# REPRESENTATION THEORY METHODS IN EXTREMAL COMBINATORICS

by

Rafael Plaza

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

Fall 2016

**REPRESENTATION THEORY METHODS**

**IN EXTREMAL COMBINATORICS**

by

Rafael Plaza

Approved: _____

Louis Rossi, Ph.D.
Chair of the Department of Mathematical Sciences

Approved: _____

George Watson, Ph.D.
Dean of the College of Arts and Sciences

Approved: _____

Ann L. Ardis, Ph.D.
Senior Vice Provost for Graduate and Professional Education

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Qing Xiang, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Sebastian Cioaba, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Felix Lazebnik, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Peter Sin, Ph.D.
Member of dissertation committee

## ACKNOWLEDGEMENTS

My deep gratitude goes first to Professor Xiang for providing the right combination of supervision, encouragement, and support during my Ph.D. studies. I thank him for his efforts on helping me become a better researcher. The freedom that Prof. Xiang gave me to approach research problems and to study topics of my interest was extremely important to keep me motivated during the past five years. I thank Professors Cioaba and Lazebnik for the courses that I took with them. I would also like to thank my collaborators, whose significant input is reflected in this document: Ling Long, and Peter Sin.

I must thank my wonderful girlfriend Luisa for her continuous support. Furthermore, I must also thank the friends that were with me at Delaware. Special thanks to: Jesus, David, Marie, Irene and Claudio.

Finally, I am deeply grateful to my family in special to my grandmother who taught me to work hard.

## TABLE OF CONTENTS

## LIST OF TABLES

## ABSTRACT

The research of this thesis lies in the area of extremal combinatorics. The word "extremal" comes from the kind of problems that are studied in this field. In fact, if a collection of finite objects (numbers, subsets, subspaces, graphs, etc.) satisfies some restrictions then the following questions are of interest from the perspective of extremal combinatorics: what is the maximum (minimum) size of those collections? what is the structure of the collections of maximum (minimum) size?

For example, in extremal set theory one studies these questions for subsets of $[n] = \{1, 2, \ldots, n\}$ subject to conditions such as the families of subsets are intersecting, anti-chain, included in another family of subsets, etc. This field has seen a tremendous growth in the past few decades. Remarkably, some of the results obtained in extremal set theory can be generalized when, instead of subsets, other objects are considered. The main results in this thesis are analogues of theorems in extremal set theory where, instead of subsets, objects like groups and subspaces are considered. First, we focus on generalizations of the Erdös-Ko-Rado theorem for permutation groups. In particular, for the group $PGL(2, q)$ we prove that intersecting families of maximum size are stable. Moreover, for the group $PSL(2, q)$ we prove that every intersecting family of maximum size is a coset of a point stabilizer. Secondly, we study rank resilience property of higher inclusion matrices of $r$-subsets vs. $s$-subsets. We prove that a $q$-analogue of this property holds, that is, the rank of the higher inclusion matrices of $r$-subspaces vs. $s$-subspaces is also resilient. Furthermore, we prove that this resilience property holds over any field in the set case and over any field of characteristic coprime to $q$ in the vector space case.

It is well known that, in general, these analogues of classical results are hard to prove. In fact, most of the proof ideas used to prove results in extremal set theory

cannot be applied in a straightforward way. The main tools used here to prove our results come from representation theory.

Representation theory is a branch of mathematics that studies algebraic structures by representing their elements as linear transformations of vector spaces. Indeed, one of the objectives of this thesis is to highlight how some tools provided by representation theory can be used to prove analogues of classical results in extremal combinatorics.

# Chapter 1

# INTRODUCTION

Extremal combinatorics is an area of discrete mathematics. The word extremal comes from the kind of problems that are studied in this field. In fact, if a collection of finite objects (numbers, subsets, subspaces, graphs, etc.) satisfies some restrictions then the following problems are of interest from the perspective of extremal combinatorics:

I What is the maximum (minimum) size of those collections?

II What is the structure of the collections attaining the maximum (minimum) size?

III What is the structure of the collections whose size is close to the maximum (minimum)?

Problem I is known as the upper or lower bound problem. In Problem II the objective is to characterize the structure of extremal (in terms of size) collections, therefore, this problem is known as the characterization problem. Similarly, in Problem III the objective is to characterize the structure of the collections whose size is close to the maximum. If the structure of these "almost" extremal collections is similar to the structure of the collections of maximum size, then we say that the extremal collections are *stable*. Hence, Problem III is know as the stability problem.

In particular, the area of extremal set theory studies the above three problems for subsets of a finite set $X$ subject to conditions such as the families of subsets are intersecting, anti-chain, included in another family of subsets, etc [33]. This field has seen an astonishing growth in the past few decades. As a consequence, many proof techniques have been used and developed to solve extremal set problems; for

example, the pigeonhole principle, inclusion-exclusion, induction, double-counting and more recently the probabilistic and linear algebra methods.

Remarkably, some of the results obtained in extremal set theory can be generalized when, instead of subsets, other objects are considered. The main results in this thesis are analogues of extremal set theory theorems where, instead of subsets, objects like groups and vector spaces are considered.

The Erdös-Ko-Rado (EKR) theorem [18] is a classical result in extremal set theory. It states that if $k < n/2$, an intersecting family of $k$-subsets of $[n] = \{1, 2, \ldots, n\}$ has size at most $\binom{n-1}{k-1}$; equality holds if and only if the family consists of all $k$-subsets containing a fixed element from $[n]$. Intersecting families of maximum size are called *extremal families*. Note that the EKR theorem solves Problems I and II for collections of $k$-subsets of $[n]$ constrained to be pairwise intersecting.

Some decades later, Frankl [19] completed the above program. He proved that the extremal intersecting families of $k$-subsets are not only unique, but also stable: any intersecting family of size close to the maximum is "close" in structure to an extremal family. Here, we prove analogues of these characterization and stability results for permutations groups. In particular, we consider the natural right actions of $PGL(2, q)$ and $PSL(2, q)$ on the set of points of $PG(1, q)$, where $q$ is a prime power.

A general approach in mathematics is to associate an algebraic object with the problem we want to study. The idea is that properties of the algebraic object may give valuable information that can be helpful to solve the problem. This general approach has been applied with success in extremal set theory where the notion of higher inclusion matrices has been used to prove many results [9, 19, 20, 23, 29, 38, 57, 58]. In this thesis we consider the following definition of higher inclusion matrices of $r$-subsets vs. $s$-subsets.

**Definition 1.** Let $n \geq r \geq s \geq 0$ be integers and $\mathcal{F}$ a family of $r$-subsets of $[n]$. The higher inclusion matrix $W_{r,s}^{\mathcal{F}}$ is a $(0, 1)$-matrix with rows indexed by the $r$-subsets in $\mathcal{F}$ and columns indexed by the $s$-subsets of $[n]$: the entry corresponding to $R \in \mathcal{F}$ and

$S \in \binom{[n]}{s}$[1] is equal to 1 if $S \subset R$ and 0, otherwise. If $\mathcal{F} = \binom{[n]}{r}$ we shall write $W_{r,s}$ instead of $W_{r,s}^{\mathcal{F}}$.

Let $\mathcal{F}$ be a family of $r$-subsets of $[n]$. The $s$-shadow of $\mathcal{F}$, denoted by $\partial_s^r \mathcal{F}$, consists of all $s$-subsets of $[n]$ that are contained in some element of $\mathcal{F}$. A fundamental result in extremal combinatorics, the Kruskal-Katona theorem, gives a sharp lower bound on the size of $\partial_{r-1}^r \mathcal{F}$. In order to state the theorem, we note that for positive integers $m$ and $r$ there are always unique integers $m_r > m_{r-1} > \cdots > m_j$ with $j \geq 0$ such that $m = \binom{m_r}{r} + \binom{m_{r-1}}{r-1} + \cdots + \binom{m_j}{j}$.

**Theorem 2.** *(Katona, [35]) Let $r \geq 1$ and $m \geq 1$. For every $\mathcal{F} \subset \binom{[n]}{r}$ with $m = |\mathcal{F}|$ we have*

$$|\partial_{r-1}^r \mathcal{F}| \geq \binom{m_r}{r-1} + \binom{m_{r-1}}{r-2} + \cdots + \binom{m_j}{j-1}.$$

*The inequality is best possible for every $r$ and $m \leq \binom{n}{r}$. Furthermore, if $m = \binom{m_r}{r}$, then equality holds if and only if $\mathcal{F} = \binom{X}{r}$, where $X$ is a $m_r$-subset of $[n]$.*

The following classical result in extremal combinatorics is known as the Lovász version of Kruskal-Katona theorem.

**Theorem 3.** *(Lovász, [44]) Let $\mathcal{F}$ be a family of $r$-subsets of $[n]$ such that $|\mathcal{F}| = \binom{x}{r}$. If $s < r$ then $|\partial_s^r \mathcal{F}| \geq \binom{x}{s}$. Equality holds if and only if $x$ is an integer and there exists a subset $X$ of $[n]$ of size $x$ such that $\mathcal{F} = \binom{X}{r}$.*

The above theorem can be proved in several different ways. Keevash [38] showed that Theorem 1 follows immediately from the following result on the rank of higher inclusion matrices.

**Theorem 4.** *(Keevash, [38]) For every $r > s > 0$ there is a number $n_{r,s}$ so that if $\mathcal{F}$ is a family of $r$-subsets of $[n]$ with $|\mathcal{F}| = \binom{x}{r} \geq n_{r,s}$ then $rank_{\mathbb{Q}}(W_{r,s}^{\mathcal{F}}) \geq \binom{x}{s}$. Equality holds if and only if $x$ is an integer and there exists a subset $X$ of $[n]$ of size $x$ such that $\mathcal{F} = \binom{X}{r}$.*

[1] We denote by $\binom{[n]}{s}$ the family of $s$-subsets consisting of all $s$-subsets of $[n]$.

To see how Theorem 3 follows from Theorem 4 (for large $x$), one simply observes that $\text{rank}_{\mathbb{Q}}(W_{r,s}^{\mathcal{F}})$ is less than or equal to the number of nonzero columns of $W_{r,s}^{\mathcal{F}}$ (which is the size of the $s$-shadow). In order to prove Theorem 4, Keevash [38] showed that the rank of the matrix $W_{r,s}$ is *resilient* or *robust*, that is, one can remove many rows (in an arbitrary way) of $W_{r,s}$ without lowering its rank.

**Theorem 5.** *(Keevash, [38]) Suppose $0 \leq s \leq r$ and $2r + s \leq n$. If $\mathcal{F}$ is a family of $r$-subsets with $|\binom{[n]}{r} \setminus \mathcal{F}| \leq \binom{n}{s}^{-1}\binom{n}{r-s}$ then $\text{rank}_{\mathbb{Q}}(W_{r,s}^{\mathcal{F}}) = \text{rank}_{\mathbb{Q}}(W_{r,s})$.*

Keevash went further to ask whether Theorem 5 remains true under the assumption $|\binom{[n]}{r} \setminus \mathcal{F}| < \binom{n-s}{r-s}$. This question was answered in the affirmative by Grosu, Person and Szabó [29] for $n$ large compared to $r$ and $s$. Furthermore, Theorem 5 implies that the $s$-shadow of every family of $r$-subsets of $[n]$ whose size is close enough to $\binom{n}{r}$ is equal to $\binom{[n]}{s}$ (although this observation follows immediately from the definition of $s$-shadow). In the end of [29], the authors remarked that the resilience property of the higher inclusion matrices has not been studied over fields of positive characteristic. In this thesis we prove that the rank of $W_{r,s}$ is resilient over any field $K$.

Moreover, we prove an analogue of Theorem 5 where instead of consider families of $r$-subsets we consider families of $r$-dimensional subspaces of a vector space of dimension $n$ over $\mathbb{F}_q$.

Experience in extremal combinatorics has shown that these analogues of classical results are hard to prove in general. In fact, most of the proof ideas used to prove results in extremal set theory cannot be applied in a straightforward way. The main tools used in this thesis to prove our results come from representation theory.

Representation theory [53] is a branch of mathematics that studies algebraic structures by representing their elements as linear transformations of vector spaces. Indeed, one of the objectives of this thesis is to highlight how some tools provided by representation theory can be used to prove analogues of classical results in extremal combinatorics. We expect to provide enough evidence to support our claim that *the*

*representation theory method* is another powerful tool to attack problems in extremal combinatorics.

## 1.1 Main Results of the Thesis

### 1.1.1 Stability of Intersecting Families in $PGL(2,q)$

We consider the right action of the 2-dimensional projective general linear group $PGL(2,q)$ on the projective line $PG(1,q)$. A subset $S$ of $PGL(2,q)$ is said to be an *intersecting family* if for every $g_1, g_2 \in S$, there exists $x \in PG(1,q)$ such that $x^{g_1} = x^{g_2}$.

In [45], Meagher and Spiga studied Problems I and II for the group $PGL(2,q)$ acting on the set of points of the projective line $PG(1,q)$. These authors proved that the maximum size of an intersecting family in $PGL(2,q)$ is $q(q-1)$. Furthermore, they also solved the characterization problem: Every intersecting family of maximum size in $PGL(2,q)$ is a coset of a point stabilizer.

In this thesis, we prove that intersecting families of maximum size in $PGL(2,q)$ are also stable; that is, an intersecting family in $PGL(2,q)$ whose size is close to $q(q-1)$ must be close in structure to a coset of a point stabilizer. This result is stated more precisely in Theorem 40. Moreover, in Theorem 41 we use this stability result to show that if the size of $S$ is close enough to $q(q-1)$ then $S$ must be contained in a coset of a point stabilizer. Note that our stability result completes the program for $PGL(2,q)$, that is, Problem I, II and III have been solved for $PGL(2,q)$.

The main tools used to prove this result are the eigenvalue method and analysis of Boolean functions on $PGL(2,q)$. The eigenvalue method was introduced by Lóvasz [43] as a new way to prove the EKR theorem. Since then, it has been used many times to prove analogues of the EKR theorem [15, 26, 45, 57]. The analysis of Boolean functions on finite groups has been an active research area especially in theoretical computer science. A lot of work has been done in recent years to characterize Boolean functions whose Fourier transforms are highly concentrated on some irreducible representations. Friedgut, Kalai and Naor [22] proved that a Boolean function on $\mathbb{Z}_2^n$ whose Fourier transform is close to being concentrated on the first two levels, must be close to a

dictatorship (a function determined by just one coordinate). Furthermore, similar results have been obtained for other abelian groups [1, 31]. Recently, Ellis, Filmus and Friedgut [16] showed that similar results can be obtained for the symmetric group $S_n$. Specifically, they proved that if the Fourier transform of a Boolean function $f$ is highly concentrated on the first two irreducible representations of $S_n$ and $\frac{1}{n!}\sum_{x\in S_n} f(x) = O(\frac{1}{n})$ then $f$ must be close to a union of cosets of points stabilizers.

### 1.1.2 Characterization of Intersecting Families of Maximum Size in $PSL(2,q)$

*This work is in collaboration with L. Long, P. Sin and Q. Xiang.*

We consider the action of the 2-dimensional projective special linear group $PSL(2,q)$ on the projective line $PG(1,q)$. A subset $S$ of $PSL(2,q)$ is said to be an intersecting family if for any $g_1, g_2 \in S$, there exists $x \in PG(1,q)$ such that $x^{g_1} = x^{g_2}$.

In this thesis, we study Problem II for the group $PSL(2,q)$ acting on $PG(1,q)$ when $q$ is an odd prime power[2]. It is known, from the combined results of [3, 45], that the maximum size of an intersecting family in $PSL(2,q)$ is $q(q-1)/2$. However, it is only a conjecture that all intersecting families of maximum size are cosets of point stabilizers. (See the second part of Conjecture 1 in [45].) In Theorem 46, we prove this conjecture in the affirmative for all odd prime powers $q$.

To prove Theorem 46 we apply a general method for solving Problem II for some 2-transitive groups. This technique was proposed by Ahmadi and Meagher in [3] and they called it "The Module Method". This method reduces the characterization of intersecting families of maximum size to the computation of the $\mathbb{C}$-rank of a matrix whose definition is given below.

**Definition 6.** Let $X$ be a finite set and $G$ a finite group acting on $X$. An element $g \in G$ is said to be a *derangement* if its action on $X$ is fixed-point-free. The *derangement matrix* of $G$ acting on $X$ is the $(0,1)$-matrix $M$, whose rows are indexed by the derangements of $G$, whose columns are indexed by the ordered pairs of distinct

[2] The case when $q$ is a power of 2 was already solved in [45] because when $q$ is even one has $PGL(2,q) = PSL(2,q)$.

elements in $X$, and for any derangement $g \in G$ and $(a, b) \in X \times X$ with $a \neq b$, the $(g, (a, b))$-entry of $M$ is defined by

$$M(g, (a, b)) = \begin{cases} 1, & \text{if } a^g = b, \\ 0, & \text{otherwise.} \end{cases}$$

The Module Method states that, under certain conditions, if the rank of the derangement matrix $M$ of $G$ acting on $X$ is equal to $(|X| - 1)(|X| - 2)$, then the cosets of point stabilizers are the only intersecting families of maximum size in $G$. This technique has been applied to show that the cosets of points stabilizers are the only intersecting families of maximum size for the symmetric group [26], the alternating group [4], $PGL(2, q)$ [45], and many others groups [3].

Thus, in order to prove Theorem 46 by applying the Module Method, it is enough to show that the rank of the derangement matrix $M$ of $PSL(2, q)$ acting on $PG(1, q)$ is equal to $q(q - 1)$. This result is proven in Theorem 47.

Our main tools in the proof of Theorem 47 are the representation theory of $PGL(2, q)$ and character sums over finite fields. We use representation theory to reduce the problem of computing the rank of $M$ to the problem of showing that $q$ character sums over $PGL(2, q)$ are not equal to zero. It turns out that these character sums can be written in terms of Legendre and Soto-Andrade sums (see Section 2.7). This is not a surprise; it is well known that these finite fields character sums appear in connection with the complex representation theory of $PGL(2, q)$ [34]. To prove that the values of these character sums are not equal to zero the following facts will be crucial:

1. The Legendre and Soto-Andrade sums (see Definitions 24 and 25) on $\mathbb{F}_q$ form an orthogonal basis in the inner product space $\ell_2(\mathbb{F}_q, m)$ [34], where $m$ is the measure assigning mass $q + 1$ to the points $\pm 1$ and mass 1 to all other points.

2. The Legendre sums may be expressed in terms of hypergeometric functions over finite fields (see Section 2.5). These functions were introduced by Greene in [25] and Katz in [37] and since that they have been extensively studied [2, 24, 34].

### 1.1.3 Rank Resilience of Higher Inclusion Matrices

*This work is in collaboration with Q. Xiang.*

We generalize Theorem 5 in two directions. First, we prove that the rank of $W_{r,s}$ is resilient over any field $K$. In fact, Theorem 65 shows that if the size of $\mathcal{F}$ is close to $\binom{n}{r}$ then $\text{rank}_K(W_{r,s}) = \text{rank}_K(W_{r,s}^{\mathcal{F}})$. Furthermore, a similar result is proven for higher inclusion matrices of $r$-subspaces vs. $s$-subspaces whose definition is given below.

**Definition 7.** Let $q = p^t$ with $t$ a positive integer and $p$ a prime number. We denote by $\mathbb{F}_q$ the finite field with $q$ elements and by $\mathbb{F}_q^n$ a $n$-dimensional vector space over $\mathbb{F}_q$. Let $n \geq r \geq s \geq 0$ be integers and $\mathcal{F}$ a family of $r$-dimensional subspaces of $\mathbb{F}_q^n$. The higher inclusion matrix of $r$-subspaces vs. $s$-subspaces, denoted by $W_{r,s}^{\mathcal{F}}(q)$, is a $(0,1)$-matrix with rows indexed by the $r$-dimensional subspaces of $\mathcal{F}$ and columns indexed by the $s$-dimensional subspaces of $\mathbb{F}_q^n$ such that the entry corresponding to $R \in \mathcal{F}$ and $S \in \begin{bmatrix} \mathbb{F}_q^n \\ s \end{bmatrix}$ is equal to 1 if $S$ is a subspace of $R$ and 0, otherwise. In the case when $\mathcal{F} = \begin{bmatrix} \mathbb{F}_q^n \\ r \end{bmatrix}$ we shall write $W_{r,s}(q)$ instead of $W_{r,s}^{\mathcal{F}}(q)$.

In Theorem 75 we prove that the $K$-rank of $W_{r,s}(q)$ is also resilient or robust over any field $K$ with $char(K) \neq p$. Therefore, if the size of $\mathcal{F}$ is close enough to $\begin{bmatrix} n \\ r \end{bmatrix}$ then $\text{rank}_K(W_{r,s}(q)) = \text{rank}_K(W_{r,s}^{\mathcal{F}}(q))$. This result implies that the $s$-shadow of every family of $r$-subspaces of $\mathbb{F}_q^n$ whose size is close enough to $\begin{bmatrix} n \\ r \end{bmatrix}$ is equal to $\begin{bmatrix} \mathbb{F}_q^n \\ s \end{bmatrix}$.

Our techniques to prove these resilience results are different from those used by Keevash in [38] and Grosu, Person and Szabó in [29]. The main tool we use here to prove Theorem 65 is a basis which provides a diagonal form for the higher inclusion matrix $W_{r,s}$. This basis was found by Bier in [9]. Remarkably, if the size of $\mathcal{F}$ is close to $\binom{n}{r}$ then it also provides an almost diagonal form for the matrix $W_{r,s}^{\mathcal{F}}$. We shall use this property to compute the rank of $W_{r,s}^{\mathcal{F}}$.

To prove Theorem 75 we proceed as in the proof of Theorem 65. Unfortunately, to the best of our knowledge there is no $q$-analogue of Bier basis available. To deal with this difficulty we use some results from representation theory of $GL(n,q)$. The work

of James [32] and Frumkin and Yakir [23] explicitly shows a connection between the rank of higher inclusion matrices and the Specht modules of $GL(n,q)$. We apply some properties of Specht modules of $GL(n,q)$ to prove that the column space of $W_{r,s}^{\mathcal{F}}(q)$ contains at least $rank_K(W_{r,s}(q))$ linearly independent vectors. This result is enough to prove Theorem 75, because the rank of $W_{r,s}^{\mathcal{F}}(q)$ is clearly bounded above by the rank of $W_{r,s}(q)$.

## 1.2 Organization of the Thesis

In Chapter 2 we recall some definitions and results that will be used in later chapters. In the process we also introduce our notation. Section 2.6 requires some advanced knowledge of number theory. The reader may focus on the result of Proposition 23 and skip the rest of this section since only that result will be used later. In Chapter 3 we introduce EKR-problems for permutation groups. Furthermore, we give a brief review of some techniques that have been used to solve these problems such as the eigenvalue, module and Fourier analysis methods. In Chapter 4, applying the Fourier analysis method we prove a stability result for intersecting families in $PGL(2,q)$. In chapter 5 we characterize intersecting families of maximum size in $PSL(2,q)$ by applying the module method. In Chapter 6 and 7 we prove the resilience property of the higher inclusion matrices $W_{r,s}$ and $W_{r,s}(q)$, respectively. We conclude the thesis in Chapter 8, raising some open problems related to the work developed here.

# Chapter 2

# PRELIMINARIES

In this chapter we recall some definitions and results that will be used in later chapters, in the process we also introduce our notation. We start by reviewing standard facts about general representation theory and Fourier transform on finite groups. We continue reviewing some properties of the groups $PGL(2,q)$ and $PSL(2,q)$, and their complex irreducible characters. Finally, we present a brief introduction to the study of hypergeometric functions over finite fields and their connections with Legendre and Soto-Andrade sums.

## 2.1 General Representation Theory

In this section we recall some basic notions and results from representation theory. For more background, the reader may consult [53].

**Definition 8.** Let $G$ be a finite group and $K$ a field. A $K$-representation of $G$ is a pair $(\rho, V)$, where $V$ is a finite dimensional $K$-vector space and $\rho$ is a homomorphism from $G$ to the group of linear automorphisms of $V$. In this context, the vector space $V$ is called a $G$-module. Moreover, if $\dim(V) = n$ then we say that $(\rho, V)$ is a representation of $G$ of degree $n$.

Assume that $(\rho, V)$ is a $K$-representation of some finite group $G$. A subspace $W$ of $V$ is said to be a submodule of $V$ if it is closed under the action of $G$; that is, for any $w \in W$ one has $\rho(g)w \in W$, for all $g \in G$. The $G$-module $V$ contains at least two submodules, $W = V$ and $W = \{0\}$. These are called the trivial submodules. We say that $V$ is a reducible $G$-module if it contains a non-trivial submodule. Otherwise, $V$ is said to be irreducible.

**Definition 9.** Let $V$ and $W$ be $G$-modules. A $G$-module homomorphism is a linear transformation $\theta : V \to W$ such that $\theta(\rho(g)v) = \rho(g)\theta(v)$ for all $g \in G$ and $v \in V$. If $\theta$ is a bijection then we say $\theta$ is a $G$-module isomorphism and that $V$ and $W$ are isomorphic $G$-modules.

The following fact follows directly from Definition 9.

**Lemma 10.** *Let $V$ and $W$ be $G$-modules and $\theta : V \to W$ a $G$-module homomorphism. Then the kernel and image of $\theta$ are $G$-submodules of $V$ and $W$, respectively.*

Remarkably, $G$-module homomorphisms of irreducible modules are easy to characterize. A classical result in representation theory deals with this characterization.

**Lemma 11** (Schur's Lemma)**.** *Let $W_1$ and $W_2$ be two irreducible $G$-modules. If $\theta : W_1 \to W_2$ is a $G$-module homomorphism, then either*

1. *$\theta$ is a $G$-module isomorphism, or*
2. *$\theta$ is the zero map.*

Let $\langle \cdot, \cdot \rangle$ be an inner product defined on $V$. Let $W$ be a subspace of $V$. We define the orthogonal complement of $W$ by

$$W^{\perp} = \{v \in V : \langle v, w \rangle = 0 \text{ for all } w \in W\}.$$

We say that $\langle \cdot, \cdot \rangle$ is *invariant under the action* of $G$ if it satisfies that,

$$\langle gv, gw \rangle = \langle v, w \rangle \quad \text{for all } g \in G \text{ and } v, w \in V.$$

Moreover, the next lemma establishes that when $W$ is a $G$-submodule of $V$ and the inner product $\langle \cdot, \cdot \rangle$ is $G$-invariant then $W^{\perp}$ is not only a subspace of $V$ but also a submodule.

**Lemma 12.** *Let $V$ be a $G$-module, $W$ a submodule of $V$, and $\langle \cdot, \cdot \rangle$ an inner product invariant under the action of $G$. Then $W^{\perp}$ is a $G$-submodule.*

We denote by $K[G]$ the vector space of $K$-valued functions on $G$. We equip $K[G]$ with the following inner product

$$\langle \chi, \psi \rangle_G = \frac{1}{G} \sum_{g \in G} \chi(g) \overline{\psi(g)}.$$

where $\chi$ and $\psi$ are functions in $K[G]$. For a representation of $G$, we define the character of the representation as follows.

**Definition 13.** Let $(\rho, V)$ be a $K$-representation of $G$. We define the function $\chi_\rho$ associated with $\rho$ as the map given by

$$\begin{array}{rccc} \chi_\rho : & G & \to & K \\ & g & \mapsto & Tr(\rho(g)), \end{array}$$

where $Tr$ denotes the trace of a linear transformation. We say that $\chi_\rho$ is the character associated with $\rho$.

If $\rho$ is an irreducible representation then we say that $\chi_\rho$ is an irreducible character. These functions have been extensively studied [53]. In particular, we recall the orthogonality relations for characters.

