xI_\ell - C).$$

To determine the size of the fibers of Φ, we require a theorem of Wimmer.

Theorem 4.2.7 (Wimmer)**.** Let F be an arbitrary field and let $Y \in M_{\ell,k}(F)$. Suppose $f \in F[x]$ is a monic polynomial of degree ℓ and let $f_1(x) \mid \cdots \mid f_k(x)$ be the invariant factors of the polynomial matrix $xI_{\ell,k} - Y$. There exists a matrix $Z \in M_{\ell,\ell-k}(F)$ such that the block matrix $[Y \; Z]$ has characteristic polynomial $f(x)$ if and only if the product $\prod_{i=1}^{k} f_i(x)$ divides $f(x)$.

Proof. See Wimmer [51] or Cravo [11, Thm. 15]. □

Theorem 4.2.8. Suppose that $f \in \mathcal{P}(\ell, \mathbb{F}_q)$ is irreducible. Then

$$|\Phi^{-1}(f)| = \prod_{t=1}^{m-1} (q^\ell - q^{\ell-t}).$$

Proof. Let $C = [J^{\ell,\ell-m}\ A] \in \mathcal{C}(\ell, m; q)$ with $A = [\mathbf{a}_1\ \mathbf{a}_2 \cdots \mathbf{a}_{m-1}\, \mathbf{a}_m]$, where the $\mathbf{a}_i$'s are the columns of A. Let $C_0 = J^{\ell,\ell-m}$ and let $C_i = [J^{\ell,\ell-m}\ \mathbf{a}_1\ \mathbf{a}_2 \cdots \mathbf{a}_i]$ denote the submatrix of C formed by the first $\ell - m + i$ columns for $1 \leq i < m$. Suppose that $\Phi(C) = f$. Since f is irreducible, it follows by Lemma 4.2.5 and Wimmer's theorem that the linear matrix polynomials

$$x \begin{bmatrix} I_{\ell-m+i} \\ \mathbf{0} \end{bmatrix} - C_i \tag{4.2}$$

are unimodular for $0 \leq i \leq m-1$. Conversely, if $\mathbf{a}_1, \ldots, \mathbf{a}_{m-1}$ are chosen such that the matrix polynomials in (4.2) are unimodular, then there is a unique choice of $\mathbf{a}_m$ for which $\Phi(C) = f$. This follows since there are q^ℓ total choices for $\mathbf{a}_m$ and for each monic polynomial g of degree ℓ, Wimmer's theorem ensures that there exists some choice of $\mathbf{a}_m$ such that the characteristic polynomial is g. By Lemma 3.2.13 it follows that the number of choices for the first $m-1$ columns of A is equal to $\prod_{i=1}^{m-1}(q^\ell - q^{\ell-m+i})$ which proves the result. □

Remark 4.2.9. In the case where m divides ℓ, say $d = \ell/m$, the set $\mathcal{C}(\ell, m; q)$ consists precisely of all (m, d)-block companion matrices over $\mathbb{F}_q$. This observation yields the following corollary stated earlier as Theorem 4.2.3.

Corollary 4.2.10. For any irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree md, the number of (m, d)-block companion matrices over $\mathbb{F}_q$ having f as their characteristic polynomial equals

$$q^{m(m-1)(d-1)} \prod_{i=1}^{m-1} (q^m - q^i).$$

Proof. It follows by the above remark that the number of (m, d)-block companion matrices over $\mathbb{F}_q$ having f as their characteristic polynomial equals

$$\prod_{i=1}^{m-1}(q^{md} - q^{m(d-1)+i}) = \prod_{i=1}^{m-1} q^{m(d-1)}(q^m - q^i),$$

which is clearly equal to the given product. □

In light of the above corollary and Remark 4.2.2 we can view Theorem 4.2.8 as a more general result than the Splitting Subspace Theorem. While our proof relies on results in control theory, it is shorter than the proofs of the theorem appearing in [8] and [29].

4.3 Probability of Unimodular Polynomial Matrices

We apply Lemma 3.2.13 to positively resolve a conjecture [42, Conj. 4.1] concerning the number of unimodular polynomial matrices. For positive integers d, k, n with $k < n$, define

$$M_{n,k}(\mathbb{F}_q[x]; d) := \left\{ \mathbf{A} = x^d I_{n,k} + \sum_{i=0}^{d-1} x^i A_i \ : \ A_i \in M_{n,k}(\mathbb{F}_q) \text{ for } 0 \leq i \leq d-1 \right\}.$$

Theorem 4.3.1. The probability that a uniformly random element of the set $M_{n,k}(\mathbb{F}_q[x]; d)$ is unimodular is given by $\prod_{i=1}^{k}(1 - q^{i-n})$.

Proof. To each element $\mathbf{A}$ in $M_{n,k}(\mathbb{F}_q[x]; d)$, we associate the corresponding d-tuple of its coefficients $(A_0, A_1, \ldots, A_{d-1}) \in [M_{n,k}(\mathbb{F}_q)]^d$. Now consider the matrix

$$B = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & -A_0 \\ I_n & \mathbf{0} & \ldots & \mathbf{0} & -A_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & I_n & -A_{d-1} \end{bmatrix} \tag{4.3}$$

of dimension $nd \times (nd - n + k)$. Let

$$\mathbf{B} = x \begin{bmatrix} I_{(d-1)n+k} \\ \mathbf{0} \end{bmatrix} - B.$$

By adding x times the i^{th} block row to the $(i-1)^{\text{th}}$ block row successively for $i = d, d-1, \ldots, 2$ in $\mathbf{B}$ and using suitable column block operations, we obtain

$$\mathbf{B}' = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & \mathbf{A} \\ I_n & \mathbf{0} & \ldots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & I_n & \mathbf{0} \end{bmatrix},$$

where $\mathbf{A} = x^d I_{n,k} + \sum_{i=0}^{d-1} x^i A_i \in M_{n,k}(\mathbb{F}_q[x]; d)$. Observe that $\mathbf{B}$ is equivalent to $\mathbf{B}'$. So the invariant factors of $\mathbf{B}$ and $\mathbf{B}'$ are the same. Therefore $\mathbf{B}$ is unimodular if and only if $\mathbf{A}$ is unimodular. By Lemma 3.2.13, the number of ways to choose the last k columns of the matrix B in (4.3) in such a way that $\mathbf{B}$ is unimodular is

$$\prod_{i=1}^{k} (q^{nd} - q^{n(d-1)+i}).$$

On the other hand, the cardinality of $M_{n,k}(\mathbb{F}_q[x]; d)$ is clearly q^{nkd} and therefore the probability that a uniformly random element of $M_{n,k}(\mathbb{F}_q[x]; d)$ is unimodular

is precisely $\prod_{i=1}^{k}(1-q^{i-n})$. □

Note that the probability computed in the theorem is independent of d.

Remark 4.3.2. The above theorem is a generalization of Corollary 3.2.12 which is evidently the special case $d = 1$.

Theorem 4.3.1 parallels a result of Guo and Yang [22, Thm. 1] who prove that the natural density of unimodular $n \times k$ matrices over $\mathbb{F}_q[x]$ is precisely $\prod_{i=1}^{k}(1-q^{i-n})$.

Remark 4.3.3. To study the invariant factors of an element $\mathbf{A} \in M_{n,k}(\mathbb{F}_q[x]; d)$, it suffices to study those of the corresponding linear matrix polynomial $\mathbf{B}$ associated to the matrix B as defined in Equation (4.3). The matrix polynomial $\mathbf{B}$ is called the linearization of $\mathbf{A}$.

Chapter 5

Enumerating partial linear transformations in a similarity class

5.1 Introduction

Let V be an n dimensional vector space over $\mathbb{F}_q$ and let W be a subspace of V. Let $L(W,V)$ denote the vector space of all $\mathbb{F}_q$-linear transformations from W to V. Recalling the definition of similar linear transformations from Chapter 1, we say that the two linear transformations $T \in L(W,V)$ and $\widetilde{T} \in L(\widetilde{W},V)$ defined on subspaces W and $\widetilde{W}$ of V respectively are similar if there exists a linear isomorphism $S : V \to V$ such that the following diagram commutes:

$$\begin{array}{ccc} W & \xrightarrow{T} & V \\ {\scriptstyle S_W}\downarrow & & \downarrow{\scriptstyle \simeq S} \\ \widetilde{W} & \xrightarrow{\widetilde{T}} & V \end{array}.$$

In other words, we must have $S \circ T = \widetilde{T} \circ S_W$ where S_W denotes the restriction of S to W. Let $\mathcal{L}(V)$ denote the union of the vector spaces $L(W,V)$ as W varies over all possible subspaces of V. Given $T \in \mathcal{L}(V)$ define $\mathcal{C}(T)$, the conjugacy

class of T, by

$$\mathcal{C}(T) := \{\widetilde{T} : \widetilde{T} \in \mathcal{L}(V),\ \widetilde{T} \text{ is similar to } T\}.$$

In this chapter, we determine the cardinality of $\mathcal{C}(T)$ for an arbitrary linear map T. The case where T is a linear operator on V (the case $W = V$) is a well-studied problem. Two linear operators T and $\widetilde{T}$ on V are similar if and only if they have the same invariant factors. In this case, the problem of determining $|\mathcal{C}(T)|$ is equivalent to the problem of counting the number of $n \times n$ square matrices over a finite field in a conjugacy class. An explicit formula for the size of $\mathcal{C}(T)$ for an arbitrary linear operator T was given by Phillip Hall (see Section 2.2). On the other hand, rectangular matrices arise in many contexts in linear control theory and matrix completion problems and are also of considerable interest. We refer to Cravo [11, Thms. 15, 32] for specific examples of matrix completion problems. Thus, the case of an arbitrary linear transformation T is an intriguing combinatorial problem, and we extend the result on square matrices to the setting of rectangular matrices by giving an explicit counting formula for the size of the conjugacy class of an arbitrary transformation $T \in \mathcal{L}(V)$.