**Lemma 14.** *Let $\rho_1$ and $\rho_2$ be non-isomorphic irreducible representations of $G$. Then their irreducible characters $\chi_{\rho_1}$ and $\chi_{\rho_2}$ are orthogonal, i.e. $\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle_G = 0$.*

For the rest of this section we consider complex representations. It is well known that there exists a finite number of non-isomorphic complex irreducible representations of $G$. The following result implies that every complex representation of $G$ is isomorphic to a direct sum of irreducible representations.

**Theorem 15** (Maschke's Theorem)**.** *Let $G$ be a finite group and let $V$ be a nonzero $G$-module over $\mathbb{C}$. Let $\{V_1, \ldots, V_n\}$ is a complete set of non-isomorphic irreducible representations of $G$. Then*

$$V \cong V^{\oplus m_1} \oplus V_2^{\oplus m_2} \oplus \cdots \oplus V_n^{\oplus m_n} \tag{2.1}$$

*where each $m_i$ is a non-negative integer called the multiplicity of $V_i$ in $V$.*

We will usually denote by $V_\chi$ the $G$-module associated with an irreducible character $\chi$ of G. Let $\chi_1, \ldots, \chi_n$ be the characters associated with irreducible representations $(\rho_1, V_{\chi_1}), \ldots, (\rho_n, V_{\chi_n})$, respectively. We can rewrite equation (2.1) in terms of characters,

$$\chi_\rho = m_1\chi_1 + m_2\chi_2 + \cdots + m_n\chi_n.$$

Furthermore, there is a nice formula to express the integers $m_i$ in terms of the characters $\chi_\rho$ and $\chi_i$. In fact, we have

$$m_i = \langle \chi_\rho, \chi_i \rangle_G$$

for any irreducible character $\chi_i$.

Let $H$ be a subgroup of $G$ and $\chi$ a character of $G$. We can easily note that if we restrict $\chi$ to $H$ then we get a character of $H$. We denote the restriction of $\chi$ to $H$ by $\mathrm{Res}^H_G(\chi)$. On the other hand, if $\psi$ is a character of $H$ then we can get a character of $G$ using the following formula:

$$\mathrm{Ind}^G_H(\psi)(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \psi(x^{-1}gx).$$

The character $\mathrm{Ind}^G_H(\psi)$ is called the character induced by $\psi$ from $H$ to $G$. The following result relates inner products of restricted and induced characters.

**Theorem 16** (Frobenius Reciprocity Law)**.** *Let $H \leq G$. Let $\chi$ and $\psi$ be characters of $H$ and $G$, respectively. Then*

$$\langle \psi, Ind^G_H(\chi) \rangle_G = \langle Res^H_G(\psi), \chi \rangle_H$$

*where the inner product on the left is calculated in $G$ and the one to the right in $H$.*

## 2.2 Fourier Analysis

Let G be a finite group. We denote by $\mathbb{C}[G]$ the vector space of all complex valued functions on $G$.

**Definition 17.** Let $R$ be a complete set of non-isomorphic irreducible matrix representations of $G$. The *Fourier transform* of $f \in \mathbb{C}[G]$ is a matrix-valued function on irreducible representations. Its value at the irreducible representation $\rho \in R$ is

$$\widehat{f}(\rho) = \frac{1}{|G|} \sum_{s \in G} f(s)\rho(s).$$

We apply the Fourier transform to decompose the vector space $\mathbb{C}[G]$ into a direct sum of subspaces indexed by the irreducible representations of $G$. For every $\rho \in R$, we denote by $\widehat{V}_\rho$ the subspace of $\mathbb{C}[G]$ consisting of all functions whose Fourier transform is supported only on $\rho$, more precisely,

$$\widehat{V}_\rho = \{f \in \mathbb{C}[G] : \widehat{f}(\rho') = 0, \text{ for all } \rho' \neq \rho, \ \rho' \in R\}.$$

Since the Fourier transform is an invertible linear transformation, we can write

$$\mathbb{C}[G] = \bigoplus_{\rho \in R} \widehat{V}_\rho.$$

By abuse of notation, we will sometimes use $\widehat{V}_{\chi_\rho}$ to denote $\widehat{V}_\rho$ where $\chi_\rho$ is the irreducible character afforded by $\rho$.

*Remark* 18. In the previous section, we define $V_{\chi_\rho}$ as the $G$-module associated with the irreducible character $\chi_\rho$. There is a close relation between $V_{\chi_\rho}$ and $\widehat{V}_{\chi_\rho}$, in fact

$$\widehat{V}_{\chi_\rho} \cong \underbrace{V_{\chi_\rho} \oplus \cdots \oplus V_{\chi_\rho}}_{n \text{ times}}$$

where $n$ is the degree of $\rho$. Therefore, if the degree of $\rho$ is $n$ then $V_{\chi_\rho}$ is a module of dimension $n$ and $\widehat{V}_{\chi_\rho}$ is a module of dimension $n^2$.

Recall that we can make $\mathbb{C}[G]$ an inner product space. For any $f, g \in \mathbb{C}[G]$ we define

$$\langle f, g \rangle_G = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)},$$

and we denote by $\|f\|_G$ the Euclidean norm induced by this inner product

$$\|f\|_G = \sqrt{\frac{1}{|G|} \sum_{g \in G} |f(g)|^2}.$$

Let $U$ be any subspace of $\mathbb{C}[G]$ and $f \in \mathbb{C}[G]$. We denote by $U^{\perp}$ the orthogonal complement of $U$ and by $P_U(f)$ the projection of $f$ onto $U$. Thus, we can write

$$f = P_U(f) + P_{U^{\perp}}(f).$$

For every 2-transitive group $G$, the vector space $\mathbb{C}[G]$ contains a subspace $V_{\chi_{std}}$ associated with an irreducible representation called standard representation. We review some basic facts about this representation. Let $X = \{1, \ldots, n\}$ be a set and $\mathbb{C}[X]$ be the vector space of all $\mathbb{C}$-valued functions defined on $X$. For every $i \in X$, we define $e_i$ as the function on $X$ which takes the value 1 at $i$ and 0 elsewhere. Let $G$ be a group acting on $X$ on the right. This action turns $\mathbb{C}[X]$ into a representation of $G$ of degree $n$. Indeed, this representation is produced by a linear extension of the (left) action defined by $g(e_i) = e_{ig^{-1}}$ for all $g \in G$ and $i \in X$. The vector subspace $V_{\chi_{std}}$ spanned by the vectors $\{\sum_{i=1}^{n} x_i e_i : \sum x_i = 0\}$ is a subrepresentation of $\mathbb{C}[X]$ of degree $n-1$, known as the standard representation of $G$. We denote by $\chi_{std}$ the character afforded by the standard representation (we will refer to $\chi_{std}$ as the standard character of $G$). It follows by definition that for every $g \in G$, the value $\chi_{std}(g)$ corresponds to the number of elements in $X$ fixed by $g$ minus one. Furthermore, if the action of $G$ on $X$ is 2-transitive then $\chi_{std}$ is an irreducible character and there exists a subspace $\widehat{V}_{\chi_{std}}$ of $\mathbb{C}[G]$ of dimension $(n-1)^2$.

### 2.3 The Groups $PGL(2,q)$ and $PSL(2,q)$

Let $\mathbb{F}_q$ be the finite field of size $q$ and $\mathbb{F}_{q^2}$ its unique quadratic extension. We denote by $\mathbb{F}_q^*$ and $\mathbb{F}_{q^2}^*$ the multiplicative groups of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, respectively. Let $GL(2,q)$ be the group of all invertible $2 \times 2$ matrices over $\mathbb{F}_q$ and $SL(2,q)$ the subgroup of all invertible $2 \times 2$ matrices with determinant 1. The center $Z(GL(2,q))$ of $GL(2,q)$ consists of all non-zero scalar matrices and we define $PGL(2,q) = GL(2,q)/Z(GL(2,q))$ and $PSL(2,q) = SL(2,q)/\left(SL(2,q) \cap Z(SL(2,q))\right)$. If $q$ is odd then $PSL(2,q)$ is a subgroup of $PGL(2,q)$ of index 2, while if $q$ is even then $PGL(2,q) = PSL(2,q)$.

We denote by $PG(1,q)$ the set of 1-dimensional subspaces of the space $\mathbb{F}_q^2$ of row vectors of length 2. Thus, $PG(1,q)$ is a projective line over $\mathbb{F}_q$ and its elements

are called projective points. An easy computation shows that $PG(1,q)$ has cardinality $q+1$. From the above definitions, it is clear that the $GL(2,q)$-action on $\mathbb{F}_q^2$ by right multiplication induces a natural right action of the groups $PGL(2,q)$ and $PSL(2,q)$ on $PG(1,q)$. The action of the subgroup $PSL(2,q)$ is 2-transitive, that is, given any two ordered pairs of distinct points there is a group element sending the first pair to the second. The action of $PGL(2,q)$ is *sharply* 3-*transitive*, that is, given any two ordered triples of distinct points there is a unique group element sending the first triple to the second.

### 2.4 The Character Table of $PGL(2,q)$

We briefly describe the character table of $PGL(2,q)$. We refer the reader to [48] for a complete study of the complex irreducible characters of $PGL(2,q)$. We start by describing its conjugacy classes. By abuse of notation we will denote the elements of $PGL(2,q)$ by $2\times 2$ matrices with entries from $\mathbb{F}_q$.

First note that, the elements of $PGL(2,q)$ can be collected into four sets: The set consisting of the identity element only; the set consisting of the non-scalar matrices with only one eigenvalue in $\mathbb{F}_q$; the set consisting of matrices with two distinct eigenvalues in $\mathbb{F}_q$; and the set of matrices with no eigenvalues in $\mathbb{F}_q$. Recall that the elements of $PGL(2,q)$ are projective linear transformations so if $\{x_1,x_2\}$ are eigenvalues of some $g\in PGL(2,q)$ then $\{ax_1,ax_2\}$ are also eigenvalues of $g$ for any $a\in\mathbb{F}_q^*$. Hence, the eigenvalues of elements in $PGL(2,q)$ are defined up to multiplication by elements of $\mathbb{F}_q^*$.

The identity of $PGL(2,q)$, denoted by $I$, defines a conjugacy class of size 1. Every non-identity element of $PGL(2,q)$ having only one eigenvalue in $\mathbb{F}_q^*$ is conjugate to

$$u=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

The conjugacy class of $u$ contains $q^2-1$ elements. The elements having two distinct

eigenvalues in $\mathbb{F}_q$ are conjugate to

$$d_x = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

for some $x \in \mathbb{F}_q^* \setminus \{1\}$. Moreover, $d_x$ and $d_y$ are conjugated if and only if $x = y$ or $x = y^{-1}$. The size of the conjugacy class containing $d_x$ is $q(q+1)$ for $x \in \mathbb{F}_q^* \setminus \{\pm 1\}$ and $q(q+1)/2$ for $x = -1$ (note that when $q$ is even there is no element of order 2 in $\mathbb{F}_q^*$). Finally, the elements of $PGL(2,q)$ with no eigenvalues in $\mathbb{F}_q^*$ are conjugate to

$$v_r = \begin{pmatrix} 0 & 1 \\ -r^{1+q} & r + r^q \end{pmatrix}$$

for some $r \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$. The matrices $v_r$ have eigenvalues $\{r, r^q\}$. Hence, $v_{r_1}$ and $v_{r_2}$ lie in the same conjugacy class if and only if $r_1\mathbb{F}_q^* = r_2\mathbb{F}_q^*$ or $r_1\mathbb{F}_q^* = r_2^{-1}\mathbb{F}_q^*$. The size of the conjugacy class containing $v_r$ is $q(q-1)$ if $r \in \mathbb{F}_{q^2}^* \setminus (\mathbb{F}_q^* \cup j\mathbb{F}_q^*)$ and $q(q-1)/2$ if $r \in j\mathbb{F}_q^*$, where $j$ is an element of $\mathbb{F}_{q^2}^*$ such that $j^2 \in \mathbb{F}_q^*$ (again when $q$ is even there is no element of order 2 in $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$).

The complex irreducible characters of $PGL(2,q)$ are described in Table 2.1. They also come in four families. First the characters $\lambda_1$ and $\lambda_{-1}$ correspond to representations of degree 1. Here $\lambda_1$ is the trivial character and the values of $\lambda_{-1}$ depend on a function $\delta$ which is defined as follows: $\delta(x) = 1$ if $d_x \in PSL(2,q)$ and $\delta(x) = -1$ otherwise, similarly, $\delta(r) = 1$ if $v_r \in PSL(2,q)$ and $\delta(r) = -1$ otherwise (note that $\lambda_{-1}$ arises only when $q$ is odd).

Secondly, the characters $\psi_1$ and $\psi_{-1}$ correspond to representations of degree $q$. The character $\psi_1$ is the standard character which is an irreducible character of $PGL(2,q)$. Thus, for every $g \in PGL(2,q)$, the value of $\psi_1(g)$ is equal to the number of projective points fixed by $g$ in $PG(1,q)$ minus 1. The values of $\psi_{-1}$ depend on the function $\delta$ defined above and it arises only when $q$ is odd.

The third family of irreducible characters is known as the principal series of $PGL(2,q)$. These characters correspond to representations of degree $q+1$ and their

**Table 2.1:** Character table of $PGL(2,q)$

| | $I$ | $u$ | $d_x$ | $d_{-1}$ ($q$ odd) | $v_r$ | $v_i$ ($q$ odd) |
|---|---|---|---|---|---|---|
| $\lambda_1$ | 1 | 1 | 1 | 1 | 1 | 1 |
| $\lambda_{-1}$ ($q$ odd) | 1 | 1 | $\delta(x)$ | $\delta(-1)$ | $\delta(r)$ | $\delta(i)$ |
| $\psi_1$ | $q$ | 0 | 1 | 1 | $-1$ | $-1$ |
| $\psi_{-1}$ ($q$ odd) | $q$ | 0 | $\delta(x)$ | $\delta(-1)$ | $-\delta(r)$ | $-\delta(i)$ |
| $\eta_\beta$ | $q-1$ | $-1$ | 0 | 0 | $-\beta(r)-\beta(r^q)$ | $-2\beta(i)$ |
| $\nu_\gamma$ | $q+1$ | 1 | $\gamma(x)+\gamma(x^{-1})$ | $2\gamma(-1)$ | 0 | 0 |

values depend on multiplicative characters of $\mathbb{F}_q$. In fact, the label $\gamma$ in Table 2.1 runs through all the homomorphism $\gamma : \mathbb{F}_q^* \to \mathbb{C}$ of order greater than 2 up to inversion.

Finally, the fourth family is known as the cuspidal characters of $PGL(2,q)$. They correspond to representations of degree $q-1$ and their values depend on multiplicative characters of $\mathbb{F}_{q^2}$. In fact, the label $\beta$ in Table 2.1 runs through all homomorphism $\beta : \mathbb{F}_{q^2}^*/\mathbb{F}_q^* \to \mathbb{C}$ of order greater than 2 up to inversion. Note that every $\beta$ corresponds to a unique multiplicative character of $\mathbb{F}_{q^2}$ which is trivial on $\mathbb{F}_q^*$.

We define some subsets of multiplicative characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$. We use these sets as indexes for the irreducible representations of $PGL(2,q)$.

**Definition 19.** Assume that $q$ is an odd prime power. We denote by $A$ and $B$ a fixed selection of characters $\gamma$ and $\beta$, as defined above, up to inversion of size $(q-3)/2$ and $(q-1)/2$, respectively. Therefore, the principal series and cuspidal irreducible characters of $PGL(2,q)$ are given by $\{\nu_\gamma\}_{\gamma\in A}$ and $\{\eta_\beta\}_{\beta\in B}$, respectively.

## 2.5 Hypergeometric Functions over Finite Fields

A (generalized) hypergeometric function with parameters $a_i, b_j$ is defined by

$$ {}_{n+1}F_n\left[\begin{matrix} a_1 & a_2 & \cdots & a_{n+1} \\ & b_1 & \cdots & b_n \end{matrix}\ ;\ x\right] = \sum_{k\geq 1} \frac{(a_1)_k \cdots (a_{n+1})_k}{(b_1)_k \cdots (b_n)_k} \frac{x^k}{k!}, $$

where $a_0 = 1$ and for $k \geq 1$ $(a)_k = a(a+1)\cdots(a+k-1)$ is called the Pochhammer symbol.

Hypergeometric functions over finite fields were introduced independently by John Greene [25] and Nick Katz [37]. In this paper, we consider Greene's hypergeometric sum, however, note that the two definitions differ only in a normalizing factor for cases related to our discussion.

In this section and throughout this thesis we denote by $\epsilon$ and $\phi$ the trivial and quadratic multiplicative characters of $\mathbb{F}_q$, respectively. Also, we adopt the convention of extending multiplicative characters by declaring them to be zero at $0 \in \mathbb{F}_q$. Let $\gamma_0, \gamma_1, \gamma_2$ be multiplicative characters of $\mathbb{F}_q$ and $x \in \mathbb{F}_q$. Greene defines the following finite field analogue of a hypergeometric sum

$$ {}_2\mathbb{F}_1\left[\begin{matrix}\gamma_0 & \gamma_1 \\ & \gamma_2\end{matrix}; x; q\right] = \epsilon(x)\frac{\gamma_1\gamma_2(-1)}{q}\sum_{y\in\mathbb{F}_q}\gamma_1(y)(\gamma_2\gamma_1^{-1})(1-y)\gamma_0^{-1}(1-xy). \tag{2.2} $$

Since the seminal work of Greene and Katz a lot of work has been done on special functions over finite fields, in particular generalized hypergeometric functions. In this section, we recall some definitions and results that we will use later in this thesis.

Following Greene [25], we introduce other ${}_{n+1}\mathbb{F}_n$ functions inductively as follows. For multiplicative characters $A_0, A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ of $\mathbb{F}_q$ and $x \in \mathbb{F}_q$, define

$$ {}_{n+1}\mathbb{F}_n\left[\begin{matrix}A_0 & A_1 & \cdots & A_n \\ & B_1 & \cdots & B_n\end{matrix}; x; q\right] := $$
$$ \frac{A_nB_n(-1)}{q}\sum_{y\in\mathbb{F}_q} {}_n\mathbb{F}_{n-1}\left[\begin{matrix}A_0 & A_1 & \cdots & A_{n-1} \\ & B_1 & \cdots & B_{n-1}\end{matrix}; y; q\right] A_n(y)\overline{A_n}B_n(1-y) $$

The following lemma is a generalization of Lemma 2.2 in [2].

**Lemma 20.** *For any non-trivial multiplicative character $\gamma$ of $\mathbb{F}_q$,*

$$ q\,{}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix}; 1; q\right] = \sum_{y\in\mathbb{F}_q}\phi(y){}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}; y; q\right] {}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \epsilon\end{matrix}; y; q\right] $$

*Proof.* The lemma follows from the recursive definition of ${}_{n+1}\mathbb{F}_n$. First,

$$q\,{}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix};\,1;q\right] = \phi(-1)\sum_{x\in\mathbb{F}_q^*}\phi(x)\phi(1-x)\,{}_3\mathbb{F}_2\left[\begin{matrix}\gamma & \gamma^{-1} & \phi \\ & \epsilon & \epsilon\end{matrix};\,x;q\right]$$
$$= \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\phi(x)\phi(1-x)\phi(y)\phi(1-y)\,{}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \epsilon\end{matrix};\,xy;q\right].$$

Now replacing $y$ with $y/x$, $x$ with $xy$ and using equation (2.2) we get,

$$q\,{}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix};\,1;q\right] = \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\phi(1-\frac{1}{x})\phi(1-xy)\phi(y)\,{}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \epsilon\end{matrix};\,y;q\right]$$
$$= \sum_{y\in\mathbb{F}_q}\phi(y)\,{}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix};\,y;q\right]\,{}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \epsilon\end{matrix};\,y;q\right].$$

□

Like their classical counterparts hypergeometric functions over finite fields satisfy many transformation formulas [24, 25, **?**]. In particular, the next one will be useful for our purpose.

**Lemma 21.** *(Greene, [25]) For $x \in \mathbb{F}_q$ with $x \neq 0$ we have,*

$${}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix};\,x;q\right] = \phi(x)\,{}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix};\,\frac{1}{x};q\right].$$

### 2.6 Some Related Arithmetic Results

We first introduce some more notation. Let $p$ be an odd prime and $K$ a finite Galois extension of $\mathbb{Q}$ unramified at $p$ and $\mathcal{O}_K$ the ring of algebraic integers of $K$. Then at each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above $p$, the quotient $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_q$ is a finite field extension of $\mathbb{F}_p$ of size $q = p^s$ for some $s \geq 1$. Note that for every $p$ and $s$ it is possible to realize $\mathbb{F}_q$ in this way. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ be the absolute Galois group of $K$. Let $\ell$ be a prime and $\mathbb{Q}_\ell$ be the local $\ell$-adic field. Below, we will use some results in finite dimensional $\ell$-adic Galois representations. A dimension-$m$

representation $\rho$ of $G_K$ is a continuous homomorphism from $G_K$ to $GL_m(L)$ where $L = \mathbb{Q}_\ell$ or an extension of $\mathbb{Q}_\ell$. When such a representation $\rho$ arises from algebraic equations (or varieties), it ramifies at only finitely many prime ideals of $\mathcal{O}_K$. To describe $\rho$ up to semisimplification, it is sufficient to compute all $\rho(\mathrm{Frob}_\mathfrak{p})$ for unramified $\mathfrak{p}$ where $\mathrm{Frob}_\mathfrak{p}$ denotes the (geometric) Frobenius conjugacy class of $G_K$ at $\mathfrak{p}$. ($\mathrm{Frob}_\mathfrak{p}$ is the inverse of the arithmetic Frobenius $\mathrm{Fr}_\mathfrak{p}$, which on the residual field level sends $x$ to $x^{|\mathcal{O}/\mathfrak{p}|}$.) For example, the $\ell$-adic cyclotomic character $\varepsilon_\ell : G_\mathbb{Q} \to \mathbb{Q}_\ell^*$ which is a 1-dimensional representation defined by $\varepsilon_\ell(\mathrm{Fr}_p) = p$ for each prime $p \neq \ell$. For more details, see [54]. An important source of Galois representations arises from modular forms. Instead of giving the precise definition of modular forms which are graded by their weights, we will point out a few things most relevant to our discussion. It is customary to express modular forms as Laurent series in $q = e^{2\pi iz}$ (not to be confused with the prime power $q$). The Dedekind eta function is defined by $\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$. A typical example of modular form is $\Delta(z) = \eta(z)^{24}$. The function $\Delta(z)$ is of weight $k = 12$ and satisfies $\Delta(z+1) = \Delta(z)$. We use $\tau_n$ to denote its $n$th Fourier coefficient. It is known due to Ramanujan and Mordell that for each prime $p$ and natural number $n$, the following recursion holds: $\tau_{np} - \tau_n\tau_p + p^{k-1}\tau_n = 0$. This means $\Delta(z)$ is a Hecke eigenform (and other Hecke eigenforms satisfy similar Hecke recursions). Ramanujan conjectured that $|\tau_p| < 2p^{(12-1)/2} = 2p^{11/2}$ for each prime $p$. Motivated by Ramanujan's observation and based on the pioneering work of Eichler-Shimura, Deligne obtained the following important result. For each integral weight $k \geq 2$ (cuspidal) modular form $f$ with Fourier coefficient $\{a_n(f)\}_{n\geq 1}$ (we assume the character is trivial) and prime $\ell$, there is a 2-dimensional representation $\rho_{\ell,f} : G_\mathbb{Q} \to GL_2(L)$ (where $L$ is the completion of $\mathbb{Q}(a_1(f), a_2(f), \cdots)$ at any place above $\ell$) such that for almost all primes $p$, the characteristic polynomial of $\rho_{\ell,f}(\mathrm{Fr}_p)$ is of the form $T^2 - a_p(f)T + p^{k-1}$ with two eigenvalues, denoted by $\alpha_p, \beta_p$, each having complex absolute value $p^{(k-1)/2}$. Thus $|\mathrm{Tr}\rho_{\ell,f}(\mathrm{Fr}_p)| = |a_p(f)| \leq 2p^{(k-1)/2}$.

To motivate the later discussion, we will review the relation between the hypergeometric function ${}_2F_1\left[\begin{matrix}\frac{1}{2} & \frac{1}{2}\\ & 1\end{matrix}; x\right]$ and its finite field analogues. For each fixed $x \in \mathbb{Q} \setminus \{0,1\}$, the cubic equation $E_x : t^2 = s(s-1)(1-xs)$ in two variables $s,t$ defines an algebraic curve over $\mathbb{Q}$ whose compatification is a genus 1 curve. It is known as an elliptic curve and possesses an abelian group structure as topologically the curve over $\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda_x$ where $\Lambda_x$ is a rank-2 $\mathbb{Z}$-lattice. It has a unique up to scalar holomorphic differential $\omega_x := \frac{ds}{t} = \frac{ds}{\sqrt{s(s-1)(1-xs)}}$ and for $|x| < 1$, $\int_0^1 \omega_x = \pi \cdot {}_2F_1\left[\begin{matrix}\frac{1}{2} & \frac{1}{2}\\ & 1\end{matrix}; x\right]$, see [5]. Let $\ell$ be an auxiliary prime, for any integer $n \geq 1$, the subgroup$E_x[\ell^n]$ of $\ell^n$-division points of $E_x$, is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. As all torsion points of $E_x$ have coordinates in $\overline{\mathbb{Q}}$, the group $G_{\mathbb{Q}}$ acts as group automorphisms on the group $E_x[\ell^n]$. Upon choosing generators of $E_x[\ell^n]$, one has a homomorphism from $G_{\mathbb{Q}}$ to $GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$. As $n$ varies, the division points $E_x[\ell^n]$ vary compatibly using the multiplication by $\ell$ map $[\ell] : E_x[\ell^{n+1}] \to E_x[\ell^n]$. Taking the inverse limit of $E_x[\ell^n]$ and tensoring with $\mathbb{Q}_\ell$, one obtains a representation $\rho_{\ell,E_x} : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_\ell)$. This representation is unramified for almost all primes $p$ and at each unramified prime $p$, $\mathrm{Tr}\rho_{\ell,E_x}(\mathrm{Frob}_p) = p + 1 - \#(E_x/\mathbb{F}_p)$, which is denoted by $a_p(E_x)$. By [47] by Ono, it is known that when $x \neq 0, 1 \mod p$, $a_p(E_x) = -p\,{}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}; x; p\right]$. In other words, there exists a 2-dimensional representation $\rho_{\ell,E_x}$ of $G_{\mathbb{Q}}$ such that for almost all primes $p$,

$$-p\,{}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}; x; p\right] = \mathrm{Tr}\rho_{\ell,E_x}(\mathrm{Frob}_p). \tag{2.3}$$

By the Taniyama-Shimura-Weil conjecture (now a Theorem and it implies the Fermat Last Theorem), there exists a weight-2 Hecke eigenform $f$ such that $\rho_{\ell,E_x}$ is isomorphic $\rho_{\ell,f}^\vee$, the dual of $\rho_{\ell,f}$. Consequently, for almost all primes $p$,

$$\left|p\,{}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi\\ & \epsilon\end{matrix}; x; p\right]\right| = |a_p(E_x)| = |a_p(f)| < 2p^{1/2}.$$

This can be generalized from $\mathbb{F}_p$ to $\mathbb{F}_q$ naturally since if $-p\,{}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\,;\,x;p\right] = \alpha_p + \beta_p$ then $-q\,{}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix}\,;\,x;q\right] = \alpha_p^s + \beta_p^s$, following from the fact that the conjugacy classes $\mathrm{Frob}_{\mathfrak{p}}$ and $\mathrm{Frob}_p^s$ agree, where $|\mathcal{O}_K/\mathfrak{p}| = p^s$.

For other generalized hypergeometric functions, the roles of the elliptic curves $E_x$ are replaced by the so-called hypergeometric motives described in [37, 52]. In [8], Beukers, Cohen and Mellit gave a realization of hypergeometric motives defined over $\mathbb{Q}$ on explicit hypergeometric varieties based on toric varieties. A different way to realize hypergeometric motives over any number field was given in [24]. Following [8], for ${}_4F_3\left[\begin{matrix}\frac{1}{n} & \frac{n-1}{n} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1 & 1\end{matrix}\,;\,1\right]$ with $n = 2,\ 3,\ 4$ or 6, the following varieties can be used to replace the roles of $E_x$ above respectively:

$$\begin{aligned}
W_{2,2,2,2} \quad &: \quad x_1 + x_2 + x_3 = x_4 + x_5 + x_6 = x_7 + x_8 + x_9 = x_{10} + x_{11} + x_{12} = 0 \\
&\qquad 2^8 x_1^2 x_4^2 x_7^2 x_{10}^2 = x_2 x_3 x_5 x_6 x_8 x_9 x_{11} x_{12} \\
W_{2,2,3} \quad &: \quad x_1 + x_2 + x_3 + x_4 = x_5 + x_6 + x_7 = x_8 + x_9 + x_{10} = 0 \\
&\qquad 3^3 2^4 x_1^3 x_5^2 x_8^2 = -x_2 x_3 x_4 x_6 x_2 x_7 x_9 x_{10} \\
W_{2,4} \quad &: \quad x_1 + x_2 + x_3 + x_4 + x_5 = x_6 + x_7 + x_8 = 0 \\
&\qquad 2^{10} x_1^4 x_6^2 = -x_2 x_3 x_4 x_5 x_7 x_8 \\
W_{2,6} \quad &: \quad x_1 + x_2 + x_3 + x_4 + x_5 = x_6 + x_7 + x_8 = 0 \\
&\qquad 3^3 2^8 x_1^6 x_6^2 = x_2^3 x_3 x_4 x_5 x_7 x_8.
\end{aligned}$$

Now we state the needed result from hypergeometric motives due to Katz [37] and Rodriguez-Villegas [52] which is analogous to (2.3) for the $E_x$ case. Let $n = 2, 3, 4, 6$ and assume $K$ contains $\mathbb{Q}(\zeta_n)$, where $\zeta_n$ denotes a primitive $n$th root of unity. This implies $q \equiv 1 \mod n$ and hence $\mathbb{F}_q$ has a primitive order $n$ character $\gamma_{\mathfrak{p}}$.

**Theorem 22** (Katz, Rodriguez-Villegas)**.** *Notation as above. Let $n = 2, 3, 4,$ or 6 and assume $K$ contains $\mathbb{Q}(\zeta_n)$ and $\ell$ be any fixed prime. There exists a 3-dimensional*

*continuous representation* $\sigma_{\ell,n} : G_{\mathbb{Q}(\zeta_n)} \to GL_3(\mathbb{Q}_\ell(\zeta_n))$ *such that at each prime ideal* $\mathfrak{p}$ *coprime to* $2n \cdot \ell$ *and the discriminant of* $K$ *with residue field size* $q$*,*

$$-q^3 \cdot {}_4\mathbb{F}_3 \left[ \begin{matrix} \gamma_\mathfrak{p} & \gamma_\mathfrak{p}^{-1} & \phi & \phi \\ & & \epsilon & \epsilon \end{matrix} \epsilon \; ; \; 1; q \right] = Tr\, \sigma_{\ell,n}(Frob_\mathfrak{p})$$

*where* $\gamma_\mathfrak{p}$ *denotes any primitive order* $n$ *character of* $\mathbb{F}_q$*. Moreover,* $\sigma_{\ell,n}$ *is isomorphic to a direct sum of* $\rho_{\ell,n,1}$ *and* $\rho_{\ell,n,2}$ *of* $G_{\mathbb{Q}(\zeta_n)}$ *with dimension 2 and 1 respectively. The characteristic polynomial of* $\rho_{\ell,n,1}(Frob_\mathfrak{p})$ *(resp.* $\rho_{\ell,n,2}(Frob_\mathfrak{p})$*) is a degree-2 (resp. 1) polynomial whose coefficients are in* $\mathbb{Z}[\zeta_n]$ *and with each roots of complex absolute value* $q^{3/2}$ *(resp.* $q$*).*

Here, we give some idea on how to obtain it explicitly from numeric data. In [37], Katz described $\ell$-adic representations $\sigma_{\ell,n}$ of $G_\mathbb{Q}$ associated with the given sets of hypergeometric data, which are $\{\frac{1}{n}, \frac{n-1}{n}, \frac{1}{2}, \frac{1}{2}\}$ and $\{1,1,1,1\}$. Here we only consider the semisimplification of $\sigma_{\ell,n}$. The corresponding character sums, up to normalizing factors agree with $q^3 \cdot {}_4\mathbb{F}_3 \left[ \begin{matrix} \gamma_\mathfrak{p} & \gamma_\mathfrak{p}^{-1} & \phi & \phi \\ & & \epsilon & \epsilon \end{matrix} \epsilon \; ; \; 1; q \right]$. The dimension of the representation, is determined by the local zeta functions defined by

$$\exp\left( \sum_{s=1}^{\infty} q^{3s} \cdot {}_4\mathbb{F}_3 \left[ \begin{matrix} \gamma_\mathfrak{p} & \gamma_\mathfrak{p}^{-1} & \phi & \phi \\ & & \epsilon & \epsilon \end{matrix} \epsilon \; ; \; 1; q^s \right] T^s/s \right).$$

By Dwork, these zeta functions are rational functions in $T$ of the same degree for generic $\mathfrak{p}$. In these cases, they are degree-3 polynomials from which we know $\sigma_{\ell,n}$ is 3-dimensional. Also data reveal that for $\mathfrak{p}$ coprime to $2n\ell$ the characteristic polynomial of $\sigma_{\ell,n}(\mathrm{Frob}_\mathfrak{p})$ has three roots, two of them of absolute value $q^{3/2}$ and one has absolute value $q$. For the claimed decomposition of $\sigma_{\ell,n}$, the existence of $\rho_{\ell,n,1}$ is shown in the next proof.

**Proposition 23.** *Notation as the above theorem. For each* $n = 2, 3, 4$ *or* $6$*, there is weight-4 Hecke cuspidal eigenforms* $f_n$ *which gives rise to a 2-dimensional Galois representation* $\rho_{\ell,f_n}$ *of* $G_\mathbb{Q}$ *such that* $\rho_{\ell,n,1} \cong \rho^\vee_{\ell,f_n}|_{G_{\mathbb{Q}(\zeta_n)}}$*, the restriction of* $\rho^\vee_{\ell,f_n}$ *to* $G_{\mathbb{Q}(\zeta_n)}$*;*

*$\rho_{\ell,n,2}$ is isomorphic to $\varepsilon_\ell^{-1}|_{G_{\mathbb{Q}(\zeta_n)}} \otimes \chi_{d_n}$ where $\varepsilon_\ell$ denotes the $\ell$-adic cyclotomic character and $d_n = -1, -3, -1, 2$ for $d = 2, 3, 4, 6$ respectively and $\chi_{d_n}$ notes the character of $G_{\mathbb{Q}(\zeta_n)}$ with kernel $G_{\mathbb{Q}(\sqrt{d_n},\zeta_n)}$. Consequently,*

$$\left| q^3 \cdot {}_4\mathbb{F}_3 \left[ \begin{matrix} \gamma_{\mathfrak{p}} & \gamma_{\mathfrak{p}}^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon \end{matrix} ; 1; q \right] + \phi(-1)\gamma_n(-1)q \right| \leq 2q^{3/2}.$$

The final conclusion is a generalization of Theorem 2 in [2].

*Proof.* We first determine $\rho_{\ell,n,1}$ geometrically and then $\rho_{\ell,n,2}$.

Note that it is possible to realize the Galois representations $\sigma_{\ell,n}$ as Galois representations arising from étale cohomology groups of algebraic varieties $W_n$. Using the recipe of [8], the $W_n$ is computed as $W_{2,2,2,2}$, $W_{2,2,3}, W_{2,4}, W_{2,6}$ for $n = 2, 3, 4, 6$ respectively. According to [7] by Batyev and van Straten, the smooth model of each $W_n$ is a rigid Calabi-Yau threefold defined over $\mathbb{Q}$. (Calabi-Yau three-folds are higher analogues of elliptic curves which play important role in String theory. A Calabi-Yau threefold is said to be rigid if its $h^{2,1}$ Hodge number equals 0.) The construction of [8] implies that Galois representation of $G_{\mathbb{Q}(\zeta_n)}$ arising from the third étale cohomology of $W_n$, which is 2-dimensional $\rho_{\ell,W_n}$, is isomorphic to a subrepresentation of $\sigma_{\ell,n}$. In [28], Gouvea and Yui showed that each $\rho_{\ell,W_n}$ is modular in the sense that it is isomorphic to the dual of a 2-dimensional $\ell$-adic Deligne representation associated to an explicit weight-4 cuspidal Hecke eigenform $f_n$. Knowing these modular forms explicitly allows us to compute the values of the traces of $\rho_{\ell,n,1}(\mathrm{Frob}_p)$, which agree with the $p$th Fourier coefficients $a_p(f_n)$ of $f_n$ for primes $p$ coprime to $2n\ell$. For each $W_n$, the restriction of the Deligne representations associated with $f_n$ to $G_{\mathbb{Q}(\zeta_n)}$ will be $\rho_{\ell,n,1}$. In [55], van Geemen and Nygaard showed that $f_2 = \eta(2z)^4\eta(4z)^4$ where $\eta(z)$, is the Dedekind eta function introduced before. (The same result for a different algebraic model of $W_2$ was obtained in [56] by Verrill and in [2] by Ahlgren and Ono.) Similarly $f_4 = \frac{\eta(4z)^{16}}{\eta(2z)^4\eta(8z)^4}$. Also $f_3$ (resp. $f_6$) corresponds to the Hecke eigenform labelled by 36.4.1.a (resp. 72.4.1.b) in the LMFDB database [40] respectively. See also [51, 59] for related discussions.

Now we turn our attention to $\rho_{\ell,n,2}$. Firstly, by Theorem 22

$$\rho_{\ell,n,2}(\mathrm{Frob}_p) = -p^3 \cdot {}_4\mathbb{F}_3 \left[ \begin{matrix} \gamma_{\mathfrak{p}} & \gamma_{\mathfrak{p}}^{-1} & \phi & \phi \\ & & & \end{matrix} ; \; 1; p \right] - a_p(f_n)$$

for $p \equiv 1 \mod n$ from which we observe that $\rho_{\ell,n,2}(\mathrm{Frob}_p) \in \mathbb{Z}$ as both the finite hypergeometric sums and $a_p(f_n)$'s are integers. Also $\rho_{\ell,n,2}$ is the restriction of a Galois representation of $G_{\mathbb{Q}}$ restricted to $G_{\mathbb{Q}(\zeta_n)}$, as each $W_n$ is defined over $\mathbb{Q}$. Combining with Theorem 22, we know $\rho_{\ell,n,2}$ is isomorphic to $\varepsilon^{-1}|_{G_{\mathbb{Q}(\zeta_n)}}$ tensoring another character $\chi_{d_n}$ which has order at most 2. By its construction, $\sigma_{\ell,n}$ is unramified outside of $2n\ell$, so $\rho_{\ell,n,2}$ is also. Knowing the ramification allows us to nail down the possibilities for the character $\chi_{d_n}$ readily.

Note that the final conclusion of the proposition is a direct consequence of the previous ones. □

### 2.7 The Vector Space $\ell^2(\mathbb{F}_q, m)$

Let $m : \mathbb{F}_q \to \mathbb{C}$ be $m(x) = 1 + qD_1(x) + qD_{-1}(x)$ where $D_a(x)$ is 1 if $x = a$ and 0 otherwise. We denote by $\ell^2(\mathbb{F}_q, m)$ the vector space of complex-valued functions on $\mathbb{F}_q$ equipped with the Hermitian form

$$\langle f_1, f_2 \rangle_{\ell^2} = \sum_{x \in \mathbb{F}_q} f_1(x)\overline{f_2(x)}m(x).$$

Note that the following character sums are elements of $\ell^2(\mathbb{F}_q, m)$.

**Definition 24.** For any multiplicative character $\gamma$ of $\mathbb{F}_q$, the *Legendre sum* with respect to $\gamma$ is defined as

$$P_\gamma(a) = \frac{1}{q} \sum_{x \in \mathbb{F}_q^*} \gamma(x)\phi(x^2 - 2ax + 1), \quad \text{for all } a \in \mathbb{F}_q.$$

**Definition 25.** For any multiplicative character $\beta$ of $\mathbb{F}_{q^2}$, the *Soto-Andrade sum* with respect to $\beta$ is defined as

$$R_\beta(a) = \frac{1}{q(q-1)} \sum_{r \in \mathbb{F}_{q^2}^*} \beta(r)\phi((r + r^q)^2 - 2(a+1)r^{1+q}), \quad \text{for all } a \in \mathbb{F}_q.$$

The Legendre and Soto-Andrade sums have appeared several times in the literature in connection with the irreducible representations of $PGL(2,q)$ [34]. In fact, we will encounter them in Section 4 in our study of some character sums over $PGL(2,q)$. In this section, we recall some properties of these sums that will be useful for us in the coming sections.

The next lemma shows that the Legendre and Soto-Andrade sums form an orthogonal basis of $\ell^2(\mathbb{F}_q, m)$.

**Lemma 26.** *(Kable, [34]) The set*

$$\mathfrak{L} = \left\{ P_\epsilon - \frac{q-1}{q}, P_\phi, P_\gamma, R_\beta : \ \gamma \in A, \beta \in B \right\}$$

*is an orthogonal basis for the space $\ell^2(\mathbb{F}_q, m)$, where $A$ and $B$ are the sets introduced in Definition 19 with $|A| = \frac{q-3}{2}$ and $|B| = \frac{q-1}{2}$. The square norm of the elements of this basis are as follows:*

$$\begin{aligned} \left\| P_\epsilon - \frac{q-1}{q} \right\|_{\ell^2}^2 &= \frac{q^2-1}{q}, \\ \|P_\phi\|_{\ell^2}^2 &= \frac{q^2-1}{q^2}, \\ \|P_\gamma\|_{\ell^2}^2 &= \frac{q-1}{q}, \\ \|R_\beta\|_{\ell^2}^2 &= \frac{q+1}{q}. \end{aligned}$$

If we normalize the basis given by Lemma 26 then we can easily obtain an orthonormal basis of $\ell^2(\mathbb{F}_q, m)$. We denote the elements of this orthonormal basis by $\{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \ \gamma \in A, \beta \in B\}$.

The next lemmas list some elementary properties of the Legendre and Soto-Andrade sums that we will need later. Lemma 27 implies that the Legendre sum with respect to the trivial character is easy to evaluate. This is not true for Legendre sums with respect to characters of higher orders. On the other hand, Lemma 28 shows that the Legendre and Soto-Andrade sums are easy to evaluate at $\pm 1$. Lemma 29 implies that the values of these sums are real numbers.

**Lemma 27.** *The values of the Legendre sum with respect to $\epsilon$ are,*

$$P_\epsilon(a) = \begin{cases} \frac{q-2}{q}, & \text{if } a = \pm 1, \\ -\frac{2}{q}, & \text{if } a \neq \pm 1. \end{cases}$$

**Lemma 28.** *Let $\gamma$ and $\beta$ be characters from the sets $A$ and $B$, respectively. Then $P_\gamma(1) = -1/q$ and $R_\beta(1) = 1/q$. Moreover,*

$$P_\gamma(-1) = -\frac{\gamma(-1)}{q}, \quad R_\beta(-1) = -\frac{\beta(i)}{q}$$

*where $i \in \mathbb{F}_{q^2}^*$ satisfies that $i^2 \in \mathbb{F}_q^*$.*

**Lemma 29.** *For every $\gamma \in A$, $\beta \in B$ and $a \in \mathbb{F}_q$ we have*

$$P_{\gamma^{-1}}(a) = P_\gamma(a) \quad \text{and} \quad R_{\beta^{-1}}(a) = R_\beta(a).$$

The following result establish a relation between Legendre sums and hypergeometric sums over finite fields. This fact will be crucial later in this paper.

**Lemma 30.** *(Kable, [34]) If $\gamma$ is a nontrivial character of $\mathbb{F}_q$ and $a \in \mathbb{F}_q \setminus \{\pm 1\}$ then*

$$P_\gamma(a) = {}_2\mathbb{F}_1 \left[ \begin{matrix} \gamma & \gamma^{-1} \\ & \epsilon \end{matrix} ; \frac{1-a}{2}; q \right].$$

# Chapter 3

# ERDÖS-KO-RADO PROBLEMS

In this chapter we introduce EKR-problems for permutation groups. Furthermore, we give a brief review of some techniques that have been used to solve these problems.

Let $X$ be a finite set and $G$ a finite group acting on $X$. A subset $S$ of $G$ is said to be an *intersecting family* if for every $g_1, g_2 \in S$ there exists an element $x \in X$ such that $x^{g_1} = x^{g_2}$. Like in the original EKR-problem, we call intersecting families of maximum size *extremal families*. Moreover, intersecting families whose sizes are close to the maximum are called *almost extremal families*.

The following problems about intersecting families in $G$ are considered to be the basic problems in EKR theory.

I (Upper Bound) What is the maximum size of an intersecting family?

II (Characterization) What is the structure of extremal families?

III (Stability) Are almost extremal families similar in structure to the extremal ones?

The above three problems were solved for the symmetric group $S_n$. Indeed, Deza and Frankl [21] proved that the maximum size of an intersecting family in $S_n$ is $(n-1)!$. Moreover, they conjectured that the cosets of points stabilizers are the only extremal families. This conjecture turned out to be rather harder to prove than one might expect. It was first proved by Cameron and Ku [11], and independently by Larose and Malvenuto [41]. Finally, the stability of extremal families in $S_n$ was settled by Ellis [14], who proved that for any $\epsilon > 0$ and $n > N(\epsilon)$, any intersecting family of size at least $(1 - 1/e + \epsilon)(n-1)!$ must be strictly contained in an extremal family.

In [45], Meagher and Spiga studied Problems I and II for the group $PGL(2,q)$ acting on the set of points of the projective line $PG(1,q)$. These authors proved that the maximum size of an intersecting family in $PGL(2,q)$ is $q(q-1)$. Furthermore, they also solved the characterization problem: Every intersecting family of maximum size in $PGL(2,q)$ is a coset of a point stabilizer. In [46], they went one step further to solve Problems I and II for the group $PGL(3,q)$ acting on the points of the projective plane $PG(2,q)$.

In the next sections we go over some techniques to solve these EKR-problems for permutation groups.

### 3.1 The Eigenvalue Method

The eigenvalue method has been used several times to get upper bounds on the size of intersecting families for EKR-type problems. The first step of the method is to reformulate the problem in graph theory terminology. Indeed, the problem of finding the maximum size of an intersecting family in a group $G$ is equivalent to the problem of finding the maximum size of an independent set in a certain graph. Then, we can apply a classical result in spectral graph theory, known as Hoffman's bound, to get an upper bound on the size of an independent set. The following variant of Hoffman's theorem will be enough for the purposes of this thesis.

**Theorem 31.** *(Hoffman's bound, [43]) Let $\Gamma$ be a $k$-regular, $n$-vertex graph. Let $A$ be the adjacency matrix of $\Gamma$ and let $\lambda_{min}$ be the minimum eigenvalue of $A$. If $S$ is an independent set in $\Gamma$, then*

$$\frac{|S|}{n} \leq \frac{-\lambda_{\min}}{k-\lambda_{\min}}.$$

*If equality holds then the characteristic function $1_S$ of $S$ satisfies:*

$$1_S \in V_1 \oplus V_{\lambda_{\min}}$$

*where $V_1$ is the vector space spanned by the all-ones vector and $V_{\lambda_{\min}}$ is the $\lambda_{\min}$-eigenspace.*

To associate every intersecting family in $G$ with an independent set of a graph, we introduce the notion of Cayley graph.

**Definition 32.** Let $Y$ be an inverse-closed subset of $G$. The Cayley graph on $G$ generated by $Y$ is the graph with vertex set $G$ such that there is an edge between $g_1, g_2 \in G$ if and only if $g_1 g_2^{-1} \in Y$. We denote this graph by $Cay(G, Y)$.

Recall that an element $g \in G$ is a derangement if for any $x \in X$ we have that $x \neq x^g$. Denote by $D$ the set of derangements in $G$. We define $\Gamma$ as the Cayley graph on $G$ with generating set $D$. This graph is known as the derangement graph of $G$. Note that every independent set in $\Gamma$ corresponds to an intersecting family in $G$. Hence, an upper bound on the size of independent sets in $\Gamma$ is also an upper bound on the size of intersecting families in $G$.

To apply Hoffman's bound, we need to compute the eigenvalues of $\Gamma$. Note that the set of derangements $D$ is a union of conjugacy classes and inverse-closed. A result of Babai and Diaconis-Shahshahani shows that under these conditions the eigenvalues of $\Gamma$ are closely related to the irreducible characters of $G$.

**Lemma 33.** *(Babai [6], Diaconis-Shahshahani [12]) Let $G$ be a finite group, and let $R$ be a complete set of irreducible representations of $G$. Let $Y \subset G$ be inverse-closed and conjugation invariant, and let $Cay(G, Y)$ be the Cayley graph on $G$ with generating set $Y$. For every $\rho \in R$, the vector subspace $\widehat{V}_{\chi_\rho}$ of $\mathbb{C}[G]$ is an eigenspace of $Cay(G, Y)$ with eigenvalue*

$$\frac{1}{\chi_\rho(1)} \sum_{y \in Y} \chi_\rho(y),$$

*where $\chi_\rho$ is the irreducible character of $\rho$. Moreover, if $\lambda$ is an eigenvalue of $Cay(G, Y)$ corresponding to the irreducible representations $\{\rho_1, \ldots, \rho_s\} \subset R$ then the dimension of the $\lambda$-eigenspace is $\sum_{i=1}^{s} \chi_{\rho_i}(1)^2$.*

Since $\Gamma$ satisfies the conditions of Lemma 33, we conclude that to compute the eigenvalues of $\Gamma$ we just need to evaluate the character sum $\frac{1}{\chi(1)} \sum_{x \in D_q} \chi(x)$ for every irreducible character $\chi$ of $G$.

For example, consider the natural right action of $PGL(2,q)$ on $PG(1,q)$. Meagher and Spiga [45] applied the eigenvalue method to find an upper bound on the size of intersecting families in $PGL(2,q)$. First, using the character table of $PGL(2,q)$ (Table 2.1) and Lemma 33, it is possible to compute the eigenvalues of the graph $\Gamma = Cay(PGL(2,q), D_q)$ for every $q$ where $D_q$ is the set of derangements of $PGL(2,q)$.

| q even | $\lambda_1$ | $\psi_1$ | $\eta_\beta$ | $\nu_\gamma$ |
|---|---|---|---|---|
| eigenvalues | $\frac{q^2(q-1)}{2}$ | $-\frac{q(q-1)}{2}$ | $q$ | 0 |

| q odd | $\lambda_1$ | $\lambda_{-1}$ | $\psi_1$ | $\psi_{-1}$ | $\eta_\beta$ | $\nu_\gamma$ |
|---|---|---|---|---|---|---|
| eigenvalues | $\frac{q^2(q-1)}{2}$ | $-\frac{q(q-1)}{2}$ | $-\frac{q(q-1)}{2}$ | $\frac{q-1}{2}$ | $q$ | 0 |

Note that when $q$ is even the smallest eigenvalue arises only from $\psi_1$ which is the standard character of $PGL(2,q)$. Moreover, when $q$ is odd the smallest eigenvalue arises from $\psi_1$ and $\lambda_{-1}$.

Now it follows from Hoffman's bound that the maximum size of an intersecting family in $PGL(2,q)$ is $q(q-1)$. Since the cosets of point stabilizers in $PGL(2,q)$ are intersecting families of size $q(q-1)$ this implies that the upper bound is tight. Thus, intersecting families of maximum size in $PGL(2,q)$ contain exactly $q(q-1)$ elements.

### 3.2 The Module Method

The module method developed by Ahmadi and Meagher [4] is a technique to characterize intersecting families of maximum size in a 2-transitive group $G$ acting on a set $X$. As was remarked at the Introduction, the main ingredient of this method is the computation of the rank of the derangement matrix $M$ of $G$ (see Definition 6). In this section, we briefly explain the main steps of the module method.

For every $x, y \in X$, we denote by $T_{x,y}$ the coset of a point stabilizer sending $x$ to $y$. Note that because $G$ is 2-transitive it is easy to conclude that $|T_{x,y}| = |G|/|X|$. Furthermore, $T_{x,y}$ is an intersecting family for every $x, y \in X$.

We say that $G$ has the EKR property, if the size of any intersecting subset of $G$ is bounded above by the size of a point stabilizer in $G$. Further, $G$ is said to have the

strict EKR property if the only maximum intersecting subsets of $G$ are cosets of the point stabilizers. The module method can be used to prove that a 2-transitive group has the strict EKR property.

The standard character $\chi_{std}$ is an irreducible character for any 2-transitive group (see Section 2.2). Therefore, the vector space $\mathbb{C}[G]$ can be decomposed as

$$\mathbb{C}[G] = \widehat{V}_1 \oplus \widehat{V}_{\chi_{std}} \oplus \bigoplus_{\chi} \widehat{V}_{\chi}$$

where $\widehat{V}_1$, $\widehat{V}_{\chi_{std}}$ are the vector subspaces of complex-valued functions on $G$ whose Fourier transform has support on the trivial and the standard representation, respectively, and $\chi$ runs over all irreducible characters of $G$ except for the trivial and standard ones.

Let $1_{T_{x,y}}$ be the characteristic vector of $T_{x,y}$. It was proved in [4] that $1_{T_{x,y}}$ lies in $\widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$ for any $x, y \in X$. In fact a stronger result was proven.

**Lemma 34.** *(Ahmadi and Meagher, [4]) The vectors* $\{1_{T_{x,y}} : x, y \in X\}$ *form a spanning set for* $\widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$.

Let $\Gamma$ be the derangement graph associated with the action of $G$ on $X$ and $D$ the set of derangements in $G$. It follows from Lemma 33 that $-\frac{|D|}{|X|-1}$ is an eigenvalue of $\Gamma$ because

$$\frac{1}{\chi_{std}(1_G)} \sum_{g \in D} \chi_{std}(g) = -\frac{|D|}{|X| - 1},$$

where $1_G$ is the identity of $G$. Now, if $-\frac{|D|}{|X|-1}$ corresponds to the smallest eigenvalue of $\Gamma$ then Hoffman's bound implies that the maximum size of an intersecting family is $|G|/|X|$. Therefore, if the eigenvalue arising from the standard character is the smallest then the cosets of points stabilizers are intersecting families of maximum size.

Now, we are ready to state the module method.

**Theorem 35.** *(Ahmadi and Meagher, [4]) Let $G$ be a 2-transitive group acting on $X$. Assume the following conditions hold:*

1. *the maximum size of an intersecting family in $G$ is $|G|/|X|$,*

2. *the characteristic vector of any intersecting family of maximum size lie in the vector subspace* $\widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$ *of* $\mathbb{C}[G]$.,

3. *the rank of the derangement matrix* $M$ *of* $G$ *is* $(|X|-1)(|X|-2)$,

*then* $G$ *has the strict EKR property.*

If a group $G$ acting on $X$ satisfies conditions 1 and 2 then the module method reduces the problem of characterizing intersecting families of maximum size in $G$ to the computation of the rank of $M$. In particular, if the rank of the derangement matrix $M$ is $(|X|-1)(|X|-2)$ then the only intersecting families of maximum size are the cosets of point stabilizers.