In contrast with the case of linear operators, the invariant factors do not form a complete set of similarity invariants for an arbitrary linear map defined only on a subspace. If two linear transformations $T \in L(W, V)$ and $\widetilde{T} \in L(\widetilde{W}, V)$ are similar, then they necessarily have the same invariant factors but the converse is not true in general. We first characterize the similarity invariants for a linear transformation T defined only on a subspace W of an n-dimensional vector space V in Section 5.2 (which we referred to as partial linear map). Accordingly, let $T \in \mathcal{L}(V)$ be a linear transformation and let U denote the maximal T-invariant subspace, and suppose $\dim U = d$. Interestingly, in this case the similarity classes are indexed by pairs $(\lambda, \mathcal{I})$ where λ is an integer partition of $n - d$ and $\mathcal{I}$ is an ordered set of monic polynomials corresponding to the invariant factors of the restriction of T to U. When the domain of T is all of V, the partition λ

above is empty and the similarity class $\mathcal{C}(T)$ is completely determined by the invariant factors of T. If $T \in \mathcal{L}(V)$ is simple with domain a proper subspace of V, then the maximal T-invariant subspace U is necessarily the zero subspace and therefore the similarity class of T is determined by the pair $(\lambda, \emptyset)$ for some integer partition λ of $\dim V$ with largest part $\dim V - \dim W$ where W is the domain of T. In Section 5.3, we determine the conjugacy class size for an arbitrary simple linear transformation $T \in \mathcal{L}(V)$. We finally extend our results to arbitrary transformations $T \in L(V)$ by considering the operator part and the simple part of T as defined in Section 5.4. In fact Hall's result on matrix conjugacy class size may be recovered from Theorem 5.4.6 as well as Corollaries 5.4.7 and 5.4.8.

Using our results in Section 5.3, we give another proof of the theorem of Lieb, Jordan and Helmke [33, Thm. 1] discussed in the previous chapters, which solves the problem of counting the number of zero kernel pairs of matrices or, equivalently, reachable linear systems over a finite field. Reachability is a fundamental notion that arises in the context of control systems, discrete automata theory, convolutional error correcting codes and linear sequential machines just to name a few (see [12, 23, 44]).

5.2 Similarity invariants for maps defined on a subspace

We begin by describing a complete set of similarity invariants for a linear map in $L(W, V)$. Given $T \in L(W, V)$, define a sequence of subspaces [20, sec. III.1] $W_i = W_i(T)(i \geq 0)$ by $W_0 = V, W_1 = W$ and

$$W_{i+1} = W_i \cap T^{-1}(W_i) = \{v \in W_i : Tv \in W_i\} \quad \text{for } i \geq 1.$$

The descending chain of subspaces $W_0 \supseteq W_1 \supseteq \cdots$ eventually stabilizes as the dimensions of the subspaces are nonnegative integers. Let $d_i = d_i(T) := \dim W_i$ for $i \geq 0$ and let

$$\ell = \ell(T) := \min\{i : W_i = W_{i+1}\}.$$

The subspace W_ℓ is clearly a T-invariant subspace which is evidently the maximal T-invariant subspace. Therefore the restriction T_{W_ℓ} of T to W_ℓ is a linear operator on W_ℓ. Denote by $\mathcal{I}_T$ the ordered set of invariant factors of T_{W_ℓ}. Since the characteristic polynomial of T_{W_ℓ} equals the product of the invariant factors of T_{W_ℓ}, it follows that

$$d_\ell = \deg \prod_{p \in \mathcal{I}_T} p.$$

Now define

$$\lambda_j = \lambda_j(T) := d_{j-1} - d_j \text{ for } 1 \leq j \leq \ell.$$

Definition 5.2.1. [20, p. 52] The integers $\lambda_j(T)(1 \leq j \leq \ell)$ are called the *defect dimensions* of T.

Lemma 5.2.2. For any $T \in \mathcal{L}(V)$, we have $\lambda_j(T) \geq \lambda_{j+1}(T)$ for $1 \leq j \leq \ell - 1$.

Proof. Let the subspaces $W_j(j \geq 1)$ be as above. Note that $T(W_j) \subseteq W_{j-1}$ for each j. Fix $j \geq 1$ and define a map $\varphi : W_j/W_{j+1} \to W_{j-1}/W_j$ by

$$\varphi(v + W_{j+1}) = Tv + W_j.$$

We claim that φ is well defined. Suppose $v_1 + W_{j+1} = v_2 + W_{j+1}$ for some $v_1, v_2 \in W_j$. Then $v_1 - v_2 \in W_{j+1}$ and consequently $T(v_1 - v_2) \in W_j$. Therefore $Tv_1 + W_j = Tv_2 + W_j$ proving that φ is well defined. The linearity of φ follows easily from the fact that T is linear. In fact φ is also injective. Suppose for some $v \in W_j$ we have

$$\varphi(v + W_{j+1}) = Tv + W_j = 0 + W_j.$$

Then $Tv \in W_j$ and since v itself lies in W_j, it follows that $v \in W_{j+1}$ as well. Thus

$v + W_{j+1}$ is the zero element in W_j/W_{j+1} and φ is injective. The injectivity of φ implies that $\dim(W_{j-1}/W_j) \geq \dim(W_j/W_{j+1})$, or equivalently, $\lambda_j \geq \lambda_{j+1}$ for $1 \leq j \leq \ell - 1$. □

Hereon the sequence $W_i(T)(i \geq 0)$ will be referred to as the *chain of subspaces* associated with T.

Corollary 5.2.3. For $T \in \mathcal{L}(V)$, let $\ell = \ell(T)$. Then the sequence $\lambda_T = (\lambda_1(T), \ldots, \lambda_\ell(T))$ is an integer partition of $n - d_\ell(T)$.

We will prove that the pair $(\lambda_T, \mathcal{I}_T)$ completely determines the similarity class of a linear transformation T in the sense that two maps $T, \widetilde{T} \in \mathcal{L}(V)$ are similar if and only if $\lambda_T = \lambda_{\widetilde{T}}$ and $\mathcal{I}_T = \mathcal{I}_{\widetilde{T}}$. We require a lemma to prove this result. As the terminology in [20] differs considerably from that in this chapter, we include a proof here for the sake of completeness.

Lemma 5.2.4. [20, Ch. III, Lem. 3.3] Let $W, \widetilde{W}$ be subspaces of V. For $T \in L(W, V)$ and $\widetilde{T} \in L(\widetilde{W}, V)$, let T_U and $\widetilde{T}_{\widetilde{U}}$ denote the restrictions of T and $\widetilde{T}$ to the subspaces

$$U = \{v \in W : Tv \in W\} \text{ and } \widetilde{U} = \{v \in \widetilde{W} : \widetilde{T}v \in \widetilde{W}\}$$

respectively. Then T is similar to $\widetilde{T}$ if and only if T_U is similar to $\widetilde{T}_{\widetilde{U}}$ and $\dim W = \dim \widetilde{W}$.

Proof. First suppose that T is similar to $\widetilde{T}$. Then there exists a linear isomorphism $S : V \to V$ such that $SW = \widetilde{W}$ and $S \circ T = \widetilde{T} \circ S$. It follows that $\dim W = \dim \widetilde{W}$. We claim that T_U is similar to $\widetilde{T}_{\widetilde{U}}$ with respect to the same linear isomorphism S. To see this, we first show that S maps U onto $\widetilde{U}$. Suppose $v \in U$. Then, by definition, $v \in W$ and $Tv \in W$. This implies that $Sv \in \widetilde{W}$ and consequently $\widetilde{T} \circ Sv = S \circ Tv \in \widetilde{W}$ which further implies that $Sv \in \widetilde{U}$. Thus $SU \subseteq \widetilde{U}$. Now the isomorphism $S^{-1} : V \to V$ has the property that $S^{-1}\widetilde{W} = W$

and $S^{-1} \circ \widetilde{T} = T \circ S^{-1}$. By reasoning as above it follows that $S^{-1}\widetilde{U} \subseteq U$. It follows that $SU = \widetilde{U}$. Now since T_U and $\widetilde{T}_{\widetilde{U}}$ are restrictions of T and $\widetilde{T}$ to U and $\widetilde{U}$ respectively, it is easy to see that $S \circ T_U = \widetilde{T}_{\widetilde{U}} \circ S$ and it follows that T_U and $\widetilde{T}_{\widetilde{U}}$ are similar.

For the converse, suppose $\dim W = \dim \widetilde{W}$ and T_U is similar to $\widetilde{T}_{\widetilde{U}}$. This implies that there exists a linear isomorphism $S' : V \to V$ such that $S' \circ U = \widetilde{U}$ and $S' \circ T_U = \widetilde{T}_{\widetilde{U}} \circ S'$. First construct a linear isomorphism $S'' : V \to V$ such that $S''W = \widetilde{W}$ and $S'' \circ T_U = \widetilde{T}_{\widetilde{U}} \circ S''$. Note that $T(U) \subseteq W$. We simply set $S''v = S'v$ for all v lying in the subspace $U + TU$ of W. Since $S'(u_1 + Tu_2) = S'u_1 + S' \circ T_U u_2 = S'u_1 + \widetilde{T}_{\widetilde{U}} \circ S'u_2 \in \widetilde{U} + \widetilde{T}\widetilde{U}$, it is clear that $S'' : U+TU \to \widetilde{U}+\widetilde{T}\widetilde{U}$ is an isomorphism. Since $\dim W = \dim \widetilde{W}$, we may extend the definition of S'' to all of W to obtain a linear isomorphism $S'' : W \to \widetilde{W}$ which may be further extended to a linear isomorphism $S'' : V \to V$.