The module method has been applied to characterize intersecting families of maximum size for the symmetric group, the alternating group, $PGL(2,q)$, Mathieu groups, etc. Moreover, as was remarked at the Introduction we will apply this method to characterize extremal families in $PSL(2,q)$.

For example, let's apply the module method to prove that the cosets of points stabilizers are the only extremal families in $PGL(2,q)$. From the previous section we already know that the maximum size of an intersecting family in $PGL(2,q)$ is $q(q-1)$. Therefore, the cosets of point stabilizers in $PGL(2,q)$ are extremal families and $PGL(2,q)$ has the EKR property. Moreover, Hoffman's bound gives information about the characteristic function of any extremal family. Indeed, if $S$ is an intersecting family of maximum size then its characteristic function $1_S$ is contained in $\widehat{V}_{\lambda_1} \oplus \widehat{V}_{\psi_1}$ when $q$ is even, and in $\widehat{V}_{\lambda_1} \oplus \widehat{V}_{\psi_1} \oplus \widehat{V}_{\lambda_{-1}}$ when $q$ is odd. In the next lemma, we show that it is possible to improve this result in the case when $q$ is odd.

**Lemma 36.** *Let* $q$ *be odd. Let* $S \subset PGL(2,q)$ *be an intersecting family of size* $q(q-1)$ *and denote by* $1_S$ *its characteristic function. Then*

$$1_S \in \widehat{V}_{\lambda_1} \oplus \widehat{V}_{\psi_1}.$$

To prove Lemma 36, we will need the following result proved by Meagher and Spiga in [45].

**Lemma 37.** *(Meagher and Spiga, [45]) Consider the natural right action of $PSL(2,q)$ on the projective points of $PG(1,q)$. Let $D_{PSL}$ be the set of derangements of $PSL(2,q)$. Every independent set of maximum size in $Cay(PSL(2,q), D_{PSL})$ has size $q(q-1)/2$.*

*Proof of Lemma 36.* We already know that $1_S \in \widehat{V}_{\lambda_1} \oplus \widehat{V}_{\psi_1} \oplus \widehat{V}_{\lambda_{-1}}$. The vector space $\widehat{V}_{\lambda_{-1}}$ is one dimensional so $\widehat{V}_{\lambda_{-1}} = \text{span}_{\mathbb{C}}\{\lambda_{-1}\}$. Hence, it is enough to show that $\langle 1_S, \lambda_{-1}\rangle = 0$.

Recall that $PSL(2,q)$ is a subgroup of $G_q$. The irreducible character $\lambda_{-1}$ is a function on $G_q$ such that $\lambda_{-1}(g) = 1$ if $g \in PSL(2,q)$ and $-1$, otherwise. Therefore, $\langle 1_S, \lambda_{-1}\rangle = 0$ if and only if exactly half of the elements in $S$ are in $PSL(2,q)$.

From Lemma 37 it follows that he maximum size of an intersecting family in $PSL(2,q)$ is $q(q-1)/2$. Therefore, at most $q(q-1)/2$ elements of $S$ are contained in $PSL(2,q)$.

Since $PSL(2,q)$ is a subgroup of index 2, there exists $g' \in G_q$ such that $G_q = g'PSL(2,q) \cup PSL(2,q)$. Assume to the contrary, that more than $q(q-1)/2$ elements of $S$ are contained in $g'PSL(2,q)$. If we multiply each of these elements by $g'$ then we get an intersecting family in $PSL(2,q)$. This is a contradiction because the maximum size of an intersecting family in $PSL(2,q)$ is $q(q-1)/2$. Therefore, exactly half of the elements in $S$ are contained in $PSL(2,q)$. □

From Lemma 36 we conclude that the action of $PGL(2,q)$ on $PG(1,q)$ satisfies conditions 1 and 2 of Theorem 35 because $\psi_1$ is the standard character of $PGL(2,q)$. Thus, to prove that $PGL(2,q)$ has the strict EKR property is enough to show that the derangement matrix $M$ of $PGL(2,q)$ acting on $PG(1,q)$ has rank $q(q-1)$. For details about the computation of the rank of $M$ see [45].

### 3.3 The Fourier Analysis Method

The Fourier analysis method has been used in the area of analysis of Boolean functions with great success in recent years [1, 22, 31]. The main idea is very simple: study the Fourier transform of a Boolean function to conclude something about its

structure. Indeed, given a group $G$ and a Boolean function $f \in \mathbb{C}[G]$, if we know that the Fourier transform of $f$ is highly concentrated on some subset of the irreducible representations of $G$ then, what can we say about the structure of $f$?

It turns out that the Fourier analysis method can be used to solve EKR stability problems. Let $G$ be a group acting on a set $X$ and $V_{\lambda_{\min}}$ the eigenspace corresponding to the smallest eigenvalue of the derangement graph of $G$. The spectral method consists on two steps:

1. Fourier characterization: Prove that the Fourier transform of the characteristic function of every intersecting family in $G$ whose size is close enough to the maximum is highly concentrated on $V_1 \oplus V_{\lambda_{\min}}$.

2. Structural characterization: Prove that the structure of Boolean functions whose Fourier transforms are highly concentrated on $V_1 \oplus V_{\lambda_{\min}}$ is similar to the structure of Boolean functions whose Fourier transforms are completely supported on $V_1 \oplus V_{\lambda_{\min}}$.

For example, in [16] Ellis, Filmus and Friedgut applied the Fourier analysis method to solve the stability problem for intersecting families in the symmetric group $S_n$. We describe the main steps of their work.

Consider the natural action of $S_n$ on $[n]$. As was remarked earlier, Deza and Frankl [21] proved that the maximum size of an intersecting family in $S_n$ is $(n-1)!$. Moreover, the cosets of points stabilizers are the only extremal families (this was first proved by Cameron and Ku [11], and independently by Larose and Malvenuto [41]).

Let $\Gamma_n$ be the derangement graph of $S_n$ acting on $[n]$. For any $i, j \in [n]$ we denote by $T_{i,j}$ the coset of a point stabilizer sending $i$ to $j$. It follows from Hoffman's theorem that the characteristic function $1_{T_{i,j}}$ of any coset of a point stabilizer lies in the subspace $V_1 \oplus V_{\min}$, where $V_{\min}$ is the eigenspace associated with the smallest eigenvalue of $\Gamma_n$.

The following lemma is known as the *stability version* of Hoffman's bound.

**Lemma 38.** *(Ellis, [13]) Let $\Gamma$ be a $k$-regular, $n$-vertex graph with eigenvalues $k = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n = \lambda_{\min}$. Let $K = \max\{i : \lambda_i > \lambda_{\min}\}$. Let $S$ be an independent set in $\Gamma$. We denote by $U$ the direct sum of the subspaces $V_1$ and $V_{\min}$, where $V_1$ is the subspace spanned by the all 1's vector and $V_{\min}$ is the eigenspace associated with the $\lambda_{\min}$ eigenvalue. Let $P_U$ denote orthogonal projection onto $U$. Then*

$$\|1_S - P_U(1_S)\|^2 = \frac{1}{n}\sum_{v\in v(\Gamma)} |1_S(v) - P_U(1_S)(v)|^2 \leq \frac{(1-\alpha)|\lambda_{\min}| - k\alpha}{|\lambda_{\min}| - |\lambda_K|}\alpha$$

*where $\alpha = |S|/n$.*

Note that we can apply Lemma 38 to solve the Fourier characterization step of the spectral method. To do this we need to know the spectrum of the derangement graph $\Gamma_n$. This task was accomplished in [50] by Renteln. This author proved that the minimum eigenvalue $\lambda_{\min}$ of $\Gamma_n$ arises only from the standard character $\chi_{std}$ and is equal to $-d_n/(n-1)$, where $d_n$ is the number of derangements in $S_n$. Furthermore, from his work it is also possible to conclude that $\lambda_K = O(d_n/n^2)$, where $K$ is the integer defined in the statement of Lemma 38. Also, note that applying the principle of inclusion-exclusion we get that $d_n = n!(1/e + o(1))$.

Now, let $S$ be an intersecting family in $S_n$ such that $|S| = \alpha n!$. Using Lemma 38 we conclude that

$$\|1_S - P_U(1_S)\|_{S_n}^2 \leq (1-\alpha n)(1+O(1/n))\alpha \tag{3.1}$$

where $U = \widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$.

Since we know that the maximum size of an intersecting family in $S_n$ is $(n-1)!$ then $\alpha \leq 1/n$. If the value of $\alpha$ is close to $1/n$ then $S$ is an intersecting family whose size is close to the maximum. On the other hand, Equation 3.1 implies that if $\alpha$ is close to $1/n$ then the Fourier transform of $1_S$ is highly concentrated on the trivial and standard representation. Therefore, the characteristic function of every intersecting family in $S_n$ whose size is close enough to $(n-1)!$ is highly concentrated on $U$.

The second step of the Fourier analysis method requires to study the structure of Boolean functions whose Fourier transforms are highly concentrated on some irreducible representations. For this particular case we need to study Boolean functions in $\mathbb{C}[S_n]$ whose Fourier transforms are highly concentrated on the trivial and standard representation. The following remarkably theorem deals with the characterization of these Boolean functions.

**Theorem 39.** *(Ellis, Filmus and Friedgut, [16]) There exists absolute constants $C_0, \epsilon_0 > 0$ such that the following holds. Let $S \subset S_n$, with $|S| = \alpha n!$, where $\alpha < 1/n$, and let $1_S \in \mathbb{C}[S_n]$ be the characteristic function of $S$, so that $\|1_S\|_{S_n}^2 = \alpha$. Let $P_U(1_S)$ denote the orthogonal projection of $1_S$ onto $U = \widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$. If $\|1_S - P_U(1_S)\|_{S_n}^2 \leq \epsilon\alpha$, where $\epsilon \leq \epsilon_0$, then there exists $i, j \in [n]$ such that*

$$\|1_S - T_{i,j}\|_{S_n}^2 \leq C_0(\epsilon^{1/2} + 1/n)/n.$$

In fact, Theorem 39 is a particular case of a more general theorem proved by the authors in [16]. Theorem 39 proves that every Boolean function with squared norm less than $1/n$ and whose Fourier transform is highly concentrated in $U$ is close in structure to a coset of a point stabilizer. Since the characteristic function of every intersecting family whose size is close to $(n-1)!$ has squared norm less than $1/n$ and a Fourier transform concentrated in $U$, the stability result follows from Theorem 39.

# Chapter 4

## STABILITY FOR INTERSECTING FAMILIES IN $PGL(2,q)$

In [45], Meagher and Spiga proved that the maximum size of an intersecting family in $PGL(2,q)$ is $q(q-1)$. Furthermore, they also solved the characterization problem: Every extremal family in $PGL(2,q)$ is a coset of a point stabilizer. In this thesis we prove that extremal families in $PGL(2,q)$ are also stable, that is, an almost extremal family in $PGL(2,q)$ must be close in structure to a coset of a point stabilizer[1]. We make this statement explicit in the following theorem.

**Theorem 40.** *There exists an absolute constant $C_0$ such that the following holds. Let $S \subset PGL(2,q)$ be an intersecting family with $|S| = (1-\delta)q(q-1)$, where $0 \leq \delta \leq 1/2$. Then there exists a coset of a point stabilizer $T \subset PGL(2,q)$ such that*

$$|S \triangle T| \leq C_0 \left(\delta^{1/2} + \frac{1}{q+1}\right)|S|,$$

*where $\triangle$ is the symmetric difference of sets.*

Using Theorem 40 and some properties of intersecting families in $PGL(2,q)$ we get the following stronger result on almost extremal families in $PGL(2,q)$.

**Theorem 41.** *There exists an absolute constant $\delta_0 > 0$ such that the following holds. If $S \subset PGL(2,q)$ is an intersecting family with $|S| \geq (1-\delta_0)q(q-1)$, then $S$ is contained within a coset of a point stabilizer in $PGL(2,q)$.*

Theorem 41 is a direct analogue of the Cameron-Ku conjecture proved by Ellis in [14].

---

[1] A point stabilizer in $PGL(2,q)$ is a subgroup that fixes a particular element of $PG(1,q)$.

The proof of Theorem 40 is an application of the Fourier analysis method (Section 3.3), therefore, it is divided into two parts. First, we prove that the Fourier transform of the characteristic function of the almost extremal families are highly concentrated on two irreducible representations of $PGL(2,q)$. Second, we use this Fourier characterization of almost extremal families to get structural information. In particular, we note that most of the ideas used in [16], can be used to characterize Boolean functions on $PGL(2,q)$ whose Fourier transforms are highly concentrated on the trivial and standard representations of $PGL(2,q)$. This partially answers a question of Ellis, Filmus and Friedgut in [17]. These authors asked if there were others groups (besides $S_n$) for which there is an elegant characterization of Boolean functions whose Fourier support is concentrated on certain irreducible representations. Actually, in Section 4.2, we explain that 3-transitive groups satisfying certain extra conditions have a similar characterization.

The proof of Theorem 41 follows from Theorem 40 and some basic properties of intersecting families in $PGL(2,q)$.

### 4.1 Fourier Characterization

Let $S$ be an intersecting family of maximum size in $PGL(2,q)$. It follows from Section 3.2 that the Fourier transform of $1_S$ is supported only on the irreducible representations affording the characters $\lambda_1$ and $\psi_1$. In this section, we prove that the characteristic functions of almost extremal families in $PGL(2,q)$ have Fourier transforms highly concentrated on the irreducible representations affording the characters $\lambda_1$ and $\psi_1$. To do this we apply a stability version of Hoffman's bound (this term was coined by Ellis in [13]). The next two lemmas show that if an intersecting family $S \subset PGL(2,q)$ satisfies that $|S|$ is close to $q(q-1)$ then $1_S$ must be close to $U := \widehat{V}_{\lambda_1} \oplus \widehat{V}_{\psi_1}$.

**Lemma 42.** *Let $S$ be an intersecting family in $PGL(2,q)$. If $q$ is a power of 2 then,*

$$\|P_{U^\perp}(1_S)\|^2_{PGL(2,q)} \leq \left(1 - \frac{|S|}{q(q-1)}\right) \|1_S\|^2_{PGL(2,q)}.$$

*Proof.* First, to ease notation we will denote by $\langle \cdot, \cdot \rangle$ and $\|\cdot\|$ the inner product and norm in $\mathbb{C}[PGL(2,q)]$. Let $A$ be the adjacency matrix of the graph $\Gamma = Cay(PGL(2,q), D_q)$ where $D_q$ is the set of derangement in $PGL(2,q)$. Let $\{x_1, \ldots, x_N\} \subset \mathbb{C}[PGL(2,q)]$ be an orthonormal basis of real eigenvectors for $A$ (recall that $A$ is symmetric). Let $\theta_i$ be the eigenvalue of $A$ such that $Ax_i = \theta_i x_i$, for $1 \leq i \leq N$. Note that,

- $1_S = \sum_{i=1}^{N} \epsilon_i x_i$ where $\epsilon_i = \langle 1_S, x_i \rangle$ for every $i = 1, \ldots, N$.
- $\|1_S\|^2 = \sum_{i=1}^{N} \epsilon_i^2$.
- $\langle 1_S, 1 \rangle = \|1_S\|^2 = \epsilon_1$.

Let $x_1$ be the all $1'$s vector with eigenvalue $q^2(q-1)/2$. Since every intersecting family corresponds to an independent set in the graph $\Gamma$ we get

$$0 = 1_S^T A 1_S = \sum_{i=1}^{N} \theta_i \epsilon_i^2 = \theta_1 \epsilon_1^2 + \sum_{i:i\neq 1, \theta_i \neq \lambda_{\min}} \theta_i \epsilon_i^2 - \frac{q(q-1)}{2} \sum_{i:\theta_i = \lambda_{\min}} \epsilon_i^2, \tag{4.1}$$

where $\lambda_{\min} = -q(q-1)/2$.

Recall that the second smallest eigenvalue of $\Gamma$ is zero. Therefore, from equation (4.1) we obtain the following inequality

$$\theta_1 \|1_S\|^4 - \frac{q(q-1)}{2} \sum_{i:\theta_i = \lambda_{\min}} \epsilon_i^2 \leq 0. \tag{4.2}$$

By definition we have

$$\|P_{U^\perp}(1_S)\|^2 = \sum_{i:i\neq 1, \theta_i \neq \lambda_{\min}} \epsilon_i^2,$$

hence

$$\sum_{i:\theta_i = \lambda_{\min}} \epsilon_i^2 = \|1_S\|^2 - \|1_S\|^4 - \|P_{U^\perp}(1_S)\|^2. \tag{4.3}$$

Combining (4.2) and (4.3) we get

$$\|P_{U^\perp}(1_S)\|^2 \leq \left(1 - \frac{|S|}{q(q-1)}\right) \|1_S\|^2.$$

□

The next lemma deals with the case $q$ odd. The proof is a little more complicated because in that case the minimum eigenvalue of $\Gamma$ is afforded by two distinct irreducible characters, $\psi_1$ and $\lambda_{-1}$.

**Lemma 43.** *Let $S$ be an intersecting family in $G_q$ such that $|S| = (1-\delta)q(q-1)$, $\delta > 0$. If $q$ is an odd prime power then*

$$\|P_{U^\perp}(1_S)\|^2_{PGL(2,q)} \leq \left(1 - \frac{|S|}{q(q-1)}\right)\|1_S\|^2_{PGL(2,q)} + \left(\frac{\delta}{q+1}\right)^2.$$

*Proof.* Using the notation introduced in the proof of Lemma 42 we get

$$\frac{q^2(q-1)}{2}\|1_S\|^4 - \frac{q(q-1)}{2}\sum_{i:\theta_i=\lambda_{min}} \epsilon_i^2 \leq 0. \tag{4.4}$$

Recall that the vector space $\widehat{V}_{\lambda_{-1}}$ is one dimensional. Hence, we denote by $x_{\lambda_{-1}}$ the only eigenvector in the set $\{x_i\}_{i=1}^N$ contained in $V_{\lambda_{-1}}$. We claim that $\epsilon^2_{\lambda_{-1}} = \langle 1_S, x_{\lambda_{-1}}\rangle^2 \leq (\delta/(q+1))^2$.

Note that $x_{\lambda_{-1}}$ is the irreducible character $\lambda_{-1}$. Hence, $x_{\lambda_{-1}}$ is a function on $PGL(2,q)$ such that $x_{\lambda_{-1}}(g) = 1$ if $g \in PSL(2,q)$ and $-1$, otherwise. Besides, note that $S \cap PSL(2,q)$ and $S \cap (PGL(2,q) \setminus PSL(2,q))$ have size at most $q(q-1)/2$ because the maximum size of an intersecting family in $PSL(2,q)$ is $q(q-1)/2$. Putting all the above remarks together

$$\begin{aligned}
\epsilon^2_{\lambda_{-1}} &= \langle 1_S, x_{\lambda_{-1}}\rangle^2 \\
&= \frac{1}{|PGL(2,q)|^2}(|S \cap PSL(2,q)| - |S \cap (PGL(2,q) \setminus PSL(2,q))|)^2 \\
&\leq \left(\frac{\delta}{q+1}\right)^2.
\end{aligned} \tag{4.5}$$

By definition we have

$$\|P_{U^\perp}(1_S)\|^2 = \sum_{i:i\neq 1,\theta_i\neq\lambda_{min}} \epsilon_i^2 + \epsilon^2_{\lambda_{-1}},$$

hence

$$\sum_{i:\theta_i=\lambda_{min}} \epsilon_i^2 = \|1_S\|^2 - \|1_S\|^4 - \|P_{U^\perp}(1_S)\|^2 + \epsilon^2_{\lambda_{-1}}. \tag{4.6}$$

Combininig (4.4), (4.5) and (4.6) we get

$$\|P_{U^\perp}(1_S)\|^2 \leq \left(1 - \frac{|S|}{q(q-1)}\right)\|1_S\|^2 + \left(\frac{\delta}{q+1}\right)^2.$$

□

### 4.2 Structural Characterization

In this section we give a characterization of the structure of Boolean functions on $PGL(2,q)$ whose Fourier transform is highly concentrated on $U$. The technique used to prove this result is from [16]. In that paper, Ellis, Filmus and Friedgut proved that if a Boolean function on $S_n$ has Fourier transform that is highly concentrated on the first two irreducible representations of $S_n$ (which correspond to the trivial and standard representation) then it must be close to a union of cosets of points stabilizers. Their proof is only based on the fact that the action of $S_n$ on $[n]$ is 3-transitive.

Let $G$ be a group acting 3-transitively on a set $X$. It is well-known (and easy to show) that the standard representation is irreducible for any 2-transitive group. Also, recall that $\widehat{V}_1$ and $\widehat{V}_{\chi_{std}}$ are the vector subspaces of complex-valued functions on $G$ whose Fourier transform have support on the trivial and the standard representation, respectively. The following proposition is a generalization of Theorem 1 from [16][2].

**Proposition 44.** *There exist absolute constants $C_1, \epsilon_1 > 0$ such that the following holds. Let $G$ be a finite group acting 3-transitively on a set $X$ of size $n$. Let $S \subset G$ with $|S| = (1-\delta)|G|/n$, where $0 \leq \delta < 1/2$. Let $U = \widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$. If $\|P_{U^\perp}(1_S)\|_G^2 = \epsilon \|1_S\|_G^2$, where $\epsilon \leq \epsilon_1$, then there exists $T \subset G$ such that $T$ is a coset of the stabilizer of an element of $X$, and*

$$|S \triangle T| \leq C_1 \left(\epsilon^{1/2} + \frac{1}{n}\right) |S|.$$

The proof of this proposition is exactly the same as the proof of Theorem 1 in [16]. Since the action of $PGL(2,q)$ on $PG(1,q)$ is 3-transitive, Proposition 44 can be used to characterize Boolean functions on $PGL(2,q)$ whose Fourier transform are highly concentrated on $U$. Recall that $U$ is the vector subspace of all of complex-valued functions on $PGL(2,q)$ whose Fourier transform has support on the trivial and the standard representation.

---

[2] Actually, Proposition 44 is a generalization of a special case of Theorem 1 from [16]. To fully generalize that theorem we need to consider $S \subset G$ with $|S| = c|G|/n$, where $c = o(n)$.

**Corollary 45.** *There exist absolute constants $C_1, \epsilon_1 > 0$ such that the following holds. Let $S \subset G_q$ with $|S| = (1-\delta)q(q-1)$, where $0 \leq \delta < 1/2$. If $\|P_{U^\perp}(1_S)\|^2_{PGL(2,q)} = \epsilon\|1_S\|^2_{PGL(2,q)}$ where $\epsilon \leq \epsilon_1$, then there exist $\alpha, \beta \in PG(1,q)$ such that $T_{\alpha,\beta}$ satisfies that*

$$|S \triangle T_{\alpha,\beta}| \leq C_1 \left(\epsilon^{1/2} + \frac{1}{q+1}\right)|S|.$$

Now we are ready to prove Theorem 40.

*Proof of Theorem 40.* First, to ease notation we will denote by $\|\cdot\|$ the norm in $\mathbb{C}[PGL(2,q)]$. We choose $C_0 = \max(\frac{4\sqrt{2}}{\sqrt{\epsilon_1}}, \sqrt{2}C_1)$ where $C_1$ and $\epsilon_1$ are the absolute constants from Corollary 45. With this choice of $C_0$, if $\epsilon_1/2 \leq \delta \leq 1/2$ then the statement of the theorem holds trivially with any choice of a coset of a point stabilizer $T$.

Now, we consider the case where $\delta < \epsilon_1/2$. By assumption we know that $|S| = (1-\delta)q(q-1)$. Thus, it follows from Lemmas 42 and 43 that $\|P_{U^\perp}(1_S)\|^2 \leq \delta\|1_S\|^2$ when $q$ is even and $\|P_{U^\perp}(1_S)\|^2 \leq 2\delta\|1_S\|^2$ when $q$ is odd. This implies that the characteristic function $1_S$ is highly concentrated on $U$. Hence, we can apply Corollary 45 to conclude that

$$|S \triangle T| \leq C_0 \left(\delta^{1/2} + \frac{1}{q+1}\right)|S|,$$

where $T$ is some coset of a point stabilizer. □

Theorem 40 implies that almost extremal families are almost contained in a coset of a point stabilizer. Furthermore, we can refine this result to conclude that almost extremal families are fully contained in a coset of a point stabilizer.

*Proof of Theorem 41.* First assume that $q \leq 4C_0 - 1$, where $C_0$ is the absolute constant from Theorem 40. Note that we can choose $\delta_1 > 0$ small enough such that for all $q \leq 4C_0 - 1$ we have

$$(1-\delta_1)q(q-1) > q(q-1) - 1.$$

Hence, if $S$ is an intersecting family of $PGL(2,q)$ with $|S| \geq (1-\delta_1)q(q-1)$ then $|S| = q(q-1)$. Therefore, by the characterization of intersecting families of maximum

size in $PGL(2,q)$ given in [45], we conclude that $S$ must be equal to a coset of the stabilizer of a point.

Now, we assume that $q > 4C_0 - 1$. It is clear that if we choose $\delta_2$ such that $0 \leq \delta_2 \leq 1/(16C_0^2)$ then

$$C_0\left(\delta_2^{1/2} + \frac{1}{q+1}\right) < \frac{1}{2}. \tag{4.7}$$

From Theorem 40 it follows that if $|S| \geq (1-\delta_2)q(q-1)$ then

$$|S \triangle T| \leq C_0\left(\delta_2^{1/2} + \frac{1}{q+1}\right)|S|, \tag{4.8}$$

where $T$ is a coset of a point stabilizer. Combining (4.7) and (4.8), we get that $|S \triangle T| < \frac{1}{2}q(q-1)$.

Suppose without loss of generality that $T = T_{\alpha,\alpha}$ for some $\alpha \in PG(1,q)$. Assume for a contradiction that there exists $g \in S$ such that $\alpha^g = \beta$ with $\beta \in PG(1,q)$, $\beta \neq \alpha$. We use this assumption to estimate the size of $T_{\alpha,\alpha} \setminus S$.

If $h \in S \cap T_{\alpha,\alpha}$ then $g^{-1}h$ contains at least one fixed point (recall that $S$ is an intersecting family). Hence, the elements $h \in T_{\alpha,\alpha}$ such that $g^{-1}h$ is a derangement must be contained in $T_{\alpha,\alpha} \setminus S$.

We compute the number of derangements in $g^{-1}T_{\alpha,\alpha} = T_{\beta,\alpha}$. The number of derangements in $T_{\alpha,\alpha}$ is zero. Thus, the $\frac{q^2(q-1)}{2}$ derangements in $PGL(2,q)$ are contained in $\bigcup_{\delta \neq \alpha} T_{\delta,\alpha}$. Using the 2-transitivity of the action of $PGL(2,q)$ on $PG(1,q)$, we get that the number of derangements in $T_{\delta,\alpha}$ is the same for every $\delta \neq \alpha$. Indeed, for any two distinct $\delta, \delta' \in PG(1,q)$ with $\delta, \delta' \neq \alpha$, let $m \in PGL(2,q)$ such that $\alpha^m = \alpha$ and $\delta^m = \delta'$. Then the bijection $\Phi : PGL(2,q) \to PGL(2,q) : g \mapsto m^{-1}gm$ satisfies $\Phi(D_q) = D_q$, and $\Phi(T_{\delta,\alpha}) = T_{\delta',\alpha}$, so $|T_{\delta',\alpha} \cap D_q| = |\Phi(T_{\delta,\alpha} \cap D_q)| = |T_{\delta,\alpha} \cap D_q|$.

Therefore, the number of derangements in $T_{\beta,\alpha}$ is $q(q-1)/2$. Hence, there are at least $q(q-1)/2$ elements in $T_{\alpha,\alpha} \setminus S$ which implies

$$|S \triangle T_{\alpha,\alpha}| \geq \frac{q(q-1)}{2}.$$

Thus, we get a contradiction. Finally, we choose the universal constant $\delta_0$ to be equal to $\min(\delta_1, \delta_2)$. □

# Chapter 5

## INTERSECTING FAMILIES OF MAXIMUM SIZE IN $PSL(2,q)$

Throughout this chapter we assume that $q$ is an odd prime power. It is known, from the combined results of [3, 45], that the maximum size of an intersecting family in $PSL(2,q)$ is $q(q-1)/2$. However, it is only a conjecture that all intersecting families of maximum size are cosets of point stabilizers. (See the second part of Conjecture 1 in [45].) In this paper, we prove that the second part of Conjecture 1 in [45] is true for all odd prime powers $q$.

**Theorem 46.** *Let $S$ be an intersecting family in $PSL(2,q)$ of maximum size. Then $S$ is a coset of a point stabilizer.*

To prove Theorem 46 we apply a general method for solving the characterization EKR-problem for some 2-transitive groups. This technique was proposed by Ahmadi and Meagher in [3] and they called it "The Module Method" (see Section 3.2). This method reduces the characterization of intersecting families of maximum size to the computation of the rank of a derangement matrix (Definition 6 ). Recall that the *derangement matrix* of $G$ acting on $X$ is the $(0,1)$-matrix $M$, whose rows are indexed by the derangements of $G$, whose columns are indexed by the ordered pairs of distinct elements in $X$, and for any derangement $g \in G$ and $(a,b) \in X \times X$ with $a \neq b$, the $(g,(a,b))$-entry of $M$ is defined by

$$M(g,(a,b)) = \begin{cases} 1, & \text{if } a^g = b, \\ 0, & \text{otherwise.} \end{cases}$$

The Module Method states that, under certain conditions (given in Theorem 35), if the rank of the derangement matrix $M$ of $G$ acting on $X$ is equal to $(|X|-1)(|X|-2)$,

then the cosets of point stabilizers are the only intersecting families of maximum size in $G$.

Since it is known that the maximum size of an intersecting family in $PSL(2,q)$ is $q(q-1)/2$ and that the characteristic function of every intersecting family of maximum size lies in the subspace $\widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$ of $\mathbb{C}[PSL(2,q)]$, then in order to prove Theorem 46 by applying the Module Method, it is enough to show that the rank of the derangement matrix $M$ of $PSL(2,q)$ acting on $PG(1,q)$ is equal to $q(q-1)$. Therefore, Theorem 46 follows directly from the next theorem.

**Theorem 47.** *Let $M$ be the derangement matrix of $PSL(2,q)$ acting on $PG(1,q)$. Then the $\mathbb{C}$-rank of $M$ is $q(q-1)$.*

Exactly the same statement for $PGL(2,q)$ is proved in [45, Prop. 9], so we must first examine why the proof does not immediately carry over to $PSL(2,q)$. In [45] the matrix $M^\top M$ represents a certain $PGL(2,q)$-module endomorphism of a permutation module. The main calculation is to show, for each irreducible constituent character of this module, that the image of $M^\top M$ is not annihilated by the corresponding central idempotent. Consequently, the image also contains the character as a constituent, and the rank result follows due to the fact that the module in question is almost multiplicity-free, in the sense that, with one exception, each irreducible constituent character occurs with multiplicity one. If one attempts to follow the same procedure for $PSL(2,q)$ one runs immediately into the problem that the $PSL(2,q)$-constituents of the permutation module have high multiplicity. Fortunately, this obstacle can be sidestepped by observing that although we are working in $PSL(2,q)$, our sets and permutation modules admit the action of $PGL(2,q)$, and for the larger group the permutation module has the property of being almost multiplicity-free. A more serious difficulty arises when one attempts to show that the central idempotents have nonzero images in the permutation module. As for $PGL(2,q)$, the problem boils down to showing that certain sums of character values are not zero. For $PGL(2,q)$, these sums could be estimated by elementary arguments. However, the sums for $PSL(2,q)$ appear

to be much harder to deal with, and our proof proceeds by reformulating the sums as character sums over finite fields and applying some deep results on hypergeometric functions over finite fields. The finite field character sums which appear are Legendre and Soto-Andrade sums (see Section 2.7). This is not a surprise; it is well known that these sums appear in connection with the complex representation theory of $PGL(2,q)$ [34].

The rest of this Chapter is organized as follows. In Section 5.1, we show that the rank of the derangement matrix $M$ is equal to the dimension of the image of a $PGL(2,q)$-module homomorphism. We use this fact to reduce the problem of computing the rank of $M$ to that of showing some explicit character sums over $PGL(2,q)$ are not equal to zero. In Section 5.2, we find some formulas to express those character sums over $PGL(2,q)$ in terms of Legendre and Soto-Andrade sums. Finally, in Section 5.3, we prove Theorem 47.

## 5.1 A $PGL(2,q)$-module Homomorphism

In this section we show that the rank of the derangement matrix $M$ of $PSL(2,q)$ is equal to the dimension of the image of a certain $PGL(2,q)$-module homomorphism. Actually, we will show that $N = M^\top M$ is a matrix representation of a $PGL(2,q)$-module homomorphism. We will use this fact to compute the rank of $M$.

### 5.1.1 The Matrix $N$

We identify the points of the projective line $PG(1,q)$ with elements of the set $\mathbb{F}_q \cup \{\infty\}$, by letting $a \in \mathbb{F}_q$ denote the point spanned by $(1,a) \in \mathbb{F}_q^2$ and denoting by $\infty$ the point spanned by $(0,1)$. We consider the natural right action of $PGL(2,q)$ on $PG(1,q)$. Let $a \in \mathbb{F}_q \cup \{\infty\}$ and $g \in PGL(2,q)$. We use $a^g$ to denote the element in $PG(1,q)$ obtained by applying $g$ to $a$. The action of $PGL(2,q)$ on $PG(1,q)$ is faithful. Hence, we can associate with each element of $PGL(2,q)$ a permutation of the $q+1$ elements of $PG(1,q)$. Moreover, recall that an element $g \in PGL(2,q)$ is said to be a *derangement* if its associated permutation is fixed-point-free.

**Definition 48.** Let $\Omega$ be the set of ordered pairs of distinct projective points in $PG(1,q)$. The matrix $N$ is a $q(q+1)$ by $q(q+1)$ matrix whose rows and columns are both indexed by the elements of $\Omega$; for any $(a,b),(c,d) \in \Omega$ we define

$$N_{(a,b),(c,d)} = \text{ the number of derangements of } PSL(2,q) \text{ sending } a \text{ to } b \text{ and } c \text{ to } d.$$

Note that the above definition of $N$ agrees with our former definition, $N = M^\top M$. Hence, basic linear algebra implies that $\text{rank}_{\mathbb{C}}(M) = \text{rank}_{\mathbb{C}}(N)$. The next lemma gives information about the entries of $N$.

**Lemma 49.** *Let $a,b,c,d \in \mathbb{F}_q \cup \{\infty\}$. Then,*

1. $N_{(a,b),(a,b)} = \dfrac{(q-1)^2}{4}, \quad \forall (a,b) \in \Omega.$

2. $N_{(a,b),(c,d)} = 0$, *if* $a = c, b \neq d$ *or* $a \neq c, b = d$.

3. $N_{(a,b),(b,a)} = \begin{cases} 0, & \text{if } q \equiv 1 \bmod 4, \\ (q-1)/2, & \text{if } q \equiv 3 \bmod 4, \end{cases} \quad \forall (a,b) \in \Omega.$

4. (a) $N_{(0,\infty),(1,0)} = \begin{cases} (q-1)/4, & \text{if } q \equiv 1 \bmod 4, \\ (q-3)/4, & \text{if } q \equiv 3 \bmod 4. \end{cases}$

   (b) $N_{(0,\infty),(1,d)} = \dfrac{q-3}{4} - \dfrac{\phi(1-d)}{2} - \dfrac{1}{4}\displaystyle\sum_{x \in \mathbb{F}_q^*} \phi((x+x^{-1})^2 - 4d), \quad \forall d \neq 0,1,\infty.$

*Moreover, the value of $N_{(a,b),(c,d)}$ for any $(a,b),(c,d) \in \Omega$ is given by one of the above expressions.*

*Proof.* Let $g$ be an arbitrary element in $PGL(2,q)$. Note that for every $h \in PSL(2,q)$ sending $a$ to $b$ and $c$ to $d$, the element $g^{-1}hg \in PSL(2,q)$ sends $a^g$ to $b^g$ and $c^g$ to $d^g$. Hence the entries of $N$ satisfy the following property

$$N_{(a,b),(c,d)} = N_{(a^g,b^g),(c^g,d^g)}, \tag{5.1}$$

because $PSL(2,q)$ is a normal subgroup of $PGL(2,q)$ and the set of derangements in $PSL(2,q)$ is closed under conjugation. To prove Lemma 49 we proceed case by case.

- **Case 1**.

  Recall that $N_{(a,b),(a,b)}$ is the number of derangements in $PSL(2,q)$ sending $a$ to $b$. From (5.1) and the 2-transitivity of $PGL(2,q)$ we conclude that $N_{(a,b),(a,b)} = N_{(c,d),(c,d)}$ for any $(a,b),(c,d) \in \Omega$. The total number of derangements in $PSL(2,q)$ is $q(q-1)^2/4$ and this number can also be written as

$$\frac{q(q-1)^2}{4} = \sum_{\substack{b \in PG(1,q) \\ b \neq a}} N_{(a,b),(a,b)}, \quad \text{for any fixed } a \in PG(1,q),$$

  which implies that $N_{(a,b),(a,b)} = (q-1)^2/4$ for every $(a,b) \in \Omega$.

- **Case 2**.

  Every element of $PSL(2,q)$ is related to a permutation of projective points in $PG(1,q)$. This implies $N_{(a,b)(a,d)} = 0$ and $N_{(a,b)(c,b)} = 0$ whenever $b \neq d$ and $a \neq c$.

- **Case 3**.

  Using the 2-transitivity of $PGL(2,q)$ and (5.1) we can assume without loss of generality that $a = 0$ and $b = \infty$. The elements $g_\lambda \in PSL(2,q)$ sending 0 to $\infty$ and $\infty$ to 0 are of the form

$$g_\lambda = \begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{pmatrix}, \quad \lambda \in \mathbb{F}_q^*.$$

  This representation of elements in $PSL(2,q)$ is redundant because $g_\lambda$ and $g_{-\lambda}$ represent the same element of $PSL(2,q)$. Let $\xi$ be an element in $\mathbb{F}_q^*$ such that $\langle \xi \rangle = \mathbb{F}_q^*$. Hence, the set $\{g_\lambda : \lambda = \xi^i, \quad i = 1, \ldots, (q-1)/2\}$ corresponds precisely to the $(q-1)/2$ elements in $PSL(2,q)$ sending 0 to $\infty$ and $\infty$ to 0.

  Recall that $g_\lambda$ is a derangement if and only if its eigenvalues are not in $\mathbb{F}_q$. Thus, $g_\lambda$ is a derangement if and only if its characteristic polynomial,

$$p_\lambda(t) = \det \begin{vmatrix} -t & \lambda \\ -\lambda^{-1} & -t \end{vmatrix} = t^2 + 1,$$

  is irreducible over $\mathbb{F}_q$.

  If $q \equiv 1 \pmod 4$ then $-1$ is a square in $\mathbb{F}_q$; so $p_\lambda(t)$ is reducible for every $\lambda \in \mathbb{F}_q^*$. Hence $N_{(a,b),(b,a)} = N_{(0,\infty),(\infty,0)} = 0$ in this case. On the other hand, if $q \equiv 3 \pmod 4$ then $-1$ is not a square in $\mathbb{F}_q$; this implies that $p_\lambda(t)$ is irreducible for every $\lambda \in F_q^*$. Thus $N_{(a,b),(b,a)} = N_{(0,\infty),(\infty,0)} = (q-1)/2$.

- **Case 4**.

Every element of $PSL(2,q)$ sending 0 to $\infty$ and 1 to $d$ is of the form

$$g_\lambda = \begin{pmatrix} 0 & -\lambda \\ \lambda^{-1} & \lambda^{-1}d+\lambda \end{pmatrix}, \quad \lambda \in \mathbb{F}_q^*.$$

Again note that $g_\lambda$ and $g_{-\lambda}$ represent the same element of $PSL(2,q)$. The matrix $g_\lambda$ is a derangement if and only if its characteristic polynomial,

$$p_\lambda(t) = \det \begin{vmatrix} -t & \lambda \\ \lambda^{-1} & \lambda^{-1}d+\lambda-t \end{vmatrix} = t^2 - (\lambda^{-1}d+\lambda)t + 1,$$

is irreducible over $\mathbb{F}_q$. To compute $N_{(0,\infty)(1,d)}$ it is enough to count the number of values of $\lambda$ such that $p_\lambda(t)$ is reducible.

If $p_\lambda(t)$ is reducible then there exist $x$ and $y$ in $\mathbb{F}_q^*$ such that

$$p_\lambda(t) = t^2 - (\lambda^{-1}d+\lambda)t + 1 = (t-x)(t-y) = t^2 - (x+y)t + xy.$$

Hence, $xy = 1$ and $x + y = \lambda^{-1}d + \lambda$. Assume without loss of generality that $y = x^{-1}$. If there exist values of $\lambda$ such that $g_\lambda$ has eigenvalues $\{x, x^{-1}\}$ then they have to satisfy the following quadratic equation

$$\lambda^2 - (x + x^{-1})\lambda + d = 0. \tag{5.2}$$

– **Case 4 (a)**:

If we assume $d = 0$ then $\lambda = 0$ is a solution of (5.2), however, that solution is not admissible by the definition of $g_\lambda$. Hence, we just consider the solution $\lambda = x + x^{-1}$ for every $x \in \mathbb{F}_q^*$. Moreover, note that $x$ and $x^{-1}$ generate the same value of $\lambda$. In fact, we can relate to each set $\{x, x^{-1}\}$ a unique value of $\lambda$.

Let $q \equiv 1 \pmod 4$ and $k \in \mathbb{F}_q^*$ be an element of order 4. Note that the set $\{k, k^{-1}\}$ does not generate any admissible value of $\lambda$. Thus, the number of values of $\lambda$ such that $p_\lambda(t)$ is reducible is $(q-1)/2$. Therefore,

$$N_{(0,\infty),(1,0)} = \frac{1}{2}\left(q - 1 - \frac{q-1}{2}\right) = \frac{q-1}{4}.$$

On the other hand, if $q \equiv 3 \pmod 4$ then $\mathbb{F}_q^*$ does not have an element of order 4. This implies that every set $\{x, x^{-1}\} \subset \mathbb{F}_q^*$ generates an admissible value of $\lambda$. Thus, the number of values for $\lambda$ such that $p_\lambda(t)$ is reducible is $(q+1)/2$ and $N_{(0,\infty),(1,0)} = (q-3)/4$.

– **Case 4 (b)**:

The number of solutions of (5.2) in $\mathbb{F}_q$ is given by $1 + \phi((x+x^{-1})^2 - 4d)$. In this case, we also have that $x$ and $x^{-1}$ generate the same values of $\lambda$. Thus, the number of values of $\lambda \in \mathbb{F}_q^*$ such that $p_\lambda(t)$ is reducible is

$$2(1+\phi(1-d)) + \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_q^* \\ x\neq 1,-1}} (1+\phi((x+x^{-1})^2 - 4d)),$$

Therefore, for $d \neq 0, 1, \infty$,

$$N_{(0,\infty),(1,d)} = \frac{1}{2}[q - 1 - (2(1 + \phi(1 - d)) + \frac{1}{2} \sum_{\substack{x \in \mathbb{F}_q^* \\ x \neq 1, -1}} (1 + \phi((x + x^{-1})^2 - 4d))]$$

which gives the desired formula for $N_{(0,\infty),(1,d)}$.

□

**Corollary 50.** *Let $d \in \mathbb{F}_q$, $d \neq 0, 1$. The number of derangements of $PSL(2, q)$ sending $0$ to $\infty$ and $1$ to $d$ can be expressed in terms of the Legendre sum with respect to $\phi$. Specifically,*

$$N_{(0,\infty),(1,d)} = \frac{q - 1}{4} - \frac{\phi(1 - d)}{2} - \frac{q}{4} P_\phi(2d - 1). \tag{5.3}$$

*Proof.* To prove this corollary we use part 4(b) of Lemma 49 and the following computation,

$$\begin{aligned} \sum_{x \in \mathbb{F}_q^*} \phi((x + x^{-1})^2 - 4d) &= \sum_{x \in \mathbb{F}_q^*} \phi(x^2 - 2(2d - 1)x + 1)(1 + \phi(x)) \\ &= -2 + qP_\phi(2d - 1) \end{aligned}$$

□

### 5.1.2 A Permutation $PGL(2, q)$-module

In this section we define a $PGL(2, q)$-module $V$ and a $PGL(2, q)$-module homomorphism $T_N$ from $V$ to $V$. We use the subscript $N$ to emphasize that $N$ is the matrix associated with $T_N$ with respect to a certain basis of $V$.

Recall that we denote by $\Omega$ the set of ordered pairs of distinct projective points in $PG(1, q)$. Let $V$ be the $\mathbb{C}$-vector space spanned by the vectors $\{e_\omega\}_{\omega \in \Omega}$, therefore, the dimension of $V$ is $q(q + 1)$.

We define a right action of $PGL(2, q)$ on the basis $\{e_\omega\}$ of $V$. Specifically, if $\omega = (a, b)$ then

$$e_\omega \cdot g = e_{\omega^g} = e_{(a^g, b^g)}$$

for any $g \in PGL(2,q)$. Thus, $V$ is a right permutation $PGL(2,q)$-module. The next lemma shows that $V$ has a very simple decomposition into irreducible modules; apart from $V_{\lambda_{-1}}$ and $V_{\psi_1}$ each irreducible module of $PGL(2,q)$ appears exactly once.

Let $\langle \chi, \psi \rangle_{PGL(2,q)}$ denote the inner product of the characters $\chi$ and $\psi$ of $PGL(2,q)$ (see Section 2.1).

**Lemma 51.** *Let $V_\chi$ denote an irreducible module of $PGL(2,q)$ with character $\chi$. Then the decomposition of $V$ into irreducible constituents is given by,*

$$V \cong V_{\lambda_1} \oplus V_{\psi_1}^{\oplus 2} \oplus V_{\psi_{-1}} \oplus \bigoplus_{\beta \in B} V_{\eta_\beta} \oplus \bigoplus_{\gamma \in A} V_{\nu_\gamma}$$

*Proof.* Let $\pi$ be the character afforded by the $PGL(2,q)$-module $V$. By definition we have

$$\pi(g) = |\{\omega \in \Omega : \omega^g = \omega\}|$$

hence the character $\pi$ has an easy description,

| | $1$ | $u$ | $d_x$ | $v_r$ |
|---|---|---|---|---|
| $\pi$ | $q(q+1)$ | $0$ | $2$ | $0$ |

Now let $V_\chi$ be an irreducible representation of $PGL(2,q)$ and $\chi$ its irreducible character. It is known ([53, Chapter 2, Theorem 4]) that the multiplicity of $V_\chi$ in $V$ is equal to the character inner product $\langle \pi, \chi \rangle_{PGL(2,q)}$. Now, the lemma follows by direct calculation using the character table of $PGL(2,q)$. □

For $a, b \in PG(1,q)$, consider the following vectors in V,

$$l_{a,b} = \sum_{\substack{p \in PG(1,q) \\ p \neq a,b}} (e_{(a,p)} - e_{(b,p)}) + e_{(a,b)} - e_{(b,a)} \tag{5.4}$$

$$r_{a,b} = \sum_{\substack{p \in PG(1,q) \\ p \neq a,b}} (e_{(p,a)} - e_{(p,b)}) + e_{(b,a)} - e_{(a,b)} \tag{5.5}$$

We use these vectors to define the following vector subspaces of $V$,

$$V_1 = \text{span}_{\mathbb{C}}\{l_{a,b} : a, b \in PG(1,q)\} \quad \text{and} \quad V_2 = \text{span}_{\mathbb{C}}\{r_{a,b} : a, b \in PG(1,q)\}$$

In fact, the next lemma shows that $V_1$ and $V_2$ are $PGL(2,q)$-submodules of $V$.

**Lemma 52.** *The vector subspaces $V_1$ and $V_2$ satisfy the following properties,*

1. $\dim_{\mathbb{C}}(V_1) = \dim_{\mathbb{C}}(V_2) = q$
2. $V_1 \cap V_2 = \{0\}$
3. *$V_1$ and $V_2$ are $PGL(2,q)$-submodules of $V$*
4. *$V_1 \cong V_2$ as $PGL(2,q)$-modules*

*Proof.* Note that the vectors defined in (5.4) and (5.5) satisfy the following relations,

$$l_{a,b} - l_{a,c} = l_{c,b} \quad \text{and } r_{a,b} - r_{a,c} = r_{c,b}$$

for all $a, b, c \in PG(1,q)$ with $a \neq b \neq c$. Hence, fixing $a \in PG(1,q)$ we get that $\{l_{a,b} : b \in PG(1,q), b \neq a\}$ and $\{r_{a,b} : b \in PG(1,q), b \neq a\}$ are basis for $V_1$ and $V_2$, respectively.

To prove the conclusion in part (2) we proceed by contradiction. Assume there exists $v \in V_1 \cap V_2$ with $v \neq 0$. Hence we can write,

$$v = \sum_{\substack{p \in PG(1,q) \\ p \neq a}} \alpha_p l_{a,p} = \sum_{\substack{p \in PG(1,q) \\ p \neq a}} \beta_p r_{a,p} \tag{5.6}$$

where not all $\alpha_p$ and $\beta_p$ are equal to zero.

For a fix $b \in PG(1,q)$, the vector $l_{a,b}$ is the only one in the set $\{l_{a,p}\}_{p \in PG(1,q)}$ that contains $e_{(b,a)}$. On the other hand, every vector of the form $r_{a,p}$ contains $e_{(b,a)}$ . Therefore, using (5.6) we get,

$$\alpha_b = \sum_{\substack{p \in PG(1,q) \\ p \neq a}} \beta_p$$

which implies that the values of the coefficients $\alpha_p$ in (5.6) are all the same. Analogously, we can show that the values $\beta_p$ in (5.6) are the same. Thus, we can rewrite equation (5.6) in the following way,

$$\sum_{\substack{p \in PG(1,q) \\ p \neq a}} l_{a,p} = \frac{\beta}{\alpha} \sum_{\substack{p \in PG(1,q) \\ p \neq a}} r_{a,p}$$

where $\alpha = \sum_{p \neq a} \beta_p$ and $\beta = \sum_{p \neq a} \alpha_p$. This implies that $\beta/\alpha = 1/q$, a contradiction.

To prove part (3) it is enough to note that $l_{a,b} \cdot g = l_{a^g,b^g}$ and $r_{a,b} \cdot g = r_{a^g,b^g}$ for all $a, b \in PG(1,q)$ with $a \neq b$. For part (4) consider the function $\theta$ from $V_1$ to $V_2$ defined by $\theta(l_{a,b}) = r_{a,b}$ for all $a, b \in PG(1,q)$ with $a \neq b$; we extend the definition of $\theta$ to all elements of $V_1$ linearly. Now, from the definition of $\theta$ we see that clearly

$$\theta(l_{(a,b)} \cdot g) = \theta(l_{(a,b)}) \cdot g$$

for all $g \in PGL(2,q)$ and $(a,b) \in \Omega$. Therefore, $\theta$ is a $PGL(2,q)$-module isomorphism. This completes the proof of part (4). □

**Lemma 53.** *The submodules $V_1$ and $V_2$ are isomorphic to $V_{\psi_1}$.*

*Proof.* This result follows directly from Lemmas 51 and 52. If we consider the decomposition of $V$ into irreducible constituents, we note that each irreducible representation appears only once, except for $V_{\psi_1}$ . Therefore, because $V_1$ is isomorphic to $V_2$, we must have $V_{\psi_1} \cong V_1 \cong V_2$. □

We now define a linear transformation $T_N$ from $V$ to $V$. We first define $T_N$ on the basis $\{e_\omega\}_{\omega \in \Omega}$ of $V$ by

$$T_N(e_{(a,b)}) = \sum_{\omega \in \Omega} N_{\omega,(a,b)} e_\omega$$

for any $(a,b) \in \Omega$, and then extend the definition of $T_N$ to all elements of $V$ linearly. It follows from the definition of $T_N$ that $N$ is the matrix associated with $T_N$ with respect to the basis $\{e_\omega\}_{\omega \in \Omega}$ of $V$. Therefore, the dimension of the image of $T_N$ is equal to the rank of the derangement matrix $M$ of $PSL(2,q)$ acting on $PG(1,q)$.

**Lemma 54.** *The linear transformation $T_N$ defined above is a $PGL(2,q)$-module homomorphism from $V$ to $V$.*

*Proof.* To prove the lemma we just need to check that the next equation

$$T_N(e_{(a,b)} \cdot g) = T_N(e_{(a,b)}) \cdot g \tag{5.7}$$

holds for all $g \in PGL(2,q)$ and $(a,b) \in \Omega$. First, consider the left hand side of (5.7). From the definition of $T_N$ it follows that

$$T_N(e_{(a,b)} \cdot g) = T_N(e_{(a^g,b^g)}) = \sum_{\omega \in \Omega} N_{\omega,(a^g,b^g)} e_\omega.$$

Furthermore, note that using equation (5.1), the right hand side of (5.7) can be written as

$$T_N(e_{(a,b)}) \cdot g = \sum_{\omega \in \Omega} N_{\omega,(a,b)} e_{\omega^g} = \sum_{\omega^{g^{-1}} \in \Omega} N_{\omega^{g^{-1}},(a,b)} e_\omega = \sum_{\omega \in \Omega} N_{\omega,(a^g,b^g)} e_\omega$$

which implies that (5.7) holds. This completes the proof of the lemma. □

### 5.1.3 The Image of $T_N$

Recall that the rank of the derangement matrix $M$ of $PSL(2,q)$ acting on $PG(1,q)$ is equal to the dimension of the image of $T_N$. Since $T_N$ is a $PGL(2,q)$-module homomorphism (Lemma 54) we can use some tools from representation theory to compute the dimension of the image of $T_N$. We start by observing that the submodules $V_1$ and $V_2$ are in the kernel of $T_N$.

**Lemma 55.** *The subspaces $V_1$ and $V_2$ lie in the kernel of $T_N$.*

*Proof.* First, recall that the derangement matrix $M$ is a $q(q-1)^2/4$ by $(q+1)q$ matrix whose rows are indexed by the derangements of $PSL(2,q)$ and whose columns are indexed by elements of $\Omega$. For any derangement $g \in PSL(2,q)$ and $(a,b) \in \Omega$ we have

$$M(g,(a,b)) = \begin{cases} 1, & \text{if } a^g = b, \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, also by definition we have $N = M^\top M$. Thus, the lemma follows from the following observation

$$Ml_{a,b} = 0 \quad \text{and} \quad Mr_{a,b} = 0 \quad \text{for all } a,b \in PG(1,q), \text{ with } a \neq b,$$

and the fact that for a fix $a \in PG(1,q)$ the sets $\{l_{a,b} : b \in PG(1,q), b \neq a\}$ and $\{r_{a,b} : b \in PG(1,q), b \neq a\}$ are basis of $V_1$ and $V_2$, respectively.