Now we use S'' to construct another linear isomorphism $S : V \to V$ such that $SW = \widetilde{W}$ and $S \circ T = \widetilde{T} \circ S$ which will imply that the linear transformations T and $\widetilde{T}$ are similar. Let $Sv = S''v$ for any $v \in W$ and let $Sv' = \widetilde{T} \circ S''v$ for any $v' = Tv \in TW$. We assert that $S : W + TW \to \widetilde{W} + \widetilde{T}\widetilde{W}$ is well defined and a linear isomorphism. If $v' = Tv$ lies in W, then $v \in U$ and hence $S''v' = S'' \circ Tv = S'' \circ T_U v = \widetilde{T}_{\widetilde{U}} \circ S''v = \widetilde{T} \circ S''v$. Therefore Sv' is uniquely defined. If $Tv = Tu$ for some $v, u \in W$, then $T(v-u) = 0$ lies in W. Thus, $S \circ T(v-u) = S'' \circ T(v-u) = 0$ which further implies $\widetilde{T} \circ S'v - \widetilde{T} \circ S'u = \widetilde{T} \circ S'(v-u) = 0$, and hence $S \circ Tv = S \circ Tu$. This implies that S is well defined. To prove that S is injective, let $v' = Tv$ for some $v \in W$ and $Sv' = 0$. This implies $Sv' = \widetilde{T} \circ S''v = 0$ which further implies $S'' \circ Tv = 0$ and since S'' is invertible, it follows $v' = 0$. It is easy to check that S is surjective and $S \circ T = \widetilde{T} \circ S$. Furthermore, it can be extended to a linear isomorphism $S : V \to V$. This completes the proof. □

Proposition 5.2.5. The linear transformations $T \in L(W, V)$ and $\widetilde{T} \in L(\widetilde{W}, V)$ are similar if and only if $\lambda_T = \lambda_{\widetilde{T}}$ and $\mathcal{I}_T = \mathcal{I}_{\widetilde{T}}$.

Proof. For $T \in L(W,V)$, consider the sequence of subspaces W_i such that $W_0 = V$, $W_1 = W$ and $W_{i+1} = \{v \in W_i : Tv \in W_i\}$. Let $\ell = \min\{i : W_i = W_{i+1}\}$ and denote by T_i the restriction of T to W_i for $1 \leq i \leq \ell$. Similarly, define $\widetilde{W}_i$, $\widetilde{T}_i$, $\widetilde{\ell}$ for $\widetilde{T} \in L(\widetilde{W},V)$. By Lemma 5.2.4, it follows that T_1 is similar to $\widetilde{T}_1$ if and only if T_2 is similar to $\widetilde{T}_2$ and $\dim W_1 = \dim \widetilde{W}_1$. Using the lemma again, it is clear that T_1 is similar to $\widetilde{T}_1$ if and only if T_3 is similar to $\widetilde{T}_3$, $\dim W_2 = \dim \widetilde{W}_2$ and $\dim W_1 = \dim \widetilde{W}_1$. By repeated application of the lemma, it is evident that T is similar to $\widetilde{T}$ if and only if T_ℓ is similar to $\widetilde{T}_{\widetilde{\ell}}$ with $\ell = \widetilde{\ell}$ and $\dim W_i = \dim \widetilde{W}_i$ for $1 \leq i \leq \ell$. The linear operators $T_\ell : W_\ell \to W_\ell$ and $\widetilde{T}_{\widetilde{\ell}} : \widetilde{W}_{\widetilde{\ell}} \to \widetilde{W}_{\widetilde{\ell}}$ are similar if and only if $\mathcal{I}_T = \mathcal{I}_{\widetilde{T}}$. Thus, it follows that T and $\widetilde{T}$ are similar if and only if $\lambda_T = \lambda_{\widetilde{T}}$ and $\mathcal{I}_T = \mathcal{I}_{\widetilde{T}}$. □

Definition 5.2.6. For any ordered set of invariant factors $\mathcal{I}$, define

$$\deg \mathcal{I} = \deg \prod_{p \in \mathcal{I}} p.$$

Remark 5.2.7. In view of the above proposition similarity classes in $\mathcal{L}(V)$ are indexed by pairs $(\lambda, \mathcal{I})$ where λ is an integer partition (possibly the empty partition) and $\mathcal{I} \subseteq \mathbb{F}_q[x]$ is an ordered set of invariant factors satisfying

$$|\lambda| + \deg \mathcal{I} = \dim V.$$

Denote the similarity class in $\mathcal{L}(V)$ corresponding to the pair $(\lambda, \mathcal{I})$ by $\mathcal{C}(\lambda, \mathcal{I})$. For a given subspace W of V and an integer partition λ with largest part $\dim V - \dim W$, denote by $\mathcal{C}_{W,V}(\lambda, \mathcal{I})$ the set of all linear transformations in $L(W,V)$ corresponding to the pair $(\lambda, \mathcal{I})$, i.e.,

$$\mathcal{C}_{W,V}(\lambda, \mathcal{I}) := L(W,V) \cap \mathcal{C}(\lambda, \mathcal{I}).$$

In the case $W = V$, the similarity class $\mathcal{C}_{V,V}(\lambda, \mathcal{I})$ is defined only when λ is the

empty partition and it depends only on the invariant factors $\mathcal{I}$. In this case $\mathcal{C}_{V,V}(\emptyset, \mathcal{I})$ is abbreviated to $\mathcal{C}(\mathcal{I})$. A closed formula for the size of $\mathcal{C}(\mathcal{I})$ (briefly stated in Theorem 2.2.1) can be found in Stanley [45, Eq. 1.107].

We present simple examples for better understanding of the similarity invariants.

Example 5.2.8. Let W be any subspace of V. Let $T \in L(W, V)$ be the identity transformation defined by $Tv = v$. By definition, $W_0 = V$ and $W_1 = W$. Clearly, W is the maximal T-invariant subspace. Thus the similarity invariants of T are given by the pair $(\lambda_T, \mathcal{I}_T)$ where $\lambda_T = (\dim V - \dim W)$ is the integer partition and $\mathcal{I}_T$ denotes the ordered set of invariant factors of the identity map T_W from W to W.

Example 5.2.9. Let V be the vector space with basis $\mathcal{B}_1 = \{v_1, v_2, \ldots, v_n\}$. For $k < n$, let W be the k-dimensional subspace spanned by the vectors $v_1, \ldots, v_k$. Consider $T \in L(W, V)$ defined by $Tv_i = v_{i+1}$ for $1 \leq i \leq k$. By definition, $W_0 = V$, $W_1 = W$ and

$$W_i = \text{ span}\{v_j : 1 \leq j \leq k - i + 1\}$$

for $1 \leq i \leq k + 1$. It is easy to see that the maximal T-invariant subspace is $W_{k+1} = \{0\}$. Thus the partition $\lambda_T = (n - k, 1, 1, \ldots, 1) \vdash n$ and $\mathcal{I}_T = \emptyset$.

Example 5.2.10. Let V be the vector space of dimension 6 with basis $\mathcal{B}_1 = \{v_1, \ldots, v_6\}$ and let W be the subspace of V spanned by the vectors $v_1, \ldots, v_4$. We define T from W into V by

$$v_1 \xrightarrow{T} v_1,$$

$$v_2 \xrightarrow{T} v_3 \xrightarrow{T} v_5,$$

$$v_4 \xrightarrow{T} v_6.$$

Clearly, $T \in L(W, V)$. We then have a descending chain of subspaces $W_i(T)(i \geq 0)$ given by

$$V \supset W \supset \text{span}\{v_1, v_2\} \supset \text{span}\{v_1\}.$$

In this case, $\lambda_T = (2, 2, 1)$ and $\mathcal{I}_T$ is the ordered set of invariant factors of the restriction T_{W_3} of T to $W_3 = \text{span}\{v_1\}$. Smith normal form of $xI - T_{W_3}$ is the 1×1 matrix whose entry is $x - 1$ which implies $\mathcal{I}_T = \{x - 1\}$.

5.3 Counting simple linear transformations

Let us briefly recall the definition of simple linear transformation from Chapter 2.

Definition 5.3.1. A linear transformation $T \in \mathcal{L}(V)$ is *simple* if, for each T-invariant subspace U, either $U = \{0\}$ or $U = V$.

It follows from the definition that simple maps are injective. If $T \in \mathcal{L}(V)$ is simple with domain a proper subspace of V, then the maximal T-invariant subspace is necessarily the zero subspace and therefore $T \in \mathcal{C}(\lambda, \emptyset)$ for some integer partition λ of $\dim V$ with largest part $\dim V - \dim W$ where W is the domain of T. In this section we determine the size of $\mathcal{C}(\lambda, \emptyset)$ for an arbitrary partition λ of $\dim V$. We begin with some combinatorial lemmas.