□

From Lemma 53 and 55, we conclude that the restriction of $T_N$ to $2V_{\psi_1}$ is the zero map. It follows that the dimension of the image of $T_N$ is at most $q(q-1)$. Now, we consider the restriction of $T_N$ onto the other irreducible constituents of $V$. To do that we apply Schur's lemma.

Let $\chi$ be the irreducible character corresponding to an irreducible representation of $PGL(2,q)$ appearing as a constituent of $V$. Schur's lemma implies that,

$$T_N(V_\chi) \cong V_\chi \quad \text{or} \quad T_N(V_\chi) = \{0\}.$$

Thus, either the dimension of the restriction of $T_N$ to $V_\chi$ is zero or is equal to the dimension of $V_\chi$. Hence, to study the image of $V_\chi$ under $T_N$ for any

$$\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$$

we proceed in the following way:

1. Consider the vector $e_{(0,\infty)} \in V$.

2. Project $e_{(0,\infty)}$ onto $V_\chi$ using the following scalar multiple of a central primitive idempotent

$$E_\chi = \sum_{g\in PGL(2,q)} \chi(g^{-1})g.$$

Therefore, the projection of $e_{(0,\infty)}$ onto $V_\chi$ is equal to

$$E_\chi(e_{(0,\infty)}) = \sum_{g\in PGL(2,q)} \chi(g^{-1})e_{(0^g,\infty^g)} = \sum_{(a,b)\in\Omega} \left[\sum_{0^g=a,\infty^g=b} \chi(g^{-1})\right] e_{(a,b)}.$$

where $g$ in the inner sum runs over all elements in $PGL(2,q)$ sending 0 to $a$ and $\infty$ to $b$.

3. To prove that $T_N(V_\chi) \cong V_\chi$ it is enough to show that the $(0,\infty)$ coordinate of $T_N(E_\chi(e_{(0,\infty)}))$ is not equal to zero. This is equivalent to showing that the following character sum is not equal to zero:

$$T_{N,\chi} := T_N(E_\chi(e_{(0,\infty)}))_{(0,\infty)} = \sum_{(a,b)\in\Omega} \left[\sum_{0^g=a,\infty^g=b} \chi(g^{-1})\right] N_{(0,\infty),(a,b)}, \tag{5.8}$$

where $g$ in the inner sum runs over all elements in $PGL(2,q)$ sending 0 to $a$ and $\infty$ to $b$.

Therefore, we get the following lower bound on the rank of the derangement matrix $M$,

$$\sum_{\chi} \dim(V_\chi) \leq \operatorname{rank}(M), \tag{5.9}$$

where $\chi$ in the sum on the left hand side of (5.9) runs through the set of irreducible characters from $\{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$ satisfying that $T_{N,\chi} \neq 0$. In particular, if $T_{N,\chi}$ is not zero for all $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$ then the rank of the derangement matrix $M$ is equal to $q(q-1)$. We conclude that to prove Theorem 47, it is enough to show that the values of the character sums $T_{N,\chi}$ with $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$ are not equal to zero. This will be our objective in the next two sections.

## 5.2 The Character Sums $\sum_{0^g=\infty,\infty^g=0} \chi(g^{-1})$ and $\sum_{0^g=\infty,1^g=d} \chi(g^{-1})$

The sums $T_{N,\chi}$ are character sums over $PGL(2,q)$. In general, it is not easy to get tight bounds on the values of characters sums over non-abelian groups. Fortunately, the close relationship between the irreducible characters of $PGL(2,q)$ and the multiplicative characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ allows us to conclude in Section 5.3 that the expressions $T_{N,\chi}$ are not equal to zero. In this section, we show that we can express the sums $T_{N,\chi}$ in terms of characters sums over finite fields for every $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$.

First, we consider $T_{N,\chi}$ when $\chi = \lambda_1$. In this case, we know that $\lambda_1(g) = 1$ for any $g \in PGL(2,q)$. Moreover, there are precisely $q-1$ elements of $PGL(2,q)$ sending 0 to $\infty$ and $a$ to $b$ for any $a, b \in PG(1,q)$. Therefore, we can compute (6.5) explicitly for $\chi = \lambda_1$:

$$T_{N,\lambda_1} = (q-1) \sum_{(a,b)\in\Omega} N_{(0,\infty)(a,b)} = (q-1)(q+1)\frac{(q-1)^2}{4},$$

where we have used Lemma 49 to obtain the last equality. Thus, from the analysis given in Section 5.1.3 we conclude that $T_N(V_{\lambda_1}) \cong V_{\lambda_1}$.

The other irreducible characters of $PGL(2,q)$ are not so easy to handle. The next lemma gives an expression for $T_{N,\chi}$ with $\chi \in \{\psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$ which will be helpful to write (6.5) in terms of character sums over finite fields.

**Lemma 56.** *Let $\chi$ be any irreducible character of $PGL(2,q)$ from the set*

$$\{\psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}.$$

*Let $h$ be the unique element of $PGL(2,q)$ sending $0$ to $0$, $1$ to $\infty$, and $\infty$ to $1$. If $q \equiv 1 \bmod 4$ then*

$$T_{N,\chi} = \frac{(q-1)^3}{4} - \frac{q-1}{2} \sum_{0^g=\infty,\infty^g=0} \chi(g^{-1}) + (q-1) \sum_{\substack{b\in\mathbb{F}_q^* \\ b\neq 1}} \left[ \sum_{0^g=\infty, 1^g=b^h} \chi(g^{-1}) \right] N_{(0,\infty),(1,b)},$$

*and if $q \equiv 3 \bmod 4$ then*

$$T_{N,\chi} = \frac{(q-1)^3}{4} + \sum_{0^g=\infty,\infty^g=0} \chi(g^{-1}) + (q-1) \sum_{\substack{b\in\mathbb{F}_q^* \\ b\neq 1}} \left[ \sum_{0^g=\infty, 1^g=b^h} \chi(g^{-1}) \right] N_{(0,\infty),(1,b)}.$$

*Proof.* From (6.5) and Lemma 49 we get,

$$\begin{aligned} T_{N,\chi} \;=\; & \frac{(q-1)^2}{4} \sum_{0^g=0,\infty^g=\infty} \chi(g^{-1}) + \left[ \sum_{0^g=\infty,\infty^g=0} \chi(g^{-1}) \right] N_{(0,\infty),(\infty,0)} \\ & + \sum_{b\in\mathbb{F}_q^*} \left[ \sum_{0^g=\infty,\infty^g=b} \chi(g^{-1}) \right] N_{(0,\infty),(\infty,b)} + \sum_{a\in\mathbb{F}_q^*} \left[ \sum_{0^g=a,\infty^g=0} \chi(g^{-1}) \right] N_{(0,\infty),(a,0)} \\ & + \sum_{\substack{a,b\in\mathbb{F}_q^* \\ a\neq b}} \left[ \sum_{0^g=a,\infty^g=b} \chi(g^{-1}) \right] N_{(0,\infty),(a,b)} \end{aligned}$$

We denote by $PGL(2,q)_{0,\infty}$ the subgroup of $PGL(2,q)$ fixing $0$ and $\infty$. Analogously, $PGL(2,q)_0$ denotes the subgroup of $PGL(2,q)$ fixing $0$. Applying the Frobenius Reciprocity Theorem [53, Chapter 7, Theorem 13], we obtain the following equations:

$$\langle \mathrm{Res}(\chi), 1\rangle_{PGL(2,q)_{0,\infty}} = \langle \chi, \pi\rangle_{PGL(2,q)} \quad \text{and} \quad \langle \mathrm{Res}(\chi), 1\rangle_{PGL(2,q)_0} = \langle \chi, \lambda_1 + \psi_1\rangle_{PGL(2,q)}$$

where $\pi$ is the permutation character defined in the proof of Lemma 51 and 1 is the trivial character of the groups $PGL(2,q)_{0,\infty}$ and $PGL(2,q)_0$, respectively. Using these equations and the transitivity of $PGL(2,q)$ we evaluate the following character sums,

$$\sum_{0^g=0,\infty^g=\infty} \chi(g^{-1}) = q-1, \quad \sum_{0^g=0} \chi(g^{-1}) = 0, \quad \sum_{\infty^g=\infty} \chi(g^{-1}) = 0.$$

Note that $\chi(kgk^{-1}) = \chi(g)$ for any $k \in PGL(2,q)$ because $\chi$ is a character. Thus, from the above equations and the 2-transitivity of $PGL(2,q)$ we get

$$\sum_{0^g=\infty} \chi(g^{-1}) = \sum_{\infty^g=0} \chi(g^{-1}) = 0.$$

Now assume that $q \equiv 1 \pmod 4$. From Lemma 49 we have $N_{(0,\infty),(\infty,b)} = N_{(0,\infty),(a,0)} = (q-1)/4$ for all $a, b \in \mathbb{F}_q^*$. Hence, using the above analysis we can write,

$$\begin{aligned}
\sum_{b\in\mathbb{F}_q^*} \left[\sum_{0^g=\infty,\infty^g=b} \chi(g^{-1})\right] N_{(0,\infty),(\infty,b)} &= \frac{q-1}{4} \sum_{b\in\mathbb{F}_q^*} \left[\sum_{0^g=\infty,\infty^g=b} \chi(g^{-1})\right] \\
&= \frac{q-1}{4} \left[\sum_{0^g=\infty} \chi(g^{-1}) - \sum_{0^g=\infty,\infty^g=0} \chi(g^{-1})\right] \\
&= -\frac{(q-1)}{4} \sum_{0^g=\infty,\infty^g=0} \chi(g^{-1}),
\end{aligned}$$

and using the same ideas we get

$$\sum_{a\in\mathbb{F}_q^*} \left[\sum_{0^g=a,\infty^g=0} \chi(g^{-1})\right] N_{(0,\infty),(a,0)} = -\frac{(q-1)}{4} \sum_{0^g=\infty,\infty^g=0} \chi(g^{-1}).$$

A similar computation works for the case when $q \equiv 3 \bmod 4$.

Let $a, b \in \mathbb{F}_q^*$ with $a \neq b$. Using the 3-transitivity of the action of $PGL(2,q)$ on $PG(1,q)$ and (5.1) we conclude that $N_{(0,\infty),(a,b)} = N_{(0,\infty)(1,b^h)}$ where $h \in PGL(2,q)$ is the unique element sending 0 to 0, $\infty$ to $\infty$ and $a$ to 1. Moreover, using the definition of $h$ we obtain

$$\sum_{0^g=a,\infty^g=b} \chi(g^{-1}) = \sum_{0^g=1,\infty^g=b^h} \chi(g^{-1}).$$

Therefore, putting all these together we get that

$$\begin{aligned}\sum_{\substack{a,b\in\mathbb{F}_q^*\\ a\neq b}}\left[\sum_{0^g=a,\infty^g=b}\chi(g^{-1})\right]N_{(0,\infty),(a,b)} &= (q-1)\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}}\left[\sum_{0^g=1,\infty^g=b}\chi(g^{-1})\right]N_{(0,\infty),(1,b)}\\ &= (q-1)\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}}\left[\sum_{0^g=\infty,1^g=b^h}\chi(g^{-1})\right]N_{(0,\infty),(1,b)}.\end{aligned}$$

□

It follows from Lemma 56 that we can write $T_{N,\chi}$ in terms of the character sums

$$\sum_{0^g=\infty,\infty^g=0}\chi(g^{-1}) \quad \text{and} \quad \sum_{0^g=\infty,1^g=d}\chi(g^{-1}).$$

The next four lemmas show that these character sums can be be written in terms of character sums over finite fields for all $\chi\in\{\psi_{-1},\{\eta_\beta\}_{\beta\in B},\{\nu_\gamma\}_{\gamma\in A}\}$.

**Lemma 57.** *Let $i$ be an element of $\mathbb{F}_{q^2}^*$ such that $i^2\in\mathbb{F}_q^*$. Then,*

$$\begin{aligned}\sum_{0^g=\infty,\infty^g=0}\psi_{-1}(g^{-1}) &= \phi(-1)(q-1),\\ \sum_{0^g=\infty,\infty^g=0}\nu_\gamma(g^{-1}) &= \gamma(-1)(q-1) \quad \textit{for all } \gamma\in A,\\ \sum_{0^g=\infty,\infty^g=0}\eta_\beta(g^{-1}) &= -\beta(i)(q-1) \quad \textit{for all } \beta\in B.\end{aligned}$$

*Proof.* The elements in $PGL(2,q)$ sending 0 to $\infty$ and $\infty$ to 0 are of the form,

$$g_\lambda=\begin{pmatrix}0 & \lambda\\ 1 & 0\end{pmatrix} \quad \text{with } \lambda\in\mathbb{F}_q^*.$$

To evaluate the character sums in this lemma we need to know to which conjugacy classes these elements belong. Note that the characteristic polynomial of $g_\lambda$ is $p_\lambda(t)=t^2-\lambda$.

First, recall that the eigenvalues of $g_\lambda$ are defined up to multiplication by an element of $\mathbb{F}_q^*$. Now, if $\lambda$ is a square in $\mathbb{F}_q^*$ then $p_\lambda(t)$ is reducible and $g_\lambda$ has eigenvalues $\pm\sqrt{\lambda}\in\mathbb{F}_q^*$. This implies that $g_\lambda$ lies in the conjugacy class $d_{-1}$ whenever $\lambda$ is a square.

On the other hand, if $\lambda$ is not a square the roots of $p_\lambda(t)$ lie on $\mathbb{F}_{q^2}^*$ and they correspond to elements of order 2 in $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$. Therefore, whenever $\lambda$ is not a square we see that $g_\lambda$ lies on the conjugacy class $v_i$.

Since there are equal number of squares and nonsquares in $\mathbb{F}_q^*$, the lemma follows from the character table of $PGL(2,q)$ and Lemma 49. □

**Lemma 58.** *For every $\gamma \in A$ and $d \in \mathbb{F}_q^* \setminus \{1\}$ we have*

$$\sum_{0^g=\infty, 1^g=d} \nu_\gamma(g^{-1}) = qP_\gamma(2d-1).$$

*Proof.* The elements in $PGL(2,q)$ sending 0 to $\infty$ and 1 to $d$ are of the form,

$$g_\lambda = \begin{pmatrix} 0 & \alpha\lambda \\ \alpha & \alpha(d-\lambda) \end{pmatrix} \quad \text{with } \lambda, \alpha \in \mathbb{F}_q^*.$$

To evaluate the sum in this lemma we need to know to which conjugacy classes these elements belongs. However, we need to do this just for those elements which are not derangements because $\nu_\gamma(g) = 0$ if $g$ is a derangement.

Note that different values of $\alpha$ correspond to the same element $g_\lambda$ in $PGL(2,q)$. Indeed, as was remarked earlier the eigenvalues of $g_\lambda$ are defined up to scalar multiplication.

The characteristic polynomial of $g_\lambda$ is $p_\lambda(t) = t^2 - \alpha(d-\lambda)t - \alpha^2\lambda$ and its eigenvalues are,

$$t = \alpha\left(\frac{(d-\lambda) \pm \sqrt{(d-\lambda)^2 + 4\lambda)}}{2}\right).$$

Thus, if $\sqrt{(d-\lambda)^2+4\lambda} \in \mathbb{F}_q^*$ then there exists $\alpha \in \mathbb{F}_q^*$ such that the eigenvalues of $g_\lambda$ are $\{1, x\}$ for some $x \in \mathbb{F}_q^*$. This implies that $g_\lambda$ is contained in the same conjugacy class as $d_x$ (see Section 2.4). Here, we assume that $d_x$ with $x = 1$ corresponds to the element $u \in PGL(2,q)$ defined in Section 2.4.

For a fixed $d \in \mathbb{F}_q^* \setminus \{1\}$ and $x \in \mathbb{F}_q^*$ we want to know for how many $\lambda \in \mathbb{F}_q^*$ there exists some $\alpha$ such that $g_\lambda$ has eigenvalues $\{1, x\}$. From the above analysis it is clear that $d, x, \alpha$ and $\lambda$ must satisfy the equation below:

$$p_\lambda(t) = t^2 - \alpha(d-\lambda)t - \alpha^2\lambda = (t-x)(t-1) = t^2 - (x+1)t + x.$$

This implies that $\alpha$ satisfies the following quadratic equation,

$$d\alpha^2 - (x+1)\alpha + x = 0. \tag{5.10}$$

Therefore, given $x \in \mathbb{F}_q^*$ and $d \in \mathbb{F}_q^* \setminus \{1\}$, the number of values of $\lambda \in \mathbb{F}_q^*$ such that $g_\lambda$ is conjugate to $d_x$ is equal to

$$1 + \phi((x+1)^2 - 4xd) \text{ if } x \neq -1 \quad \text{and} \quad (1 + \phi((x+1)^2 - 4xd))/2 \text{ if } x = -1.$$

Furthermore, it is important to note that every element $g_\lambda$ having eigenvalues $\{1, x\}$ also has eigenvalues $\{1, x^{-1}\}$. Hence, given $d \in \mathbb{F}_q^* \setminus \{1\}$, the elements $x$ and $x^{-1}$ are related to the same values of $\lambda$. Now using the above remarks and the character table of $PGL(2,q)$ we get,

$$\begin{aligned}
\sum_{0^g=\infty, 1^g=d} \nu_\gamma(g) &= (1+\phi(1-d))\gamma(1) + \left(\frac{1+\phi(d)}{2}\right)(2\gamma(-1)) \\
&\quad + \frac{1}{2} \sum_{\substack{x \neq 1,-1 \\ x \in \mathbb{F}_q^*}} (1 + \phi((x+1)^2 - 4xd))(\gamma(x) + \gamma(x^{-1})) \\
&= \sum_{x \in \mathbb{F}_q^*} \gamma(x)\phi(x^2 - 2(2d-1)x + 1) \\
&= qP_\gamma(2d-1).
\end{aligned}$$

Finally, applying basic properties of characters and Lemma 29 we obtain

$$\sum_{0^g=\infty, 1^g=d} \nu_\gamma(g^{-1}) = \overline{\sum_{0^g=\infty, 1^g=d} \nu_\gamma(g)} = qP_{\gamma^{-1}}(2d-1) = qP_\gamma(2d-1).$$

□

**Lemma 59.** *For every $\beta \in B$ and $d \in \mathbb{F}_q^* \setminus \{1\}$ we have,*

$$\sum_{0^g=\infty, 1^g=d} \eta_\beta(g^{-1}) = -qR_\beta(2d-1).$$

*Proof.* Recall that the elements in $PGL(2,q)$ sending 0 to $\infty$ and 1 to $d$ all take the form,

$$g_\lambda = \begin{pmatrix} 0 & \alpha\lambda \\ \alpha & \alpha(d-\lambda) \end{pmatrix} \quad \text{with } \lambda, \alpha \in \mathbb{F}_q^*.$$

To evaluate the sum in this lemma we have to know to which conjugacy classes these elements belong. However, since $\eta_\beta(g) = 0$ if $g$ has two fixed points, we will pay attention to derangements and the elements fixing one point only (see Section 2.4).

We know that if $r \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ is an eigenvalue of $g_\lambda$ then $g_\lambda$ is a derangement with eigenvalues $\{r, r^q\}$ contained in the same conjugacy class as $v_r$. On the other hand, if $r \in \mathbb{F}_q^*$ is the only eigenvalue of $g_\lambda$ then this implies that $g_\lambda$ has exactly one fixed point and it is conjugated to $u$. In fact, when $r \in \mathbb{F}_q^*$ every element of the form $v_r$ is conjugated to $u$.

Fix $r \in \mathbb{F}_{q^2}^*$. We want to know for how many values of $\lambda \in \mathbb{F}_q^*$ there exists $\alpha$ such that $g_\lambda$ has eigenvalues $\{r, r^q\}$. From the characteristic polynomial of $g_\lambda$ the following equation is obtained

$$t^2 - \alpha(d - \lambda)t - \alpha^2\lambda = t^2 - (r + r^q)t + r^{q+1},$$

which implies that $\alpha \in \mathbb{F}_q^*$ must satisfy the quadratic equation below

$$d\alpha^2 - (r + r^q)\alpha + r^{q+1} = 0. \tag{5.11}$$

Distinct solutions of (5.11) generate distinct values of $\lambda$ unless $r \in i\mathbb{F}_q$ where $i$ is an element of $\mathbb{F}_{q^2}^*$ satisfying that $i^2 \in \mathbb{F}_q^*$. Hence, given $r \in \mathbb{F}_{q^2}^*$ and $d \in \mathbb{F}_q^* \setminus \{1\}$, the number of $\lambda \in \mathbb{F}_q^*$ such that $g_\lambda$ is conjugated to $v_r$ is equal to:

$$1 + \phi((r + r^q)^2 - 4dr^{q+1}) \text{ if } r \in \mathbb{F}_{q^2}^* \setminus i\mathbb{F}_q^* \quad \text{and} \quad (1 + \phi((r + r^q)^2 - 4dr^{q+1}))/2 \text{ if } r \in i\mathbb{F}_q^*.$$

Moreover, note that every element $g_\lambda$ having eigenvalues $\{r, r^q\}$ also has eigenvalues $\{ar, (ar)^q\}$ for any $a \in \mathbb{F}_q^*$. Thus, $r$ and $ar$ are related to the same value of $\lambda$ for

every $a \in \mathbb{F}_q$. Therefore,

$$\begin{aligned}\sum_{0^g=\infty,1^g=d} \eta_\beta(g^{-1}) &= \frac{1}{q-1}\sum_{r\in\mathbb{F}_q^*}(1+\phi((r+r^q)^2-4dr^{q+1}))(-\beta(1)) \\ &+\frac{1}{q-1}\sum_{r\in i\mathbb{F}_q^*}\left(\frac{1+\phi((r+r^q)^2-4dr^{q+1})}{2}\right)(-2\beta(i)) \\ &+\frac{1}{2(q-1)}\sum_{r\in\mathbb{F}_{q^2}^*\setminus\{\mathbb{F}_q^*,i\mathbb{F}_q^*\}}(1+\phi((r+r^q)^2-4dr^{q+1}))(-\beta(r)-\beta(r^q)) \\ &= -\frac{1}{q-1}\sum_{r\in\mathbb{F}_{q^2}^*}\phi((r+r^q)^2-4dr^{q+1}))\beta(r)\end{aligned}$$

Now, the lemma follows from Definition 25.

□

**Lemma 60.** *For every $d \in \mathbb{F}_q^* \setminus \{1\}$ we have,*

$$\sum_{0^g=\infty,1^g=d} \psi_{-1}(g) = qP_\phi(2d-1).$$

*Proof.* From the character table of $PGL(2,q)$ it follows that,

$$\psi_{-1}(g) = \begin{cases} 0 & \text{if } g \in u \\ 1 & \text{if } g \in d_x \text{ and } d_x \subset PSL(2,q) \\ -1 & \text{if } g \in d_x \text{ and } d_x \subset PGL(2,q)\setminus PSL(2,q) \\ -1 & \text{if } g \in v_r \text{ and } v_r \subset PSL(2,q) \\ 1 & \text{if } g \in v_r \text{ and } v_r \subset PGL(2,q)\setminus PSL(2,q) \end{cases} \tag{5.12}$$

Thus, to evaluate the sum $\sum_g \psi_{-1}(g)$ we need to know: how many elements sending 0 to $\infty$ and 1 to $d$ belong to each of the five categories considered in (5.12). In fact, these counting problems follow from the proof of Case (4) of Lemma 49.

For the sake of clarity, we recall some simple facts. There are $q-1$ elements in $PGL(2,q)$ sending 0 to $\infty$ and 1 to $d$, and half of them are in $PSL(2,q)$. It was proved by Meagher and Spiga [45] that if $1-d$ is a square in $\mathbb{F}_q^*$ then $(q-1)/2$ of these elements are derangements. On the other hand, if $1-d$ is not a square then $(q+1)/2$ of these elements are derangements.

First, assume that $1-d$ is a square. We can divide the $(q-1)/2$ elements of $PSL(2,q)$ sending 0 to $\infty$ and 1 to $d$ into three categories:

- 2 fix just one point.
- $\frac{1}{4}\sum_{x\in\mathbb{F}_q^*, x\neq 1,-1}(1+\phi((x+x^{-1})^2-4d))$ fix exactly two points.
- $\frac{q-5}{4}-\frac{1}{4}\sum_{x\in\mathbb{F}_q^*}\phi((x+x^{-1})^2-4d))$ are derangements.

A similar analysis can be carried out when $1-d$ is not a square. Specifically, from the $(q-1)/2$ elements of $PSL(2,q)$ sending 0 to $\infty$ and 1 to $d$,

- There are no elements fixing exactly one point.
- $\frac{1}{4}\sum_{x\in\mathbb{F}_q^*, x\neq 1,-1}(1+\phi((x+x^{-1})^2-4d))$ fix two points.
- $\frac{q-1}{4}-\frac{1}{4}\sum_{x\in\mathbb{F}_q^*}\phi((x+x^{-1})^2-4d))$ are derangements.

Putting all the above remarks together and assuming that $1-d$ is a square we obtain,

$$\begin{aligned}
\sum_{0^g=\infty, 1^g=d}\psi_{-1}(g) &= \frac{1}{4}\sum_{x\in\mathbb{F}_q^*, x\neq 1,-1}(1+\phi((x+x^{-1})^2-4d)) \\
&\quad -\left(\frac{q-1}{2}-2-\frac{1}{4}\sum_{x\in\mathbb{F}_q^*, x\neq 1,-1}(1+\phi((x+x^{-1})^2-4d))\right) \\
&\quad -\left(\frac{q-5}{4}-\frac{1}{4}\sum_{x\in\mathbb{F}_q^*}\phi((x+x^{-1})^2-4d))\right) \\
&\quad +\left(\frac{q-1}{2}-\frac{q-5}{4}+\frac{1}{4}\sum_{x\in\mathbb{F}_q^*}\phi((x+x^{-1})^2-4d))\right) \\
&= 2+\sum_{x\in\mathbb{F}_q^*}\phi((x+x^{-1})^2-4d) \\
&= 2+\sum_{x\in\mathbb{F}_q^*}\phi(x^2-2(2d-1)x+1)(1+\phi(x)) \\
&= qP_\phi(2d-1).
\end{aligned}$$

The case when $(1-d)$ is not a square follows from similar computations. □

## 5.3 The Restriction of $T_N$ onto $V_{\psi_{-1}}$, $V_{\nu_\gamma}$ and $V_{\eta_\beta}$

In this section, we study the restriction of $T_N$ onto the irreducible constituents, $V_{\psi_{-1}}$, $\{V_{\nu_\gamma}\}_{\gamma\in A}$ and $\{V_{\eta_\beta}\}_{\beta\in B}$, of $V$. From Schur's Lemma we know that the restriction of $T_N$ onto any irreducible module is an isomorphism or the zero map. The next theorem shows that the restriction of $T_N$ onto $V_{\eta_\beta}$ is a $PGL(2,q)$-module isomorphism for every $\beta \in B$. To ease the notation, in this section we will denote by $\|\cdot\|$ and $\langle\cdot,\cdot\rangle$ the norm and inner product in $\ell_2(\mathbb{F}_q, m)$, respectively.

For the proofs below, we will need the following function in $\ell^2(\mathbb{F}_q, m)$,

$$\begin{array}{rccc} f: & \mathbb{F}_q & \to & \mathbb{C} \\ & x & \mapsto & \phi(1-x)P_\phi(x) \end{array}.$$

Note that the norm of $f$ is closely related to the norm of $P_\phi$,

$$\|f\|^2 = \sum_{x\in\mathbb{F}_q} f(x)^2 m(x) = \sum_{\substack{x\in\mathbb{F}_q \\ x\neq 1}} P_\phi(x)^2 m(x) = \|P_\phi\|^2 - \frac{q+1}{q^2} = 1 - \frac{1}{q} - \frac{2}{q^2},$$

where we have used Lemma 26 to obtain the last equality.