The number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is given by the q-binomial coefficient [49, p. 292]

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \prod_{i=1}^{k} \frac{q^{n-i+1} - 1}{q^i - 1}.$$

Lemma 5.3.2. Let $U \subseteq W$ be subspaces of an n-dimensional vector space V over $\mathbb{F}_q$ with $\dim U = d$ and $\dim W = k$. The number of k-dimensional subspaces

of V whose intersection with W is U equals

$$\begin{bmatrix} n-k \\ k-d \end{bmatrix}_q q^{(k-d)^2}.$$

Proof. We count the number of k-dimensional subspaces W' for which $W \cap W' = U$. Given any ordered basis of U, there are $\prod_{i=k}^{2k-d-1}(q^n - q^i)$ ways to extend it to an ordered basis of W'. Counting in this manner, the same subspace W' arises in precisely $\prod_{i=d}^{i=k-1}(q^k - q^i)$ ways. Thus the total number of such subspaces W' is given by

$$\frac{\prod_{i=k}^{2k-d-1}(q^n - q^i)}{\prod_{i=d}^{i=k-1}(q^k - q^i)} = \begin{bmatrix} n-k \\ k-d \end{bmatrix}_q q^{(k-d)^2}.$$

□

Definition 5.3.3. [14, p. 95] A *flag* of length r in a vector space V is an increasing sequence of subspaces $W_i (0 \leq i \leq r)$ such that

$$\{0\} = W_0 \subset W_1 \subset \cdots W_{r-1} \subset W_r = V.$$

The following lemma gives the number of flags of length r with subspaces of given dimensions.

Lemma 5.3.4. [35, Sec. 1.5] Let $n_1, \ldots, n_r$ be positive integers with $n_1 + \cdots + n_r = n$. The number of flags $W_0 \subset \cdots \subset W_r$ of length r in an n-dimensional vector space V over $\mathbb{F}_q$ with $\dim W_i = n_1 + n_2 + \cdots + n_i$ is given by the q-multinomial coefficient

$$\begin{bmatrix} n \\ n_1, n_2, \ldots, n_r \end{bmatrix}_q := \frac{[n]_q!}{[n_1]_q![n_2]_q! \ldots [n_r]_q!},$$

where $[n]_q := \frac{q^n - 1}{q-1}$ and $[n]_q! := [n]_q[n-1]_q \ldots [1]_q$.

In the statement of the following theorem and the rest of this chapter, the number of nonsingular $k \times k$ matrices over $\mathbb{F}_q$ [35, Sec. 1.2] is denoted by $\gamma_q(k) =$

$\prod_{i=0}^{k-1}(q^k - q^i)$.

Theorem 5.3.5. Let λ be a partition of n. Then

$$|\mathcal{C}(\lambda, \emptyset)| = q^{\sum_{j\geq 2}\lambda_j^2} \begin{bmatrix} n \\ n-\lambda_1, \lambda_1 - \lambda_2, \ldots, \lambda_\ell \end{bmatrix}_q \gamma_q(n-\lambda_1).$$

Proof. We count the number of simple linear transformations $T \in \mathcal{L}(V)$ having defect dimensions $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ defined on some subspace of V of dimension $n - \lambda_1$. Fix a subspace W of V of dimension $n - \lambda_1$. We first determine the cardinality of $\mathcal{C}_{W,V}(\lambda, \emptyset)$. For $T \in \mathcal{C}_{W,V}(\lambda, \emptyset)$ consider the chain of subspaces $\{W_i = W_i(T)\}_{i=0}^{\ell}$ associated with T. Define a sequence $\{W_i'\}_{i=1}^{\ell}$ by $W_i' = T(W_i)$. Since T is injective, we have $\dim W_i = \dim W_i' = d_i$ for $i \geq 1$. By the choice of T we have $d_{i-1} - d_i = \lambda_i$. Note that $W_i \cap W_i' = W_{i+1}'$ for $1 \leq i \leq \ell - 1$. The sequence $\{W_i\}_{i=0}^{\ell}$ is a flag in W of length $\ell - 1$:

$$\{0\} = W_\ell \subset \cdots W_2 \subset W_1 = W$$

such that $\dim W_i = d_i = \lambda_\ell + \lambda_{\ell-1} + \cdots \lambda_{i+1}$. By Lemma 5.3.4, the number of such flags is

$$\begin{bmatrix} n-\lambda_1 \\ \lambda_\ell, \lambda_{\ell-1}, \ldots, \lambda_2 \end{bmatrix}_q.$$

For a given choice of $\{W_i\}_{i=0}^{\ell}$, the total number of choices for the sequence $\{W_i'\}_{i=0}^{\ell}$ equals the total number of flags

$$\{0\} = W_\ell' \subset \cdots W_2' \subset W_1' = TW$$

of length $\ell - 1$ where $\dim W_i' = d_i$ and $W_i \cap W_i' = W_{i+1}'$ for $1 \leq i \leq \ell - 1$. Thus $W_{\ell-1}'$ is a subspace of $W_{\ell-2}$ of dimension $d_{\ell-1}$ that intersects $W_{\ell-1}$ trivially. It follows by Lemma 5.3.2 that $W_{\ell-1}'$ can be chosen in

$$\begin{bmatrix} d_{\ell-2} - d_{\ell-1} \\ d_{\ell-1} - d_\ell \end{bmatrix}_q q^{(d_{\ell-1}-d_\ell)^2} = \begin{bmatrix} \lambda_{\ell-1} \\ \lambda_\ell \end{bmatrix}_q q^{\lambda_\ell^2}$$

ways. Similarly, the conditions $W'_{\ell-2} \subseteq W_{\ell-3}$ and $W_{\ell-2} \cap W'_{\ell-2} = W'_{\ell-1}$ imply that $W'_{\ell-2}$ can be chosen in

$$\begin{bmatrix} d_{\ell-3} - d_{\ell-2} \\ d_{\ell-2} - d_{\ell-1} \end{bmatrix}_q q^{(d_{\ell-2}-d_{\ell-1})^2} = \begin{bmatrix} \lambda_{\ell-2} \\ \lambda_{\ell-1} \end{bmatrix}_q q^{\lambda_{\ell-1}^2}$$

ways. Proceeding in this manner, it is seen that the total number of choices for the sequence $\{W'_i\}_{i=1}^{\ell}$ is equal to

$$\begin{bmatrix} \lambda_{\ell-1} \\ \lambda_\ell \end{bmatrix}_q q^{\lambda_\ell^2} \begin{bmatrix} \lambda_{\ell-2} \\ \lambda_{\ell-1} \end{bmatrix}_q q^{\lambda_{\ell-1}^2} \cdots \begin{bmatrix} \lambda_1 \\ \lambda_2 \end{bmatrix}_q q^{\lambda_2^2} = q^{\sum_{i=2}^{\ell} \lambda_i^2} \begin{bmatrix} \lambda_1 \\ \lambda_1 - \lambda_2, \lambda_2 - \lambda_3, \ldots, \lambda_\ell \end{bmatrix}_q.$$

For each choice of the flags $\{W_i\}_{i=0}^{\ell}$ and $\{W'_i\}_{i=0}^{\ell}$, we count the number of possibilities for T. Note that T is injective and $TW_i = W'_i$ for $1 \leq i \leq \ell$. Thus the number of ways to map $W_{\ell-1}$ onto $W'_{\ell-1}$ is equal to the number of invertible $\lambda_\ell \times \lambda_\ell$ matrices over $\mathbb{F}_q$, i.e., $\gamma_q(\lambda_\ell)$. The number of ways to extend T to $W_{\ell-2}$ such that $TW_{\ell-2} = W'_{\ell-2}$ is evidently

$$\prod_{i=d_{\ell-1}}^{d_{\ell-1}+\lambda_{\ell-1}-1} (q^{d_{\ell-2}} - q^i) = q^{d_{\ell-1}\lambda_{\ell-1}} \gamma_q(\lambda_{\ell-1}).$$

Following this line of reasoning, the total number of choices for the map T for a given choice of $\{W_i\}_{i=0}^{\ell}$ and $\{W'_i\}_{i=0}^{\ell}$ equals

$$q^{\sum_{i=2}^{\ell} d_i \lambda_i} \prod_{i=2}^{\ell} \gamma_q(\lambda_i).$$

It follows that

$$|\mathcal{C}_{W,V}(\lambda, \emptyset)| = \begin{bmatrix} n - \lambda_1 \\ \lambda_\ell, \lambda_{\ell-1}, \ldots, \lambda_2 \end{bmatrix}_q q^{\sum_{i=2}^{\ell} \lambda_i^2} \begin{bmatrix} \lambda_1 \\ \lambda_1 - \lambda_2, \lambda_2 - \lambda_3, \ldots, \lambda_\ell \end{bmatrix}_q q^{\sum_{i=2}^{\ell} d_i \lambda_i} \times \prod_{i=2}^{\ell} \gamma_q(\lambda_i).$$

We expand the values of $\gamma_q(\lambda_i)$ and simplify the above expression.

$$\begin{aligned}
|\mathcal{C}_{W,V}(\lambda,\emptyset)| &= q^{\sum_{i=2}^{\ell}\lambda_i^2}\begin{bmatrix}\lambda_1\\ \lambda_1-\lambda_2,\lambda_2-\lambda_3,\ldots,\lambda_\ell\end{bmatrix}_q \frac{[n-\lambda_1]_q!}{[\lambda_\ell]_q![\lambda_{\ell-1}]_q!\cdots[\lambda_2]_q!}q^{\sum_{i=2}^{\ell}d_i\lambda_i}\\
&\quad\times\prod_{i=2}^{\ell}(q-1)^{\lambda_i}q^{\binom{\lambda_i}{2}}[\lambda_i]_q!\\
&= q^{\sum_{i=2}^{\ell}\lambda_i^2}\begin{bmatrix}\lambda_1\\ \lambda_1-\lambda_2,\lambda_2-\lambda_3,\ldots,\lambda_\ell\end{bmatrix}_q [n-\lambda_1]_q!q^{\sum_{i=2}^{\ell}d_i\lambda_i}(q-1)^{\lambda_2+\cdots+\lambda_\ell}\\
&\quad\times q^{\binom{\lambda_2}{2}+\cdots+\binom{\lambda_\ell}{2}}\\
&= q^{\sum_{i=2}^{\ell}\lambda_i^2}\begin{bmatrix}\lambda_1\\ \lambda_1-\lambda_2,\lambda_2-\lambda_3,\ldots,\lambda_\ell\end{bmatrix}_q [n-\lambda_1]_q!(q-1)^{n-\lambda_1}q^{\binom{n-\lambda_1}{2}}\\
&= q^{\sum_{i=2}^{\ell}\lambda_i^2}\begin{bmatrix}\lambda_1\\ \lambda_1-\lambda_2,\lambda_2-\lambda_3,\ldots,\lambda_\ell\end{bmatrix}_q \gamma_q(n-\lambda_1). \qquad (5.1)
\end{aligned}$$

Since the domain of T is an arbitrary $n-\lambda_1$ dimensional subspace of V, we sum over all $(n-\lambda_1)$ dimensional subspaces of V to obtain

$$|\mathcal{C}(\lambda,\emptyset)| = \sum_{W:\dim W=n-\lambda_1}|\mathcal{C}_{W,V}(\lambda,\emptyset)| = \begin{bmatrix}n\\ n-\lambda_1\end{bmatrix}_q |\mathcal{C}_{W,V}(\lambda,\emptyset)|\,.$$

Substituting the expression for $|\mathcal{C}_{W,V}(\lambda,\emptyset)|$ obtained earlier, we obtain

$$\begin{aligned}
|\mathcal{C}(\lambda,\emptyset)| &= \begin{bmatrix}n\\ n-\lambda_1\end{bmatrix}_q q^{\sum_{i=2}^{\ell}\lambda_i^2}\begin{bmatrix}\lambda_1\\ \lambda_1-\lambda_2,\lambda_2-\lambda_3,\ldots,\lambda_\ell\end{bmatrix}_q \gamma_q(n-\lambda_1)\\
&= q^{\sum_{i=2}^{\ell}\lambda_i^2}\begin{bmatrix}n\\ n-\lambda_1,\lambda_1-\lambda_2,\ldots,\lambda_\ell\end{bmatrix}_q \gamma_q(n-\lambda_1). \qquad \square
\end{aligned}$$

Corollary 5.3.6. Let W be a proper subspace of an n-dimensional vector space V over $\mathbb{F}_q$. Let $\lambda \vdash n$ with $\lambda_1 = \dim V - \dim W$. Then the number of simple linear transformations defined on W with defect dimensions λ is given by

$$\sigma(\lambda) := |\mathcal{C}_{W,V}(\lambda,\emptyset)| = q^{\sum_{i\geq 2}\lambda_i^2}\gamma_q(n-\lambda_1)\prod_{i\geq 1}\begin{bmatrix}\lambda_i\\ \lambda_{i+1}\end{bmatrix}_q.$$

Proof. Follows from Equation (5.1) in the proof of the above theorem. $\square$

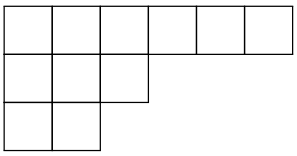

FIGURE 5.1: The Young diagram of $(6, 3, 2)$.

The above corollary may be used to deduce the number of simple linear transformations with a fixed domain by summing $\sigma(\lambda)$ over partitions with a fixed first part. We first collate some basic results on partitions. A useful graphic representation of an integer partition is the corresponding Young diagram. Given a partition $\lambda = (\lambda_1, \lambda_2, \ldots)$, put λ_i (unit) cells in row i to obtain its Young diagram. For instance, the Young diagram of the partition $(6, 3, 2)$ is shown in Figure 5.1.

Definition 5.3.7. For integers m, r, s denote by $p(m, r, s)$ the number of partitions of m with at most r parts in which each part is at most s.

The geometric interpretation of $p(m, r, s)$ is that it counts the number of partitions of m whose Young diagrams fit in a rectangle of size $r \times s$. The following lemma shows that the generating function for $p(m, r, s)$ for fixed values of r and s is a q-binomial coefficient.

Lemma 5.3.8. [3, Prop. 1.1] We have

$$\begin{bmatrix} r+s \\ s \end{bmatrix}_q = \sum_{i \geq 0} p(i, r, s) q^i.$$

The *rank* [45, p. 71] of a partition λ is the largest integer i for which $\lambda_i \geq i$. Geometrically, the rank of a partition corresponds to the side length of the largest square, called the *Durfee square*, contained in the Young diagram of λ. The Durfee square of the partition $\lambda = (6, 4, 3, 2)$ is indicated by the shaded cells in Figure 5.2.

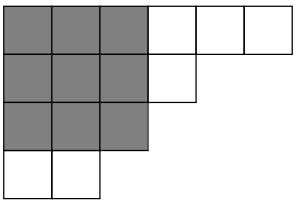

Figure 5.2: The Durfee square of the partition $(6, 4, 3, 2)$.

Proposition 5.3.9. For positive integers $m \leq n$, we have

$$\sum_{\substack{\lambda \vdash n \\ \lambda_1 = m}} q^{\sum \lambda_i^2} \prod_{i \geq 1} \begin{bmatrix} \lambda_i \\ \lambda_{i+1} \end{bmatrix}_q = q^{m^2+n-m} \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q.$$

Proof. Let S denote the set of all partitions μ of rank m and largest part n with precisely m parts. Visually S consists of partitions whose Young diagrams fit inside an $m \times n$ rectangle R and have at least m cells in each row with precisely n cells in the first row. We compute the sum

$$\sum_{\mu \in S} q^{|\mu|}$$

in two different ways. Note that each $\mu \in S$ is uniquely determined by the partition $\mu' = (\mu_2 - m, \mu_3 - m, \ldots)$ since the first row and first m columns of the Young diagram of μ are fixed. As the diagram of μ' fits in the $(m-1) \times (n-m)$ rectangle at the bottom right corner of R, it follows by Lemma 5.3.8 that

$$\begin{aligned} \sum_{\mu \in S} q^{|\mu|} &= q^{m^2+n-m} \sum_{\mu \in S} q^{|\mu'|} \\ &= q^{m^2+n-m} \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q, \end{aligned}$$

which accounts for the expression on the right hand side of the proposition. Now for any $\mu \in S$ consider the partition $\varphi(\mu) = \lambda \vdash n$ defined as follows: λ_1 is the rank of μ, λ_2 is the rank of the partition whose diagram is to the right of the Durfee square of μ, etc. For example, when $\mu = (8, 7, 6, 5)$, we have $\varphi(\mu) = (4, 2, 1, 1)$

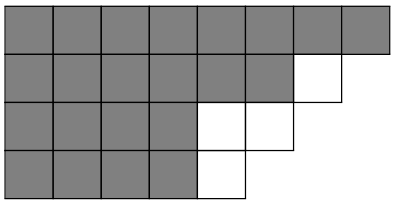

FIGURE 5.3: The partition $\varphi(\mu) = (4, 2, 1, 1)$ corresponding to $\mu = (8, 7, 6, 5)$.

as shown in Figure 5.3. As μ varies over S, the partition $\varphi(\mu)$ varies over all partitions of n with largest part m. Therefore

$$\sum_{\mu \in S} q^{|\mu|} = \sum_{\substack{\lambda \vdash n \\ \lambda_1 = m}} \sum_{\substack{\mu \in S \\ \varphi(\mu) = \lambda}} q^{|\mu|}.$$

Consider the inner sum on the right hand side. If $\varphi(\mu) = \lambda$, then λ defines a sequence of squares (corresponding to the shaded cells in Figure 5.3) which accounts for $\sum_i \lambda_i^2$ cells in the diagram of μ. The cells of μ that do not lie in any square in the sequence (the unshaded cells in the running example of Figure 5.3) correspond to a sequence of partitions: the first is a partition that fits in a rectangle of size $(\lambda_1 - \lambda_2) \times \lambda_2$, the second is a partition that fits in a rectangle of size $(\lambda_2 - \lambda_3) \times \lambda_3$ etc. Putting these observations together and applying Lemma 5.3.8, it is clear that

$$\sum_{\substack{\mu \in S \\ \varphi(\mu) = \lambda}} q^{|\mu|} = q^{\sum \lambda_i^2} \begin{bmatrix} \lambda_1 \\ \lambda_2 \end{bmatrix}_q \begin{bmatrix} \lambda_2 \\ \lambda_3 \end{bmatrix}_q \cdots$$

and the proposition follows. □

We now deduce the theorem of Lieb, Jordan and Helmke alluded to in the introduction.

Corollary 5.3.10. [33, Thm. 1] Let W be a proper k-dimensional subspace of a vector space V of dimension n over $\mathbb{F}_q$. The number of simple linear transformations with domain W equals $\prod_{i=1}^{k} (q^n - q^i)$.

Proof. The number of simple linear transformations with domain W is equal to

$$\sum_{\substack{\lambda\vdash n\\ \lambda_1=n-k}} \sigma(\lambda) = \gamma_q(k) \sum_{\substack{\lambda\vdash n\\ \lambda_1=n-k}} q^{\sum_{i\geq 2}\lambda_i^2} \prod_{i\geq 1} \begin{bmatrix} \lambda_i \\ \lambda_{i+1} \end{bmatrix}_q$$

by Corollary 5.3.6. Setting $m = n-k$ in Proposition 5.3.9 the sum on the right hand side above becomes

$$\begin{aligned} q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \gamma_q(k) &= q^k \frac{(q^{n-1}-1)\cdots(q^{n-1}-q^{k-1})}{(q^k-1)\cdots(q^k-q^{k-1})} \prod_{i=0}^{k-1}(q^k-q^i) \\ &= \prod_{i=1}^{k}(q^n-q^i). \end{aligned}$$

□

The corollary above can also be obtained [5, Cor. 2.12] by counting certain unimodular matrices over a finite field.