**Theorem 61.** *For every $\beta \in B$ we have*

$$T_N(V_{\eta_\beta}) \cong V_{\eta_\beta}.$$

*Proof.* It suffices to show that $T_{N,\eta_\beta} \neq 0$ for all $\beta \in B$. Using (5.3), Lemma 56, 57 and 59, and after some computations the following expression for $T_{N,\eta_\beta}$ is obtained:

$$T_{N,\eta_\beta} = \frac{(q-1)}{4}\left[q^2 + q + (q+1)\,\beta(i)\phi(-1) + q^2 \sum_{b\in\mathbb{F}_q^*, b\neq 1} R_\beta(2b^h - 1)P_\phi(2b-1)\right], \tag{5.13}$$

where $i \in \mathbb{F}_{q^2}^*$ such that $i^2 \in \mathbb{F}_q^*$. We will show that the expression on the right hand side of (5.13) is not equal to zero.

We claim that the character sum

$$\sum_{b\in\mathbb{F}_q^*, b\neq 1} R_\beta(2b^h - 1)P_\phi(2b-1) \tag{5.14}$$

can be expressed in terms of the function $f$. Recall that $h$ is the unique element in $PGL(2,q)$ sending 0 to 0, 1 to $\infty$ and $\infty$ to 1. Hence, if $b \in \mathbb{F}_q^*$ and $b \neq 1$ then $b^h \neq 0, 1, \infty$. Moreover, we have the following formula for $b^h$ when $b \in \mathbb{F}_q^*$ and $b \neq 1$,

$$b^h = \frac{b}{b-1}$$

which implies that $(b^h)^h = b$ for any $b \in \mathbb{F}_q$. Thus, we can rewrite the sum in (5.14) as,

$$\sum_{b \in \mathbb{F}_q^*, b \neq 1} R_\beta(2b^h - 1) P_\phi(2b-1) = \sum_{b \in \mathbb{F}_q^*, b \neq 1} P_\phi(2b^h - 1) R_\beta(2b-1).$$

Using the relation between Legendre sums and hypergeometric sums given by Lemma 30 and the transformation formula in Lemma 21, the following expression for $P_\phi(2b^h - 1)$ is obtained

$$P_\phi(2b^h - 1) = {}_2\mathbb{F}_1 \left[ \begin{matrix} \phi & \phi \\ & \epsilon \end{matrix} ; \frac{1}{1-b}; q \right] = \phi(1-b) {}_2\mathbb{F}_1 \left[ \begin{matrix} \phi & \phi \\ & \epsilon \end{matrix} ; 1-b; q \right] = \phi(1-b) P_\phi(2b-1),$$

for $b \in \mathbb{F}_q$, $b \neq 0, 1$. Putting all the above remarks together we conclude that

$$\begin{aligned} \sum_{b \in \mathbb{F}_q^*, b \neq 1} R_\beta(2b^h - 1) P_\phi(2b-1) &= \sum_{b \in \mathbb{F}_q^*, b \neq 1} \phi(1-b) P_\phi(2b-1) R_\beta(2b-1) \\ &= \phi(2) \sum_{x \in \mathbb{F}_q, x \neq \pm 1} \phi(1-x) P_\phi(x) R_\beta(x) \\ &= \phi(2) \left(1 + \frac{1}{q}\right)^{1/2} \langle f, R'_\beta \rangle - (q+1) \frac{\beta(i)\phi(-1)}{q^2} \end{aligned}$$

where $i$ is an element of $\mathbb{F}_{q^2}^*$ such that $i^2 \in \mathbb{F}_q^*$.

Therefore, combining the above expression for (5.14) and (5.13), we can also express $T_{N,\eta_\beta}$ in terms of the function $f$,

$$T_{N,\eta_\beta} = \frac{q^2(q-1)}{4} \left[ 1 + \frac{1}{q} + \phi(2) \left(1 + \frac{1}{q}\right)^{1/2} \langle f, R'_\beta \rangle \right]. \tag{5.15}$$

Recall that $\{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in A, \beta \in B\}$ is an orthonormal basis of $\ell^2(\mathbb{F}_q, m)$. Thus, we can write $f$ in terms of this orthonormal basis,

$$f = \langle f, P'_\epsilon \rangle P'_\epsilon + \langle f, P'_\phi \rangle P'_\phi + \sum_\gamma \langle f, P'_\gamma \rangle P'_\gamma + \sum_\beta \langle f, R'_\beta \rangle R'_\beta.$$

and also the squared norm of $f$,

$$\|f\|^2 = \langle f, P'_\epsilon\rangle^2 + \langle f, P'_\phi\rangle^2 + \sum_\gamma \langle f, P'_\gamma\rangle^2 + \sum_\beta \langle f, R'_\beta\rangle^2.$$

where we have used the fact the coefficients in the expansion of $f$ are all real (cf. Lemma 29).

On the other hand, we know that the squared norm of $f$ is $1 - 1/q - 2/q^2$. This implies that the square of every coefficient of the form $\langle f, g\rangle$ is less than 1 for all $g \in \{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \ \gamma \in A, \beta \in B\}$. In particular, $\langle f, R'_\beta\rangle^2 \leq 1 - 1/q - 2/q^2$ for all $\beta \in B$. This together with (5.15) proves this theorem. □

Unfortunately, the argument used in the proof of Theorem 61 cannot be applied to show that the restriction of $T_N$ onto the irreducible module $V_{\psi_{-1}}$ is a $PGL(2,q)$-module isomorphism. To deal with this case we exploit the connection between Legendre sums and Hypergeometric sums shown by Kable in [34].

**Lemma 62.** *Let $\gamma$ be a nontrivial multiplicative character of $\mathbb{F}_q$. Then*

$$\phi(2)q^2\langle f, P_\gamma\rangle = q^3\, {}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & & & \\ & \epsilon & \epsilon & \epsilon\end{matrix}; \ 1; q\right] + \phi(-1)\gamma(-1)q.$$

*Proof.* Applying Lemma 20 and 30 we obtain,

$$\begin{aligned}
\phi(2)q^2\langle f, P_\gamma\rangle &= \phi(2)q^2 \sum_{\substack{x\in\mathbb{F}_q \\ x\neq\pm 1}} \phi(1-x)P_\phi(x)P_\gamma(x) + q^2 P_\phi(-1)P_\gamma(-1)m(-1) \\
&= q^2 \sum_{\substack{y\in\mathbb{F}_q^* \\ y\neq 1}} \phi(y)\, {}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \\ & \epsilon\end{matrix}; \ y; q\right] {}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \\ & \epsilon\end{matrix}; \ y; q\right] + \phi(-1)\gamma(-1)(q+1) \\
&= q^2 \sum_{y\in\mathbb{F}_q} \phi(y)\, {}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \\ & \epsilon\end{matrix}; \ y; q\right] {}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \\ & \epsilon\end{matrix}; \ y; q\right] + \phi(-1)\gamma(-1)q \\
&= q^3\, {}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & & & \\ & \epsilon & \epsilon & \epsilon\end{matrix}; \ 1; q\right] + \phi(-1)\gamma(-1)q.
\end{aligned}$$

□

**Theorem 63.** *If $q \geq 7$ then,*

$$T_N(V_{\psi_{-1}}) \cong V_{\psi_{-1}}.$$

*Proof.* It suffices to show that $T_{N,\psi_{-1}} \neq 0$. Using (5.3), Lemma 56, 57 and 60, and after some computations we get

$$T_{N,\psi_{-1}} = \frac{(q-1)}{4}\left[q^2 - 2q - 3 - q^2 \sum_{b\in\mathbb{F}_q^*, b\neq 1} P_\phi(2b^h - 1)P_\phi(2b-1)\right].$$

Let $f$ be the function in $\ell^2(\mathbb{F}_q, m)$ defined before the statement of Theorem 61. By Lemma 21 and 30 we see that the sum

$$\sum_{b\in\mathbb{F}_q^*, b\neq 1} P_\phi(2b^h - 1)P_\phi(2b-1)$$

can be written in terms of the function $f$. In particular,

$$\begin{aligned}
\sum_{b\in\mathbb{F}_q^*, b\neq 1} P_\phi(2b^h - 1)P_\phi(2b-1) &= \sum_{b\in\mathbb{F}_q^*, b\neq 1} \phi(1-b)P_\phi(2b-1)P_\phi(2b-1) \\
&= \phi(2) \sum_{x\in\mathbb{F}_q, x\neq\pm 1} \phi(1-x)P_\phi(x)P_\phi(x) \\
&= \phi(2)\langle f, P_\phi\rangle - \frac{q+1}{q^2}.
\end{aligned}$$

Thus, $T_{N,\psi_{-1}}$ can be expressed in terms of $f$:

$$T_{N,\psi_{-1}} = \frac{(q-1)}{4}\left[q^2 - q - 2 - \phi(2)q^2\langle f, P_\phi\rangle\right]. \tag{5.16}$$

We claim that $\phi(2)q^2\langle f, P_\phi\rangle \leq 2q^{3/2}$. This claim together with (5.16) immediately implies that $T_{N,\psi_{-1}} \neq 0$ for every $q \geq 7$.

To prove our claim we note that the character sum $\phi(2)q^2\langle f, P_\phi\rangle$ can be written in terms of a hypergeometric sum ${}_4\mathbb{F}_3$. Letting $\gamma = \phi$ in Lemma 62,

$$\phi(2)q^2\langle f, P_\phi\rangle = q^3\, {}_4\mathbb{F}_3\left[\begin{matrix}\phi & \phi & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix}; 1; q\right] + q.$$

Therefore, our claim follows directly from the final conclusion of Proposition 23. □

To study the restriction of $T_N$ onto $V_{\nu_\gamma}$ we consider two cases. First, if $\gamma$ is a character whose order is not equal to three, four or six then we can apply arguments similar to the ones used in the proof of Theorem 61 to prove that the restriction is an isomorphism. On the other hand, different ideas have to be used to show that the same result holds when $\gamma$ has order three, four or six. The next two theorems deal with these cases.

**Theorem 64.** *Assume that $q \geq 11$. If $\gamma \in A$ then*

$$T_N(V_{\nu_\gamma}) \cong V_{\nu_\gamma}.$$

*Proof.* We proceed as we did in the proof of Theorem 61. To prove this theorem it is enough to show that $T_{N,\nu_\gamma} \neq 0$.

From (5.3), Lemmas 56, 57 and 58, and after some computations the following expression for $T_{N,\nu_\gamma}$ is obtained:

$$T_{N,\nu_\gamma} = \frac{(q-1)}{4}\left[q^2 - 3q - (q+1)\,\gamma(-1)\phi(-1) - q^2 \sum_{b\in\mathbb{F}_q^*, b\neq 1} P_\gamma(2b^h-1)P_\phi(2b-1)\right].$$

Applying Lemma 21 and 30 it is possible to write the sum of products of Legendre sums in terms of the function $f$. In fact,

$$\sum_{b\in\mathbb{F}_q^*, b\neq 1} P_\gamma(2b^h-1)P_\phi(2b-1) \;=\; \phi(2)\left(1-\frac{1}{q}\right)^{1/2}\langle f, P'_\gamma\rangle - (q+1)\frac{\gamma(-1)\phi(-1)}{q^2}.$$

Therefore, for every $\gamma \in \Gamma$ we have

$$T_{N,\nu_\gamma} = \frac{q^2(q-1)}{4}\left[1 - \frac{3}{q} - \phi(2)\left(1-\frac{1}{q}\right)^{1/2}\langle f, P'_\gamma\rangle\right]. \tag{5.17}$$

Recall that

$$\|f\|^2 = \langle f, P'_\epsilon\rangle^2 + \langle f, P'_\phi\rangle^2 + \sum_\gamma \langle f, P_\gamma\rangle^2 + \sum_\beta \langle f, R'_\beta\rangle^2 = 1 - \frac{1}{q} - \frac{2}{q^2}. \tag{5.18}$$

where $\{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in A, \beta \in B\}$ is an orthonormal basis of $\ell^2(\mathbb{F}_q, m)$. Equation (5.18) implies that at most one of the coefficients $\langle f, g\rangle$ with $g \in \{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in$

$A, \beta \in B\}$ can be close to 1. On the other hand, it is clear from (5.17) that $T_{N,\nu_\gamma} = 0$ if and only if the coefficient $\langle f, P'_\gamma \rangle$ is close to 1.

To prove the theorem we proceed by contradiction. Assume that there exists $\gamma \in A$ such that $T_{N,\nu_\gamma} = 0$. Hence, it follows from equation (5.17) that

$$\langle f, P'_\gamma \rangle^2 = 1 - \frac{5}{q} + \frac{4}{q(q-1)}. \tag{5.19}$$

Let $\mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$ be the Galois group where $\zeta_{q-1}$ is a primitive $(q-1)$-th root of the unity. If $\gamma$ is a nontrivial character whose order is not equal to three, four or six, there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$ such that $\gamma^\sigma \neq \gamma$ and $\gamma^\sigma \neq \gamma^{-1}$. Now, applying the Galois automorphism $\sigma$ to both sides of (5.19) we conclude that

$$\begin{aligned} \sigma\left(\langle f, P'_\gamma \rangle^2\right) &= \sigma\left(1 - \frac{5}{q} + \frac{4}{q(q-1)}\right) \\ \langle f, P'_{\gamma^\sigma} \rangle^2 &= 1 - \frac{5}{q} + \frac{4}{q(q-1)}. \end{aligned}$$

Thus, $\langle f, P'_\gamma \rangle^2$ and $\langle f, P'_{\gamma^\sigma} \rangle^2$ are equal to $1 - \frac{5}{q} + \frac{4}{q(q-1)}$ which is a contradiction because at most one of the coefficients $\langle f, g \rangle$ with $g \in \{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \ \gamma \in A, \beta \in B\}$ can be close to 1. Assume now $\gamma \in A$ is a character of order 3, 4 or 6. From equation (5.17) we get the following expression for $T_{N,\nu_\gamma}$,

$$T_{N,\nu_\gamma} = \frac{(q-1)}{4}\left[q^2 - 3q - \phi(2)q^2\langle f, P_\gamma \rangle\right].$$

By Lemma 62, $\phi(2)q^2\langle f, P_\gamma \rangle = q^3\, {}_4\mathbb{F}_3\left[\begin{matrix} \gamma & \gamma^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon \end{matrix}; 1; q\right] + \phi(-1)\gamma(-1)q$. By the final conclusion of Proposition 23, $T_{N\nu_\gamma} \neq 0$.

□

Finally, we are ready to prove Theorem 47.

*Proof of Theorem 47.* Recall that in Section 5.1.3 we proved the following lower and upper bounds on the rank of the derangement matrix $M$ of $PSL(2,q)$ acting on $PG(1,q)$,

$$\sum_{\{\chi:\ T_{N,\chi} \neq 0\}} \dim(V_\chi) \leq \mathrm{rank}(M) \leq q(q-1). \tag{5.20}$$

These bounds imply that if $T_{N,\chi}$ is not zero for every $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$ then the rank of $M$ is $q(q-1)$.

If $q \geq 11$ then it follows from Theorems 61, 63 and 64 that $T_{N,\chi} \neq 0$ for all $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in A}\}$. Furthermore, for every $q \leq 11$ computational experiments have shown that the rank of $M$ is exactly $q(q-1)$. □

# Chapter 6

# THE RANK RESILIENCE PROPERTY OF $W_{r,s}$

Recall that $W_{r,s}$ denotes the higher inclusion matrix of $r$-subsets vs. $s$-subsets. In this chapter we present some results about the rank of the matrices $W_{r,s}$ over fields of various characteristics. We also discuss some of the proof techniques that have been applied to obtain those results. Moreover, we prove that the rank of $W_{r,s}$ is resilient over any field $K$. This result is a generalization of Theorem 5 proved by Keevash. In fact, the next theorem shows that if the size of $\mathcal{F}$ is close to $\binom{n}{r}$ then $\text{rank}_K(W_{r,s}) = \text{rank}_K(W_{r,s}^{\mathcal{F}})$. To simplify notation, for any family $\mathcal{F}$ of $r$-subsets we denote by $\mathcal{F}^c$ the family of $r$-subsets $\binom{[n]}{r} \setminus \mathcal{F}$.

**Theorem 65.** *Assume that $0 \leq s < r \leq n/2$. Let $\mathcal{F}$ be a family of $r$-subsets of $[n]$. If $|\mathcal{F}^c| \leq \frac{n}{r} - 1$ then $rank_K(W_{r,s}) = rank_K(W_{r,s}^{\mathcal{F}})$.*

## 6.1 The Rank of $W_{r,s}$

The ranks of the inclusion matrices $W_{r,s}$ have been extensively studied. It was proved by Gottlieb [27] that the matrix $W_{r,s}$ has full rank over $\mathbb{Q}$. Later, Linial and Rothschild [42] computed the rank of $W_{r,s}$ over any field $K$ of characteristic 2. Finally, Wilson [58] found a beautiful formula for the rank of $W_{r,s}$ over any field $K$ when $n \geq r + s$. The formula is given by

$$\text{rank}_K(W_{r,s}) = \sum_{j \in Y} \binom{n}{j} - \binom{n}{j-1},$$

where $Y = \{j : 0 \leq j \leq s, \binom{r-j}{s-j} \neq_K 0\}$. This formula was also proven by Frankl [20], Bier [9] and Frumkin and Yakir [23] using different ideas.

In this section we discuss Bier's proof of Wilson's rank formula for $W_{r,s}$. The main idea of Bier is to find bases with respect to which the matrix $W_{r,s}$ becomes diagonal. In fact, once we have a diagonal form for $W_{r,s}$ the computation of its rank becomes trivial.

Let $K$ be an arbitrary field. For every $0 \leq r \leq n$, we denote by $M^r$ the $K$-vector space spanned by the $r$-subsets of $[n]$. Hence, the set of $r$-subsets of $[n]$ forms a "canonical basis" of $M^r$. Let $\varphi_{j,r} : M^j \to M^r$ be the linear transformation such that, for every $j$-subset $A$ of $[n]$,

$$\varphi_{j,r}(A) = \sum_{A \subseteq R} R,$$

where the sum is over all $r$-subsets containing $A$. Note that $W_{r,j}$ is the matrix associated with $\varphi_{j,r}$ with respect to the canonical basis of $M^j$ and $M^r$.

For any $j$-subset $A$ of $[n]$, with $0 \leq j \leq r$, we denote by $\langle A \rangle_r$ the image of $A$ under the linear transformation $\varphi_{j,r}$. In [20], Frankl introduced the notion of rank for a subset of $[n]$.

**Definition 66.** (Frankl, [20]) Let $A$ be any subset of $[n]$. One associates a walk $w(A)$ with $A$ on the $x$-$y$ plane. The walk $w(A)$ goes from the origin to $(n-|A|, |A|)$ by steps of length one, the $i$-th step to the right or up according as $i \notin A$ or $i \in A$ holds. The *rank* of $A$, denoted by $rk(A)$, is defined as $|A| - l$ where $l$ is the largest integer such that $w(A)$ reaches the line $y = x + l$.

From the above definition, it follows that if $A$ is a $j$-subset then its rank is at most $\min(j, n-j)$. For every $0 \leq j \leq n/2$, we define

$$S(j) = \left\{ A \in \binom{[n]}{j} : rk(A) = j \right\}.$$

Note that the elements of $S(j)$ are in one to one correspondence with the standard tableaux of shape $(n-j, j)$. In fact, in [20] it was proved that $|S(j)| = \binom{n}{j} - \binom{n}{j-1}$. Therefore, for every $r \leq n/2$ we have that $|\cup_{j=0}^{r} S(j)| = \binom{n}{r}$ which is precisely the dimension of the vector space $M^r$.

The following theorem gives a basis of $M^r$ indexed by the elements of $S(j)$ with $j$ from 0 to $r$.

**Theorem 67.** *(Bier, [9]) Let $0 \leq r \leq n/2$. The vectors $\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq r\}$ form a $K$-basis for $M^r$.*

We will refer to the basis given by Theorem 67 as the Bier basis of $M^r$. For the sake of completeness we explain in detail Bier's proof of Theorem 67 and later we show that the condition $r \leq n/2$ can be removed. The next lemma will be used in the proof of Theorem 67.

**Lemma 68.** *(Bier, [9]) Let $r$ be a positive integer. For any set $j$-subset $A$ of $[n]$ with $j < r$,*

$$\binom{r-j}{l}\langle A\rangle_r + \sum_{i=1}^{l}(-1)^i\binom{r-j-i}{l-i}\sum_{T_i}\langle T_i\rangle_r = 0 \quad \text{for all } l = 1,\ldots,r-j \tag{6.1}$$

*where the inner sum is taken over all $T_i$ with $|T_i| = j+i$ and $A \subset T_i$.*

*Proof.* Let $R$ be a $r$-subset containing $A$. In the first term of equation (6.1), $R$ appears $\binom{r-j}{l}$ times. Moreover, in each sum $\sum\langle T_i\rangle_r$ the set $R$ appears $\binom{r-j}{i}$ times. Therefore, $R$ appears in the left hand side of equation (6.1) exactly,

$$\binom{r-j}{l} + \sum_{i=1}^{l}(-1)^i\binom{r-j-i}{l-i}\binom{r-j}{i} = \sum_{i=0}^{l}(-1)^i\binom{r-j}{i}\binom{r-j-i}{l-i}$$

which is equal to 0 by the principle of inclusion-exclusion. □

*Proof of Theorem 67.* To prove this theorem we will show that,

$$\text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\} = \text{span}_K\{\langle A\rangle_r : A \text{ a } j\text{-subset of } [n], \text{ for } 0 \leq j \leq t\} \tag{6.2}$$

for any $0 \leq t \leq r$. This is enough because taking $t = r$ we conclude that the set of vectors in the left hand side of (6.2) span $M^r$ and because $|\cup_{j=0}^{r} S(j)| = \binom{n}{r}$, they form a basis.

We prove equation (6.2) by induction. Let's start with some definitions that we will use. For any set $A = \{a_1 < \ldots < a_j\}$ with $r(A) < |A|$, there exists a unique integer $m = m_A$, $1 \leq m \leq j$ such that $a_m < 2m$ and $a_i \geq 2i$ for all $i > m$. On the other hand, if $r(A) = |A|$ then $a_i \geq 2i$ for all $i$, so $m = m_A = 0$.

To prove (6.2), first note that $\text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$ is clearly contained in $\text{span}_K\{\langle A\rangle_r : A \text{ a } j\text{-subset of } [n], \text{ for } 0 \leq j \leq t\}$, hence it is enough to prove the assertion in the opposite direction. We will show that,

$$\text{span}_K\{\langle A\rangle_r : A \text{ a } j\text{-subset of } [n], \text{ for } 0 \leq j \leq s\} \leq \text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\} \tag{6.3}$$

for every $s$ from 0 to $t$.

We proceed to prove (6.3) by induction on $s$ and in the parameter $m$ of a subset defined above. Notice that,

- The assertion is trivially true for $s = 0$.
- Assume that for $0 < s < t$ we have:
  1. $\langle B\rangle_r \in \text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$, for all $B, |B| < s$.
  2. $\langle B\rangle_r \in \text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$, for all $B, |B| = s$ and $m_B < m$.

We can assume number 2 because for a $s$-subset $B$ with $m_B = 0$ it is trivial to notice that $\langle B\rangle_r \in \text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$ (actually, in this case $B \in S(j)$).

Hence, we want to show that for every set $B$ with $|B| = s$ and $m_B = m$ we have that $\langle B\rangle_r \in \text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$.

Let $B = I \cup X$ with

$$I = \{b_1 < b_2 < \ldots < b_m\} \text{ and } X = \{b_{m+1} < \ldots < b_s\}$$

such that $b_m < 2m$ and $b_i \geq 2i$ for all $b_i \in X$ (so $|B| = s$ and $m_B = m$). For any $U \subseteq I$ we define,

$$[U \cup X] = \sum_{U \subseteq J} \langle J \cup X\rangle_r$$

where the sum is taken over all sets $J = \{j_1 < j_2 < \ldots < j_m\}$ with $j_m < 2m$ containing the set $U$. Notice that $J \cup X$ is a $s$-subset with $m_{J\cup X} = m$.

**Claim 69.** *Let $U$ be a proper subset of $I$ then*

$$[U \cup X] \in span_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$$

*Proof.* We use lemma 68 with $A = U \cup X$ and $l = m - |U|$,

$$\begin{aligned}\binom{k-|U\cup X|}{l}\langle U\cup X\rangle_r + \sum_{i=1}^{l}(-1)^i\binom{k-|U\cup X|-i}{l-i}\sum_{T_i}\langle T_i\rangle_r &= 0\\ \sum_{i=0}^{l-1}(-1)^i\binom{k-|U\cup X|-i}{l-i}\sum_{T_i}\langle T_i\rangle_r + (-1)^l\sum_{T_l}\langle T_l\rangle_r &= 0\end{aligned}$$

The terms to the left of the above expression are contained in $\text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$ by induction hypothesis because the sets $T_i$ have cardinality lower than $s$. We can rewrite the term to the right as,

$$\sum_{T_l}\langle T_l\rangle_r = \sum_{T_l:m_{T_l}<m}\langle T_l\rangle_r + \sum_{T_l:m_{T_l}=m}\langle T_l\rangle_r$$

and again the term to the left belongs to $\text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \leq j \leq t\}$ by induction hypothesis. Now, because $[U \cup X] = \sum_{T_l:m_{T_l}=m}\langle T_l\rangle_r$, we conclude that,

$$[U\cup X] = \sum_{i=0}^{l-1}(-1)^{i+l+1}\binom{r-|U\cup X|-i}{l-i}\sum_{T_i}\langle T_i\rangle_k - \sum_{T_l:m_{T_l}<m}\langle T_l\rangle_k$$

□

**Claim 70.** *For any $I \subset \{1, 2, \ldots, 2m-1\}$ with $|I| = m$,*

$$\sum_{U\subseteq I}(-1)^{|U|}[U\cup X] = 0.$$

*Proof.* By definition we have,

$$\sum_{U\subseteq I}(-1)^{|U|}[U\cup X] = \sum_{U\subseteq I}(-1)^{|U|}\sum_{U\subseteq J}\langle J\cup X\rangle_r. \tag{6.4}$$

Consider any set $R \in \binom{[n]}{r}$. We want to count how many times the subset $R$ appears in the expression (6.4). We assume that $X \subseteq R$ and that $|R\cap\{1, 2, \ldots, 2m-1\}|$

is at least $m$, otherwise, $R$ does not appear in (6.4). Define $l_1 = |R \cap I|$ and $l_2 = |(R \setminus I) \cap \{1, \ldots, 2m-1\}|$, hence $R$ appears in (6.4), exactly,

$$\binom{l_1}{0}\binom{l_1+l_2}{m} - \binom{l_1}{1}\binom{l_1+l_2-1}{m-1} + \cdots = \sum_{i=0}^{m}(-1)^i\binom{l_1}{i}\binom{l_1+l_2-i}{m-i}$$

which is equal to 0 by the principle of inclusion-exclusion. □

From Claim 70 it follows that,

$$\langle B\rangle_r + \sum_{U\subset I}(-1)^{|J|}[U \cup X] = 0,$$

hence,

$$\langle B\rangle_r = [I \cup X] = (-1)^{m+1}\sum_{U\subset I}(-1)^{|U|}[U \cup X].$$

Therefore, using Claim 69 we have,

$$\langle B\rangle_r = \text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \le j \le t\}.$$

□

**Corollary 71.** *Let $0 \le r \le n$. The vectors $\{\langle A\rangle_r : A \in S(j), 0 \le j \le \min(n-r, r)\}$ form a $K$-basis for $M^r$.*

*Proof.* Assume $r > n/2$ because for $r \le n/2$ the corollary reduces to Theorem 67. We need to prove that,

$$\text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \le j \le n-r\} = M^r$$

Let $R$ be any $r$-subset of $[n]$. We claim that,

$$R = \sum_{U\subset R^c}(-1)^{|U|}\langle U\rangle_r \tag{6.5}$$

where $R^c$ is the complement of $R$ with respect to $[n]$. The set $R$ appears in the right hand side of equation (6.5) exactly once because the empty set is the only subset of $R^c$ that is also a subset of $R$. Any other $r$-subset $B$ appearing in the right side of equation

(6.5) satisfies that $|B \cap R^c| = l$ with $l = 1, \ldots, n-k$. Hence, the set $B$ appears in the right hand side of equation (6.5) exactly,

$$1 - \binom{l}{1} + \binom{l}{2} - \cdots + (-1)^l \binom{l}{l}$$

which is equal to 0. From equation (5.2), we know

$$\text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \le j \le n-r\} = \text{span}_K\{\langle A\rangle_r : A \text{ a } j\text{-subset of } [n], \text{ for } 0 \le j \le n-r\}$$

therefore, equation (6.5) implies that $R \in \text{span}_K\{\langle A\rangle_r : A \in S(j), 0 \le j \le n-r\}$. □

It follows from Corollary 71 that there is a Bier basis of $M^r$ for every $r$ from 0 to $n$.