5.4 Arbitrary linear transformations defined on a subspace

In this section we extend the results obtained on the conjugacy class size of simple linear transformations to arbitrary maps in $\mathcal{L}(V)$. Let $T \in \mathcal{L}(V)$ be a fixed but arbitrary linear transformation with domain W and let U denote the maximal invariant subspace of T. Define a map $\hat{T}$ from the quotient space W/U into V/U by

$$\hat{T}(v+U) = Tv + U.$$

Then $\hat{T}$ is well defined. If $v_1+U = v_2+U$ for some $v_1, v_2 \in W$ then $v_1 - v_2 \in U$ and consequently $T(v_1-v_2) \in U$ since U is T-invariant. It follows that $Tv_1+U = Tv_2+U$ and thus $\hat{T}$ is well defined. The linearity of $\hat{T}$ is an easy consequence of the fact that T is linear.

Lemma 5.4.1. Let $\mathcal{W} = \{v \in W : Tv \in W\}$ and $\hat{\mathcal{W}} = \{\alpha \in W/U : \hat{T}(\alpha) \in W/U\}$. Then $\hat{\mathcal{W}} = \mathcal{W}/U$.

Proof. Note that $U \subseteq \mathcal{W}$. We have

$$\begin{aligned} v + U \in \hat{\mathcal{W}} &\iff v + U \in W/U \text{ and } Tv + U \in W/U \\ &\iff v \in W \text{ and } Tv \in W \\ &\iff v \in \mathcal{W}. \end{aligned}$$

□

Lemma 5.4.2. Let W be a proper subspace of an n-dimensional vector space V over $\mathbb{F}_q$ and let $T \in L(W, V)$. Let U denote the maximal T-invariant subspace and suppose $\dim U = d$. Suppose $T \in \mathcal{C}(\lambda, \mathcal{I})$ for some integer partition $\lambda \vdash n-d$. Then the linear transformation $\hat{T} : W/U \to V/U$ defined by $\hat{T}(v + U) = Tv + U$ is simple and $\hat{T} \in \mathcal{C}(\lambda, \emptyset)$.

Proof. To show that $\hat{T}$ is simple, it suffices to show that the maximal invariant subspace of $\hat{T}$ is the zero subspace. Let $\{W_i\}_{i=0}^{\ell}$ be the chain of subspaces associated with T with $W_\ell = U$. Similarly, there is a chain of subspaces $\{\hat{W}_i\}_{i=0}^{\ell'}$ associated with $\hat{T}$. It follows by Lemma 5.4.1 that $\hat{W}_2 = W_2/U$. By applying the lemma again to the restriction of $\hat{T}$ to W_2/U, we obtain $\hat{W}_3 = W_3/U$. By repeated application of the lemma it is clear that $\hat{W}_i = W_i/U$ for $0 \leq i \leq \ell$. This implies that $\ell' = \ell$ and that the maximal invariant subspace $\hat{W}_\ell$ of $\hat{T}$ is the zero subspace. Thus $\hat{T}$ is simple. Since

$$\dim W_{j-1}/U - \dim W_j/U = \dim W_{j-1} - \dim W_j = \lambda_j$$

for $1 \leq j \leq \ell$, the sequence of defect dimensions of $\hat{T}$ is λ. □

Definition 5.4.3. For $T \in \mathcal{L}(V)$, the map $\hat{T}$ defined above is called the *simple part* of T.

Definition 5.4.4. For $T \in \mathcal{L}(V)$, the *operator part* of T denotes the linear operator obtained by restricting T to its maximal invariant subspace.

Given a subspace W of V and any $T \in L(W, V)$, associate with it a pair $(\overline{T}, \hat{T})$ where $\overline{T}$ denotes the operator part of T and $\hat{T}$ denotes the simple part of T. The following proposition asserts that the number of linear transformations having prescribed simple and operator parts is a power of q.

Proposition 5.4.5. Let $U \subseteq W$ be subspaces of an n-dimensional vector space V over $\mathbb{F}_q$ and suppose that the dimensions of U and W are d and k respectively. Let T_o be a linear operator on U with ordered set of invariant factors $\mathcal{I}$ and let $T_s \in L(W/U, V/U)$ be a simple linear transformation with defect dimensions $\lambda \vdash n-d$. The number of linear transformations $T \in L(W, V)$ with operator part T_o and simple part T_s is given by $q^{d(k-d)}$.

Proof. Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_d\}$ be an ordered basis for U. Extend $\mathcal{B}$ to a basis $\mathcal{B}' = \{\alpha_1, \ldots, \alpha_k\}$ for W. Let T_o and T_s be as in the statement of the theorem. If a linear transformation $T \in L(W, V)$ has operator part T_o, then T is uniquely defined at each element of $\mathcal{B}$. It remains to define T on each α_i for $d+1 \leq i \leq k$. Suppose that $T_s(\alpha_i + U) = \beta_i + U$ for some $\beta_i \in V$ and $d+1 \leq i \leq k$. Then $T\alpha_i + U = \beta_i + U$ for $d+1 \leq i \leq k$. It therefore suffices to count maps T satisfying

$$T\alpha_i = \beta_i + \gamma_i \text{ for some } \gamma_i \in U \quad (d+1 \leq i \leq k).$$

The number of such maps is clearly $q^{d(k-d)}$. □

The function $\sigma(\lambda)$ defined in Corollary 5.3.6 counts the number of simple maps with defect dimensions λ when λ is a partition of a positive integer. As the simple part of any linear operator on V is trivial, it is natural to extend the domain of definition of $\sigma(\lambda)$ to the empty partition by declaring $\sigma(\emptyset) = 1$.

Theorem 5.4.6. Let $U \subseteq W$ be subspaces of an n-dimensional vector space V over $\mathbb{F}_q$ and suppose $\dim U = d$ and $\dim W = k$. Let $\lambda \vdash n - d$ with $\lambda_1 = n - k$

and $\mathcal{I}$ be an ordered set of invariant factors of degree d. The number of maps in $\mathcal{C}_{W,V}(\lambda, \mathcal{I})$ with maximal invariant subspace U equals

$$q^{d(k-d)} \left|\mathcal{C}(\mathcal{I})\right| \sigma(\lambda). \tag{5.2}$$

Proof. There are precisely $|\mathcal{C}(\mathcal{I})|$ possibilities for the operator part of T. Setting $W' = W/U$ and $V' = V/U$, the simple part of T can be chosen in $|\mathcal{C}_{W',V'}(\lambda, \emptyset)| = \sigma(\lambda)$ ways. The result now follows from Proposition 5.4.5. □

Corollary 5.4.7. Let W be a k-dimensional subspace of an n-dimensional vector space V over $\mathbb{F}_q$. Let $\mathcal{I}$ be an ordered set of invariant factors with $\deg \mathcal{I} = d \leq \dim W$ and let $\lambda \vdash n - d$ with $\lambda_1 = n - k$. Then

$$|\mathcal{C}_{W,V}(\lambda, \mathcal{I})| = q^{d(k-d)} \begin{bmatrix} k \\ d \end{bmatrix}_q |\mathcal{C}(\mathcal{I})| \, \sigma(\lambda). \tag{5.3}$$

Proof. The corollary follows from Theorem 5.4.6 as there are $\begin{bmatrix} k \\ d \end{bmatrix}_q$ possibilities for the maximal invariant subspace. □

In the case $W = V$, the above expression for $|\mathcal{C}_{W,V}(\lambda, \mathcal{I})|$ reduces to $|\mathcal{C}(\mathcal{I})|$, the number of square matrices whose invariant factors are given by $\mathcal{I}$. The next corollary determines the size of the similarity classes in $\mathcal{L}(V)$.

Corollary 5.4.8. Let V be a vector space over $\mathbb{F}_q$ of dimension n. If $\deg \mathcal{I} = d$ and $\lambda \vdash n - d$, then

$$|\mathcal{C}(\lambda, \mathcal{I})| = q^{d(k-d)} \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} k \\ d \end{bmatrix}_q |\mathcal{C}(\mathcal{I})| \, \sigma(\lambda),$$

where $k = n - \lambda_1$.

Proof. Any map in $\mathcal{C}(\lambda, \mathcal{I})$ has domain of dimension k. The result follows from Corollary 5.4.7 by summing $|\mathcal{C}_{W,V}(\lambda, \mathcal{I})|$ over all k-dimensional subspaces of V. □

Corollary 5.4.9. [43, Thm. 3.8] Let W be a fixed k-dimensional subspace of an n-dimensional vector space V over $\mathbb{F}_q$. The number of linear transformations $T \in L(W, V)$ for which the operator part of T has invariant factors $\mathcal{I}$ with $\deg \mathcal{I} = d$ equals

$$\begin{bmatrix} k \\ d \end{bmatrix}_q |\mathcal{C}(\mathcal{I})| \prod_{i=d+1}^{k} (q^n - q^i).$$

Proof. By Corollary 5.4.7 the desired number of linear transformations equals

$$\begin{aligned} \sum_{\substack{\lambda \vdash n-d \\ \lambda_1 = n-k}} |\mathcal{C}_{W,V}(\lambda, \mathcal{I})| &= q^{d(k-d)} \begin{bmatrix} k \\ d \end{bmatrix}_q |\mathcal{C}(\mathcal{I})| \sum_{\substack{\lambda \vdash n-d \\ \lambda_1 = n-k}} \sigma(\lambda) \\ &= q^{d(k-d)} \begin{bmatrix} k \\ d \end{bmatrix}_q |\mathcal{C}(\mathcal{I})| \prod_{j=1}^{k-d} (q^{n-d} - q^j) \\ &= \begin{bmatrix} k \\ d \end{bmatrix}_q |\mathcal{C}(\mathcal{I})| \prod_{i=d+1}^{k} (q^n - q^i). \end{aligned}$$

The second equality above is a consequence of Corollary 5.3.10. □

Chapter 6

Future Outlook

This chapter presents brief conclusions and the future scope of this work. We discuss some of the interesting open problems in this research direction.

6.1 Splitting subspaces of linear operator over finite fields

Let d, m be positive integers. Ghorpade and Ram [19, p. 54] provided a more general version of Niederreiter's question on the number of α-splitting subspace by considering transforms of an m-dimensional subspace of $\mathbb{F}_{q^{md}}$ by an endomorphism of $\mathbb{F}_{q^{md}}$ instead of considering its multiples by powers of α. More precisely, given any $\mathbb{F}_q$-linear endomorphism $T : \mathbb{F}_{q^{md}} \to \mathbb{F}_{q^{md}}$, we say that an m-dimensional subspace W of $\mathbb{F}_{q^{md}}$ is T-*splitting* if

$$\mathbb{F}_{q^{md}} = W \oplus TW \oplus \cdots \oplus T^{d-1}W,$$

where T_i denotes the i-fold composite of T with itself $(0 \leq i < d)$. For any element $\alpha \in \mathbb{F}_{q^{md}}$, if $T : \mathbb{F}_{q^{md}} \to \mathbb{F}_{q^{md}}$ is the $\mathbb{F}_q$-linear endomorphism mapping $v \to \alpha v$, then clearly an m-dimensional subspace W of $\mathbb{F}_{q^{md}}$ is T-splitting if and only if

it is α-splitting. The following question is the generalization of Niederreiter's question.

Question 6.1.1. Determine the number of m-dimensional T-splitting subspaces of $\mathbb{F}_{q^{md}}$ for every $\mathbb{F}_q$-linear endomorphism T of $\mathbb{F}_{q^{md}}$.

The solution to this problem is challenging for an arbitrary T; however, there has been some recent remarkable progress by putting certain restrictions on T. Apart from the case where T has an irreducible characteristic polynomial (see Splitting Subspace Theorem in Section 4.2), the solution is also known for the cases where T is cyclic nilpotent [2], is regular split semisimple [38, 37], the invariant factors of T satisfy certain degree constraints [1], or when $d = 2$ [39]. The general case still remains open and would be an interesting topic to study.

6.2 Similarity invariants of extensions

Let V be an n-dimensional vector space over $\mathbb{F}_q$ and let W, W' be fixed subspaces of V of dimension k and $k+1$ respectively with $W \subset W'$. For a given simple linear transformation $T \in L(W, V)$, we determined the number of simple linear transformations $T' \in L(W', V)$ such that $T'_{|W} = T$ (see Lem. 3.2.9) in Chapter 3. In Chapter 5, we proved that the similarity invariants for an arbitrary transformation $T \in L(W, V)$ are characterized by the pair $(\lambda_T, \mathcal{I}_T)$ where $\lambda \vdash n$ denotes the defect dimensions of T and $\mathcal{I} \subseteq \mathbb{F}_q[x]$ is an ordered set of invariant factors of the restriction of T to its maximal T-invariant subspace U satisfying

$$|\lambda| + \deg \mathcal{I} = \dim V.$$

We further determined the size of the similarity class $\mathcal{C}(T)$ of T. Furthermore, we showed that if T is simple, then the similarity class $\mathcal{C}(T)$ of T is characterized by the pair $(\lambda_T, \emptyset)$ and is completely determined by defect dimensions λ_T of T.

Given a simple linear transformation $T \in L(W, V)$ with defect dimensions λ_T, it would be an interesting problem to determine the similarity invariants for an arbitrary simple linear transformation $T' \in L(W', V)$ such that $T'_{|W} = T$. We propose the following conjecture on the defect dimensions of T'.

Conjecture 6.2.1. Let V be an n-dimensional vector space over $\mathbb{F}_q$ and let W, W' be fixed subspaces of V of dimension k and $k+1$ respectively with $W \subset W'$. Suppose $T \in L(W, V)$, $T' \in L(W', V)$ are simple linear transformations with $T'_{|W} = T$ and defect dimensions $\lambda_T = (\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_\ell) \vdash n$, $\lambda_{T'} = (\lambda'_1, \lambda'_2, \lambda'_3, \ldots, \lambda'_{\ell'}) \vdash n$ respectively. Then we can obtain $\lambda_{T'}$ starting from the Young diagram of λ_T in the following manner.

(i.) For some positive integer r, we remove a single cell in each of the first r rows.

(ii.) We successively add r corner cells, i.e., the cells having cells to its left and above in the Young diagram in such a way that none of the new cells are in the same row or column as a previously deleted cell.

Conversely, let $T \in L(W, V)$ be a simple linear transformation with defect dimensions $\lambda_T = (\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_\ell) \vdash n$. Suppose $\mu = (\mu_1, \mu_2, \mu_3, \ldots, \mu_{\ell'})$ is the partition of n obtained from the Young diagram of λ_T by applying steps (i.) and (ii.). Then there exists a simple transformation T'' defined on some subspace W'' of V of dimension $k+1$ containing W with $T''_{|W} = T$ and defect dimensions μ.

Let us consider an example for ease of understanding.

Example 6.2.2. Let W, W' be any subspaces of dimension 5 and dimension 6 of a vector space V of dimension 9 with $W \subset W'$. Suppose $T \in L(W, V)$ is a fixed simple linear transformation with defect dimensions $\lambda_T = (4, 3, 1, 1)$. Let $T' \in L(W', V)$ be any simple map with $T'_{|W} = T$ and defect dimensions $\lambda_{T'}$. We will apply the steps from the above conjecture to obtain all possible partitions

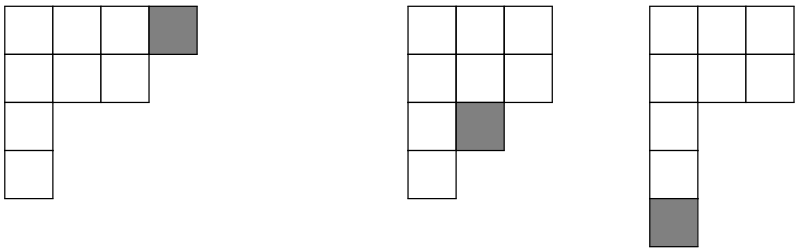

FIGURE 6.1: The Young diagrams of $(4,3,1,1)$, $(3,3,2,1)$ and $(3,3,1,1,1)$.

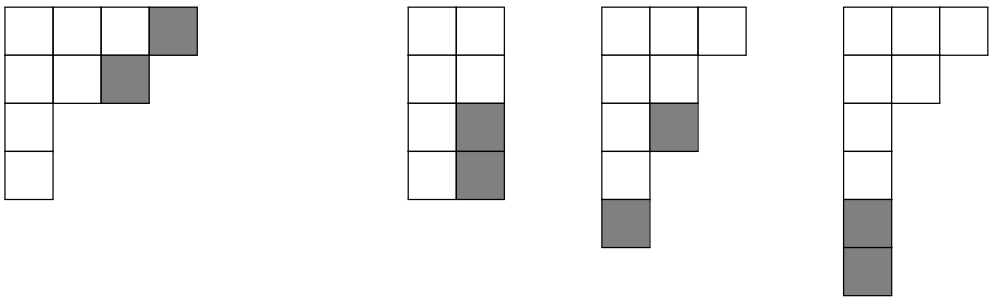

FIGURE 6.2: The Young diagrams of $(4,3,1,1)$, $(3,2,2,2)$, $(3,2,2,1,1)$ and $(3,2,1,1,1,1)$.

for $\lambda_{T'}$. Consider the Young diagram of the partition λ_T (see Figure 6.1). For $r = 1$, we remove the shaded cell from the first row of the Young diagram of λ_T and add a corner cell so that the new cell has cells to its left and above to obtain a partition of 9. This can be done in two ways and we obtain the partitions $(3,3,2,1)$ and $(3,3,1,1,1)$ as shown in Figure 6.1. Now for $r = 2$, we remove a cell from each of the first two rows (see the shaded cells in Figure 6.2) and add back two corner cells such that no new cell is in the same row or column as a previously deleted cell. This is possible in three ways; and we obtain partitions $(3,2,2,2)$, $(3,2,2,1,1)$ and $(3,2,1,1,1,1)$ as shown in Figure 6.2. Further, removing $r > 2$ cells is not possible in this case. So the possible partitions for $\lambda_{T'}$ are $(3,3,2,1)$, $(3,3,1,1,1)$, $(3,2,2,2)$, $(3,2,2,1,1)$ and $(3,2,1,1,1,1)$.

The conjecture has been verified using computer programs for smaller values of n and k, but it still seems open in the general case. Further, for given subspaces W, W' of V of dimensions k and $k+1$ respectively with $W \subset W'$ and a simple map $T \in L(W,V)$ with defect dimensions λ_T, it would be interesting to count the

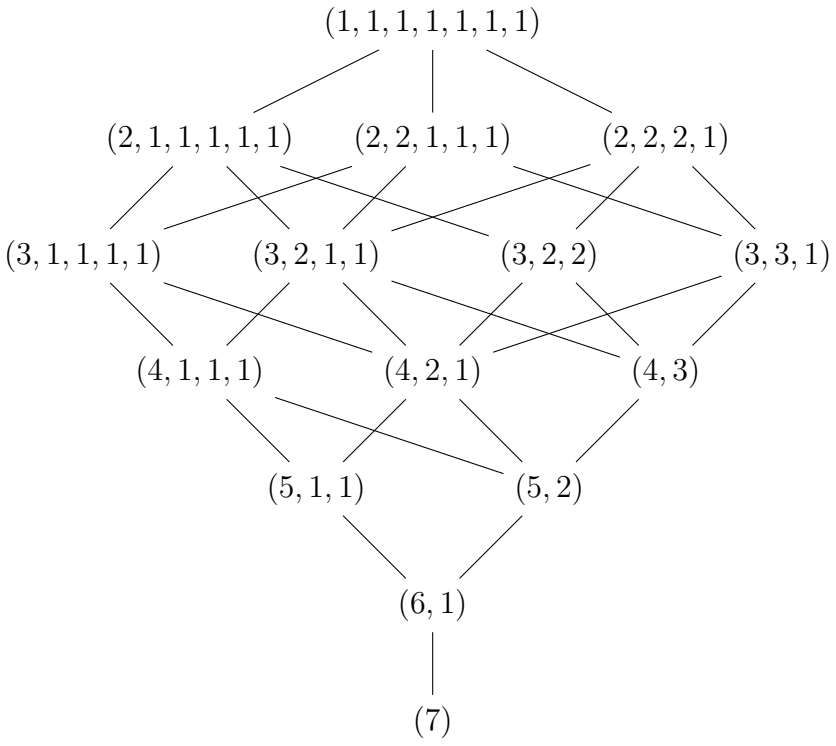

Figure 6.3: The Hasse diagram of Π_n for $n = 7$.

number of simple extension maps $T' \in L(W', V)$ corresponding to every possible partition $\lambda_{T'}$ obtained from λ_T by following the steps in Conjecture 6.2.1.

The theory of partially ordered sets (or posets) plays an important unifying role in enumerative combinatorics. We can make the set Π_n of all the integer partitions of n into a poset. To do this, we first recall that a partially ordered set (or poset) P is a set together with a binary relation $\leq$ that is reflexive ($t \leq t$ for all $t \in P$), antisymmetric (if $r \leq s$ and $s \leq r$, then $r = s$ for all $r, s \in P$) and transitive (if $r \leq s$ and $s \leq t$, then $r \leq t$ for all $r, s, t \in P$). We define $\lambda \leq \mu$ in Π_n if there exists simple linear transformations T, T' defined on some subspaces W, W' with $W \subset W'$ of an n-dimensional vector space V having defect dimensions as λ, μ respectively and $T'_{|W} = T$. It is easy to verify that the set Π_n with the relation '$\leq$' forms a poset. For example, when $n = 7$, the Hasse diagram for the poset is shown in the Figure 6.3. It would be another interesting problem

to study the properties of this poset for an arbitrary n.

Bibliography

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

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

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

[4] Akansha Arora and Samrith Ram. Enumerating partial linear transformations in a similarity class. *Linear Algebra Appl.*, 625:196–211, 2021.

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

[6] James W. Brewer, John W. Bunce, and F. S. Van Vleck. *Linear systems over commutative rings*, volume 104 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1986.

[7] Pavol Brunovský. A classification of linear controllable systems. *Kybernetika*, 6:173–188, 1970.

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

[9] Stephen D. Cohen, Sartaj Ul Hasan, Daniel Panario, and Qiang Wang. An asymptotic formula for the number of irreducible transformation shift registers. *Linear Algebra Appl.*, 484:46–62, 2015.

[10] 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.

[11] Glória Cravo. Matrix completion problems. *Linear Algebra Appl.*, 430(8-9):2511–2540, 2009.

[12] G. David Forney, Jr. Convolutional codes. I. Algebraic structure. *IEEE Trans. Information Theory*, IT-16:720–738, 1970.

[13] Paul A. Fuhrmann and Uwe Helmke. *The mathematics of networks of linear systems*. Universitext. Springer, Cham, 2015.

[14] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[15] Zhicheng Gao and Daniel Panario. Degree distribution of the greatest common divisor of polynomials over $\mathbb{F}_q$. *Random Structures Algorithms*, 29(1):26–37, 2006.

[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] Sudhir R. Ghorpade, Sartaj Ul Hasan, and Meena Kumari. Primitive polynomials, Singer cycles and word-oriented linear feedback shift registers. *Des. Codes Cryptogr.*, 58(2):123–134, 2011.

[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] Israel Gohberg, M. A. Kaashoek, and Frederik van Schagen. *Partially specified matrices and operators : classification, completion, applications*, volume 79 of *Operator theory, advances and applications*. Birkhäuser Verlag, Basel, Switzerland, Boston, 1995.

[21] M. Goresky and A. Klapper. Pseudonoise sequences based on algebraic feedback shift registers. *IEEE Transactions on Information Theory*, 52(4):1649–1662, April 2006.

[22] Xiangqian Guo and Guangyu Yang. The probability of rectangular unimodular matrices over $\mathbb{F}_q[x]$. *Linear Algebra Appl.*, 438(6):2675–2682, 2013.

[23] Michael A. Harrison. *Lectures on linear sequential machines*. Academic Press, New York-London, 1969.

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

[25] Nathan Jacobson. *Lectures in abstract algebra*. Graduate Texts in Mathematics, No. 31. Springer-Verlag, New York-Berlin, 1975. Volume II: Linear algebra, Reprint of the 1953 edition [Van Nostrand, Toronto, Ont.].

[26] Yupeng Jiang and Jiangshuai Yang. On the number of irreducible linear transformation shift registers. *Des. Codes Cryptogr.*, 83(2):445–454, 2017.

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

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

[29] Srinivasan Krishnaswamy and Harish K. Pillai. On multisequences and their extensions. *CoRR*, abs/1208.4501, 2012.

[30] Joseph P. S. Kung. The cycle structure of a linear transformation over a finite field. *Linear Algebra Appl.*, 36:141–155, 1981.

[31] Julia Lieb. The probability of primeness for specially structured polynomial matrices over finite fields with applications to linear systems and convolutional codes. *Math. Control Signals Systems*, 29(2):Art. 8, 39, 2017.

[32] Julia Lieb. Uniform probability and natural density of mutually left coprime polynomial matrices over finite fields. *Linear Algebra Appl.*, 539:134–159, 2018.

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

[34] Gérard Maze, Joachim Rosenthal, and Urs Wagner. Natural density of rectangular unimodular integer matrices. *Linear Algebra Appl.*, 434(5):1319–1324, 2011.

[35] Kent E. Morrison. Integer sequences and matrices over finite fields. *J. Integer Seq.*, 9(2):Article 06.2.1, 28, 2006.

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

[37] Amritanshu Prasad and Samrith Ram. Set partitions, tableaux, and subspace profiles under regular split semisimple matrices. arXiv: 2112.00479 [math.CO], 2021.

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

[39] Amritanshu Prasad and Samrith Ram. Splitting subspaces and a finite field interpretation of the touchard-riordan formula. arXiv:2205.11076 [math.CO], 2022.

[40] Daniel Quillen. Projective modules over polynomial rings. *Invent. Math.*, 36:167–171, 1976.

[41] Samrith Ram. Enumeration of linear transformation shift registers. *Designs, Codes and Cryptography*, 75(2):301–314, 2015.

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

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

[44] Eduardo D. Sontag. *Mathematical control theory: Deterministic Finite-Dimensional Systems*, volume 6 of *Texts in Applied Mathematics*. Springer-Verlag, New York, second edition, 1998.

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

[46] Richard Stong. Some asymptotic results on finite vector spaces. *Adv. in Appl. Math.*, 9(2):167–199, 1988.

[47] Shreyas Sundaram and Christoforos N. Hadjicostis. Structural controllability and observability of linear systems over finite fields with applications to multi-agent systems. *IEEE Trans. Automat. Control*, 58(1):60–73, 2013.

[48] A. A. Suslin. Projective modules over polynomial rings are free. *Dokl. Akad. Nauk SSSR*, 229(5):1063–1066, 1976.

[49] J. H. van Lint and R. M. Wilson. *A course in combinatorics*. Cambridge University Press, Cambridge, 1992.

[50] Yinghui Wang and Richard P. Stanley. The Smith normal form distribution of a random integer matrix. *SIAM J. Discrete Math.*, 31(3):2247–2268, 2017.

[51] Harald K. Wimmer. Existenzsätze in der Theorie der Matrizen und lineare Kontrolltheorie. *Monatsh. Math.*, 78:256–263, 1974.

[52] Ion Zaballa. Matrices with prescribed rows and invariant factors. *Linear Algebra Appl.*, 87:113–146, 1987.

List of Publications

1. Akansha Arora and Samrith Ram, Enumerating partial linear transformations in a similarity class, *Linear Algebra and its Applications* **625**, 196-211(2021). https://doi.org/10.1016/j.laa.2021.05.007.

2. Akansha Arora, Samrith Ram and Ayineedi Venkateswarlu, Unimodular polynomial matrices over finite fields, *Journal of Algebraic Combinatorics* **53**, 1299-1312(2021). https://doi.org/10.1007/s10801-020-00963-2.