### 6.2 Resilience Property

In this section we use the Bier bases to prove the resilience of the rank of the higher inclusion matrices $W_{r,s}$ over any field $K$.

By definition of $\varphi_{s,r}$, it is trivial to note that for $0 \le s \le r \le n/2$,

$$\varphi_{s,r}(\langle A\rangle_s) = \binom{r-j}{s-j}\langle A\rangle_r$$

for every $A \in S(j)$ with $j = 0, 1, \ldots, s$. Therefore, the matrix of $\varphi_{s,r}$ with respect to the Bier bases $\{\langle A\rangle_s : A \in S(j), 0 \le j \le s\}$ of $M^s$ and $\{\langle A\rangle_r : A \in S(j), 0 \le j \le r\}$ of $M^r$ has a diagonal form. This proves that $\dim_K(\text{im}(\varphi_{s,r}))$ is equal to,

$$\sum_{j \in Y} |S(j)| = \sum_{j \in Y} \binom{n}{j} - \binom{n}{j-1}$$

where $Y = \{j : 0 \le j \le s, \binom{r-j}{s-j} \neq_K 0\}$. This is precisely the $K$-rank formula given by Wilson for the matrix $W_{r,s}$ in [58].

Let $S_n$ denote the group of permutations of $[n]$. If $\sigma \in S_n$ then for any $r$-subset $A$ we define $\sigma(A) = \{\sigma(a) : a \in A\}$. In the same way, if $\mathcal{F}$ is a family of $r$-subsets then $\sigma(\mathcal{F}) = \{\sigma(A) : A \in \mathcal{F}\}$. The next lemma shows that we have a lot of freedom in the way we can remove rows from $W_{r,s}$ without affecting its $K$-rank.

**Lemma 72.** *Assume that $0 \leq s \leq r \leq n/2$. Let $\mathcal{F}$ be a family of $r$-subsets of $[n]$. If there exist some $\sigma \in S_n$ such that $\sigma(\mathcal{F}^c) \subseteq S(r)$ then $rank_K(W_{r,s}) = rank_K(W_{r,s}^{\mathcal{F}})$.*

*Proof.* First, assume $\mathcal{F}^c \subset S(r)$. We define the following linear transformation from $M^s$ to $M^r$

$$\varphi_{s,r}^{\mathcal{F}^c}(S) = \sum_{S \subset R} R - \sum_{T \in \mathcal{F}^c, S \subset T} T, \text{ for all } S \subset [n], |S| = s,$$

where in the first sum $R$ runs over all $r$-subsets of $[n]$ containing $S$, and in the second sum $T$ runs over all $r$-subsets of $[n]$ containing $S$ such that $T \in \mathcal{F}^c$. It is clear from its definition that $\dim_K(\text{im}\varphi_{s,r}^{\mathcal{F}^c}) = \text{rank}_K(W_{r,s}^{\mathcal{F}})$.

Note that for every $j$-subset $A$ with $0 \leq j \leq s$ and $\text{rank}(A) = j$ we have

$$\varphi_{s,r}^{\mathcal{F}^c}(\langle A \rangle_s) = \binom{r-j}{s-j} \langle A \rangle_r - \sum_{T \in \mathcal{F}^c, A \subset T} \binom{r-j}{s-j} T. \tag{6.6}$$

Recall that by assumption $\mathcal{F}^c \subseteq S(r)$, so any $T \in \mathcal{F}^c$ is actually a basis element of the Bier basis of $M^r$. Thus the matrix corresponding to $\varphi_{s,r}^{\mathcal{F}^c}$ with respect to the Bier bases of $M^r$ and $M^s$ is almost diagonal.

We will use the following simple result from linear algebra.

**Claim 73.** *Let $v_1, \ldots, v_m$ be linearly independent vectors of a $K$-vector space $V$. Let $z_1, \ldots, z_m$ be vectors in $V$ such that span$\{v_1, \ldots, v_m\} \cap$ span$\{z_1, \ldots, z_m\} = \{0\}$. Then $v_1 + z_1, \ldots, v_m + z_m$ are linearly independent vectors in $V$.*

Let $W$ be the subspace spanned by the following set of linearly independent vectors

$$\left\{ \binom{r-j}{s-j} \langle A \rangle_r : \ A \in S(j), j \in Y \right\}.$$

It is clear from the definition of the Bier basis of $M^r$ that

$$W \bigcap \text{span} \left\{ \sum_{T \in \mathcal{F}^c, A \subset T} \binom{r-j}{s-j} T : \ A \in S(j), j \in Y \right\} = \{0\}.$$

Therefore, by the above claim and equation (6.6) we conclude that the vectors

$$\bigcup_{j \in Y} \left\{ \varphi_{s,r}^{\mathcal{F}^c}(\langle A \rangle_s) : \ A \in S(j) \right\}$$

with $Y = \{j : 0 \leq j \leq s, \binom{r-j}{s-j} \neq_K 0\}$ are linearly independent. This implies that

$$\dim_K(\mathrm{im}\varphi_{s,r}^{\mathcal{F}^c}) \geq \sum_{i \in Y} \binom{n}{j} - \binom{n}{j-1}.$$

Hence, Lemma 72 follows from the trivial upper bound $\mathrm{rank}_K W_{r,s}^{\mathcal{F}} \leq \mathrm{rank}_K W_{r,s}$ and Wilson's rank formula.

Now, if $\mathcal{F}^c \nsubseteq S(r)$ then by assumption there exists $\sigma \in S_n$ such that $\sigma(\mathcal{F}^c) \subseteq S(r)$. We use $\sigma$ to define the following invertible linear transformations,

$$\begin{array}{rccc} \Phi_r^\sigma : & M^r & \to & M^r \\ & R & \mapsto & \sigma(R) \end{array}, \qquad \begin{array}{rccc} \Phi_s^\sigma : & M^s & \to & M^s \\ & S & \mapsto & \sigma(S) \end{array}.$$

From the above definitions it follows that

$$\varphi_{s,r}^{\mathcal{F}^c} = (\Phi_r^\sigma)^{-1} \circ \varphi_{s,r}^{\sigma(\mathcal{F}^c)} \circ \Phi_s^\sigma.$$

Thus, $\dim_K(\mathrm{im}\varphi_{s,r}^{\mathcal{F}^c}) = \dim_K(\mathrm{im}\varphi_{s,r}^{\sigma(\mathcal{F}^c)})$ which implies Lemma 72. □

The next corollary is an immediate consequence of Lemma 72.

**Corollary 74.** *Assume that $0 \leq s < r \leq n/2$. Let $\mathcal{F}$ be a family of $r$-subsets of $[n]$. If*

$$\left| \bigcup_{A \in \mathcal{F}^c} A \right| \leq n - r \tag{6.7}$$

*then $rank_K(W_{r,s}^{\mathcal{F}}) = rank_K(W_{r,s})$.*

*Proof.* First note that by definition, if an $r$-subset $A$ of $[n]$ satisfies that $A \cap [r] = \emptyset$ then $A \in S(r)$. The assumption in (6.7) implies that there exists $\sigma \in S_n$ such that $\sigma(A) \cap [r] = \emptyset$ for all $A \in \mathcal{F}^c$. Therefore, $\sigma(\mathcal{F}^c) \subseteq S(r)$. □

Note that Theorem 65 follows from Corollary 74 because every family of $r$-subsets $\mathcal{F}$ satisfying that $|\mathcal{F}^c| \leq \frac{n}{r} - 1$ also satisfies inequality (6.7).

# Chapter 7

# THE RANK RESILIENCE PROPERTY OF $W_{r,s}(q)$

Recall that $W_{r,s}(q)$ denotes the higher inclusion matrix of $r$-subspaces vs. $s$-subspaces. In this thesis we generalize Theorem 5 in two directions. In Chapter 6 we proved that the rank of $W_{r,s}$ is resilient over any field $K$. Now, in this chapter we prove a similar result for higher inclusion matrices of $r$-subspaces vs. $s$-subspaces. Indeed, we prove that the $K$-rank of $W_{r,s}(q)$ is resilient or robust over any field $K$ with $char(K) \neq p$. As we did in the set case, we denote by $\mathcal{F}^c$ the family of $r$-subspaces $\begin{bmatrix} \mathbb{F}_q^n \\ r \end{bmatrix} \setminus \mathcal{F}$.

**Theorem 75.** *Assume that $0 \leq s < r \leq n/2$. Let $\mathcal{F}$ be a family of $r$-subspaces of $\mathbb{F}_q^n$ and $K$ a field with $char(K) \neq p$. If $|\mathcal{F}^c| \leq \frac{n}{r} - 1$ then $rank_K(W_{r,s}(q)) = rank_K(W_{r,s}^{\mathcal{F}}(q))$.*

We start by presenting some results about the rank of these matrices over fields of different characteristic. We also discuss some of the proof techniques that have been applied to obtain those results. Finally, in Section 7.2 we prove Theorem 75.

## 7.1 The Rank of $W_{r,s}(q)$

The ranks of the matrices $W_{r,s}(q)$ have been extensively studied. However, the results are not as complete as in the set case. It was proven by Kantor [36] that if $s \leq \min(r, n-r)$ then the $\mathbb{Q}$-rank of $W_{r,s}(q)$ is $\begin{bmatrix} n \\ s \end{bmatrix}$. Later, Frumkin and Yakir [23] proved that if the characteristic of $K$ is not equal to $p$, where $q = p^t$, and $n \geq r + s$ then the $K$-rank of $W_{r,s}(q)$ is given by a $q$-analogue of Wilson's formula. Indeed,

$$\operatorname{rank}_K(W_{r,s}(q)) = \sum_{j \in Y} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}, \tag{7.1}$$

where $Y = \{i : 0 \leq i \leq s, \begin{bmatrix} r-i \\ s-i \end{bmatrix} \neq_K 0\}$. If the characteristic of $K$ is equal to $p$ then the problem of finding the $p$-rank of $W_{r,s}(q)$ is open in general. However, under the additional condition $s = 1$, Hamada [30] gave a formula for the $p$-rank of $W_{r,1}(q)$.

It is important to remark that although there are at least four different proofs ([9, 20, 23, 58]) of Wilson's rank formula, only the idea of Frumkin and Yakir has been generalized to find a formula for the rank of the matrix $W_{r,s}(q)$ over $K$ when $char(K) \neq p$. This is an indication that the generalization of classical results from extremal set theory is a difficult task.

Remarkably, Frumkin and Yakir proposed an uniform approach to finding a rank formula for both $W_{r,s}$ and $W_{r,s}(q)$ using exactly the same steps. Their main idea is to apply some results from representation theory. Indeed, they realized that $W_{r,s}$ and $W_{r,s}(q)$ are matrices associated with an $S_n$- and a $GL(n,q)$-module homomorphisms, respectively. Moreover, it is well known that there is a close relationship between the representation theory of $S_n$ and the representation theory of $GL(n,q)$. Therefore, many statements about a $S_n$-module homomorphism have a natural analogue for a corresponding $GL(n,q)$-module homomorphism.

In fact, the work of James [32] shows that there are striking similarities between the representation theory of $S_n$ and $GL(n,q)$. We recall some of these analogies that will be helpful later. Let $K$ be a field. For each partition $\lambda$ of $n$, we may define a $S_n$-module $S^\lambda$ over $K$, known as the Specht module, such that if $K = \mathbb{C}$ then the Specht modules are a complete set of pairwise non-isomorphic irreducible modules of $S_n$. Moreover, each Specht module corresponds to the intersection of the kernels of certain $S_n$-module homomorphisms. The dimension of the Specht module is given by the hook-length formula; in the case of partitions with two parts there is a simpler formula. Let $\lambda = (n-r, r)$. The Specht module $S^\lambda$ has dimension $\binom{n}{r} - \binom{n}{r-1}$.

Now assume that the characteristic of $K$ is not equal to $p$. Again, for each partition $\lambda$ of $n$, we may define a $GL(n,q)$-module $S^\lambda$ over $K$, also known as the Specht module. If $K = \mathbb{C}$ then the Specht modules are a complete set of pairwise non-isomorphic unipotent irreducible modules of $GL(n,q)$. Moreover, each Specht module

corresponds to the intersection of the kernels of certain $GL(n,q)$-module homomorphisms. The dimension of the Specht module is given by a $q$-analogue of hook-length formula; again for the case of partitions with two parts there is a simpler formula. Let $\lambda = (n-r, r)$. Then the Specht module $S^\lambda$ has dimension $\begin{bmatrix} n \\ r \end{bmatrix} - \begin{bmatrix} n \\ r-1 \end{bmatrix}$.

We briefly recall the main idea used by Frumkin and Yakir to prove equation 7.1. For every $0 \leq r \leq n$, we denote by $M_q^r$ the $K$-vector space spanned by the $r$-dimensional subspaces of $\mathbb{F}_q^n$. Hence, the set of $r$-dimensional subspaces forms a "canonical basis" of $M_q^r$.

Recall that $GL(n,q)$ is the group of all invertible linear transformations from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$. Every element of $GL(n,q)$ induces a permutation on the set of $r$-dimensional subspaces of $\mathbb{F}_q^n$. Thus, $M_q^r$ is a $GL(n,q)$-module for every $0 \leq r \leq n$.

Consider the linear transformation $\varphi_{j,r} : M_q^j \to M_q^r$ which maps every $j$-dimensional subspace $X$ to

$$\varphi_{j,r}(X) = \sum_{X \subseteq R} R,$$

where the sum runs over all the $r$-dimensional subspaces containing $X$. Note that $W_{r,j}(q)$ is the matrix associated with $\varphi_{j,r}$ with respect to the canonical bases of $M_q^j$ and $M_q^r$. Furthermore, it follows from Definition 9 that $\varphi_{j,r}$ is a $GL(n,q)$-module homomorphism because for every $g \in GL(n,q)$ we have that $g \cdot \varphi_{j,r} = \varphi_{j,r} \cdot g$.

We denote by $\varphi_{j,r}^*$ the transpose of $\varphi_{j,r}$ such that the matrix of $\varphi_{j,r}^*$ with respect to the canonical bases of $M_q^j$ and $M_q^r$ is equal to the transpose of $W_{r,j}(q)$. Frumkin and Yakir proved that the Specht module $S^{(n-j,j)}$ is contained in the image of $\varphi_{j,r}^*$ for every $j \leq r$ and $j + r \leq n$. This fact is crucial to proving that the $K$-rank of the matrix

$$W_{r,\leq s}(q) = \begin{bmatrix} W_{r,0}(q) & W_{r,1}(q) & \cdots & W_{r,s}(q) \end{bmatrix}$$

is equal to

$$\sum_{j=0}^{s} \dim_K(S^{(n-j,j)}) = \sum_{j=0}^{s} \begin{bmatrix} n \\ j \end{bmatrix} - \begin{bmatrix} n \\ j-1 \end{bmatrix} = \begin{bmatrix} n \\ s \end{bmatrix}$$

where we are assuming that $\begin{bmatrix} n \\ -1 \end{bmatrix} = 0$.

**Lemma 76.** *(Frumkin and Yakir) Let $K$ be a field with $char(K) \neq p$. If $s \leq r$ and $r + s \leq n$ then the $K$-rank of $W_{r,\leq s}(q)$ is equal to $\begin{bmatrix} n \\ s \end{bmatrix}$.*

Now, the $q$-analogue of Wilson's rank formula follows easily from Lemma 76.

## 7.2 Resilience Property

### 7.2.1 The $GL(n,q)$-module $M_q^r$

In this section, we assume that $K$ is a field of characteristic coprime to $q = p^t$, containing a primitive $p$-th root of unity. We use the notation introduced in Section 7.1; but from now on assume that $r \leq n/2$.

The Specht module $S^{(n-r,r)}$ is the submodule of $M_q^r$ defined by

$$S^{(n-r,r)} = \bigcap_{j<r} \left\{ \ker \phi : \phi \in \mathrm{Hom}_{GL(n,q)}(M_q^r, M_q^j) \right\},$$

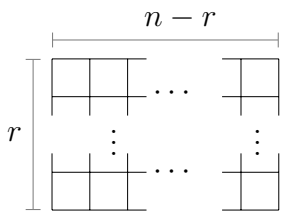
where $\mathrm{Hom}_{GL(n,q)}(M_q^r, M_q^j)$ is the set of all $GL(n,q)$-module homomorphisms from $M_q^j$ to $M_q^r$.

In [32], James proved that the dimension of $S^{(n-r,r)}$ over $K$ is equal to $\begin{bmatrix} n \\ r \end{bmatrix} - \begin{bmatrix} n \\ r-1 \end{bmatrix}$. He also proved the following important result about Specht modules.

**Theorem 77.** *(The Submodule Theorem) Let $\langle \cdot, \cdot \rangle$ be the inner product on $M_q^r$ such that for any two $r$-dimensional subspaces $X, Y$ of $\mathbb{F}_q^n$ we have that $\langle X, Y \rangle = 1$ if $X = Y$ and 0, otherwise. If $W$ is a submodule of $M_q^r$ then either $S^{(n-r,r)} \subseteq W$ or $W \subseteq (S^{(n-r,r)})^{\perp}$.*

Recently, in [10] Brandt et al. found a basis of $S^{(n-r,r)}$ which is indexed by standard tableaux of shape $(n-r, r)$. We introduce some definitions and results from [10] to describe this "standard basis".

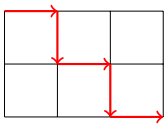
Consider a rectangular array of boxes of size $r$ by $n-r$ with $r \leq n-r$, as appears in the following figure:



It is known that every $r$-subset $A$ of $[n]$ can be represented by a path connecting the top left corner with the right bottom corner of the above array of boxes. Specifically, the $i$-th step is south or east according as $i \in A$ or $i \notin A$ holds. For example, the $r$-subsets contained in $S(r)$ correspond to the paths that do not cross the main diagonal of the array of boxes.

We denote by $P(n-r,r)$ the set of all paths connecting the top left with the bottom right corner of an array of boxes of size $r$ by $n-r$.

**Example 78.** Consider $n = 5$ and $r = 2$,



so the path corresponding to this figure is $\pi = ESESE$ where $E$ stand for east and $S$ for south. Hence, the 2-subset of $[5]$ corresponding to $\pi$ is $\{2,4\}$.

We impose the reverse lexicographic order on the set of paths $P(n-r,r)$. For example, the elements of $P(2,2)$ are ordered in the following way:

$$SSEE < SESE < SEES < ESSE < ESES < EESS.$$

Given any path $\pi \in P(n-r,r)$ we can fill the boxes below $\pi$ using elements from $\mathbb{F}_q$. For example, for $n = 7$ and $r = 3$,

| | | | |
|---|---|---|---|
| $a_1$ | | | |
| $a_2$ | $a_3$ | | |
| $a_4$ | $a_5$ | $a_6$ | |

where $a_i \in \mathbb{F}_q$ and $\pi = ESESESE$. The following well known result establishes a bijection between these objects and $r$-dimensional subspaces of $\mathbb{F}_q^n$. A proof can be found in [10].

**Lemma 79.** *(Brandt et al., [10]) Choosing a path $\pi \in P(n-r,r)$ and then filling the boxes below the path with elements of $\mathbb{F}_q$ is a way of encoding a $r$-dimensional subspace of $\mathbb{F}_q^n$. Every such subspace can be uniquely encoded in this way.*

The proof of Lemma 79 relates the reduced echelon form of a subspace with a path $\pi$ and a filling for that path. In fact, if a 3-dimensional vector subspace of $\mathbb{F}_q^7$ has the following reduced echelon form

$$\begin{pmatrix} a & 1 & 0 & 0 & 0 & 0 & 0 \\ b & 0 & 1 & 0 & 0 & 0 & 0 \\ c & 0 & 0 & d & 1 & 0 & 0 \end{pmatrix}$$

then the path and filling corresponding to this vector subspace is,

| | | | |
|---|---|---|---|
| $a$ | | | |
| $b$ | | | |
| $c$ | $d$ | | |

with $\pi = ESSESEE$.

For every $r$-subspace $X$ of $\mathbb{F}_q^n$ we will denote by $\pi(X)$ the path corresponding to $X$.

**Definition 80.** (Brandt, Dipper, James, and Lyle. [10]) Suppose that $v \in M_q^r$, and write

$$v = \sum_{X \in \begin{bmatrix} \mathbb{F}_q^n \\ r \end{bmatrix}} c_X X, \qquad \text{where } c_X \in K.$$

1. For each path $\pi$, let
$$v(\pi) = \sum_{X : \pi(X) = \pi} c_X X.$$

2. If $v \neq 0$, then let greatest$(v)$ be the greatest[1] path $\pi \in P(n-r, r)$ such that $v(\pi) \neq 0$.

3. If $v \neq 0$, then let $\text{top}(v) = v(greatest(v))$.

4. If $U$ is a subspace of $M_q^r$ and $\pi \in P(n-r, r)$, then let
$$U(\pi) = \{u(\pi) : 0 \neq u \in U \text{ and } greatest(u) = \pi\} \cup \{0\}.$$

[1] Greatest with respect to the reverse lexicographic order imposed on $P(n-r, r)$

Let $\theta$ be an additive character of $\mathbb{F}_q$. Suppose that $X$ and $L$ are $r$-dimensional subspaces of $\mathbb{F}_q^n$ such that $\pi(X) = \pi(L)$. Let $\chi_L$ be the linear character defined by

$$\chi_L(X) = \prod_{i=1}^{r} \prod_{j=1}^{n-r} \theta(l_{i,j} x_{i,j})$$

where $l_{i,j}$ and $m_{i,j}$ denote the $(i,j)$-entries in the filling corresponding to $L$ and $X$, respectively (here we are assuming that the boxes above the path are filled with zeros). Using the character $\chi_L$ it is possible to define the following element of $M_q^r$

$$e_L = \sum_{X:\pi(X)=\pi(L)} \chi_L(-X)X$$

for every $L \in \begin{bmatrix} \mathbb{F}_q^n \\ r \end{bmatrix}$. Furthermore, the orthogonality relations for linear characters imply that the sets

$$\left\{ e_L : L \in \begin{bmatrix} \mathbb{F}_q^n \\ r \end{bmatrix} \right\} \quad \text{and} \quad \left\{ e_L : L \in \begin{bmatrix} \mathbb{F}_q^n \\ r \end{bmatrix} \text{ with } \pi(L) = \pi \right\}$$

form a basis of $M_q^r$ and $M_q^r(\pi)$, respectively.

**Definition 81.** (Brandt et al., [10]) Let $\pi \in P(n-r, r)$ be a path connecting the top left with the bottom right corner of an array of boxes of size $r$ by $n-r$. Label the corners of the array by ordered pairs $(i,j)$ with $i = 1, \ldots, r+1$ and $j = 1, \ldots, n-r+1$. For every corner $(i,j)$, we define $r(i,j) = j - i$. Let $X$ be a $r$-dimensional subspace of $\mathbb{F}_q^n$ such that $\pi(X) = \pi$. We say that $X$ is *good* if its associated filling of the boxes to the south of $\pi$ with elements of $\mathbb{F}_q$ satisfies the following condition: for each corner $(i,j)$ through which the path $\pi$ passes, the matrix with bottom left and top right corners having coordinates $(r+1, 1)$ and $(i,j)$, respectively, has rank at most $r(i,j)$. If $X$ is not good then we say it is bad.

Note that Definition 81 implies that if a path $\pi \in P(n-r, r)$ crosses the main diagonal of the array of boxes then there is no good $r$-dimensional subspace $X$ with $\pi(X) = \pi$. Therefore, it follows that if $L$ is a good $r$-dimensional subspace of $\mathbb{F}_q^n$ then $\pi(L) \in S(r)$. The next theorem gives a basis for the Specht module $S^{(n-r,r)}$.

**Theorem 82.** *(Brandt et al., [10]) For every good $r$-dimensional subspace $L$ of $\mathbb{F}_q^n$ there exists a vector $z_L \in M_q^r$ with $top(z_L) = e_L$ such that the set $\{z_L : L \text{ good}\}$ forms a basis of $S^{(n-r,r)}$.*

As was remarked earlier, every path $\pi \in P(n-r,r)$ that does not cross the main diagonal is related to a unique subset in $S(r)$. Thus, by abuse of notation we will denote also by $S(r)$ the set of paths that do not cross the main diagonal. Since the elements of $S(r)$ are in one to one correspondence with the standard tableaux of shape $(n-r,r)$, it follows that Theorem 82 provides a basis of $S^{(n-r,r)}$ which is indexed by standard tableaux, i.e. a "standard" basis.

To prove Theorem 75 we will need to introduce another submodule of $M_q^r$. Consider the linear transformation $\varphi_{j,r} : M_q^j \to M_q^r$ which maps every $j$-dimensional subspace $X$ to

$$\varphi_{j,r}(X) = \sum_{X \subseteq R} R,$$

where the sum goes over all the $r$-dimensional subspaces containing $X$. Moreover, for any $j$-dimensional subspace $X$ of $\mathbb{F}_q^r$, with $j \leq r$, we denote by $\langle X \rangle_r$ the image of $X$ under the linear transformation $\varphi_{j,r}$.

Note that $W_{r,j}(q)$ is the matrix associated with $\varphi_{j,r}$ with respect to the canonical bases of $M_q^j$ and $M_q^r$. Therefore,

$$\dim_K(\mathrm{im}(\varphi_{j,r})) = \sum_{i \in Y} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}, \tag{7.2}$$

where $Y = \{i : 0 \leq i \leq j, \begin{bmatrix} r-i \\ j-i \end{bmatrix} \neq_K 0\}$. Furthermore, it follows from Definition 9 that $\varphi_{j,r}$ is a $GL(n,q)$-module homomorphism because for every $g \in GL(n,q)$ we have that $g \cdot \varphi_{j,r} = \varphi_{j,r} \cdot g$.

Consider the following subspace of $M_q^r$,

$$U_{r-1} = \varphi_{0,r}(M_q^0) + \varphi_{1,r}(M_q^1) + \cdots + \varphi_{r-1,r}(M_q^{r-1}).$$

Lemma 10 implies that $U_{r-1}$ is a $GL(n,q)$-module. This module was studied by Frumkin and Yakir in [23]. They proved that the dimension over $K$ of $U_{r-1}$ is $\begin{bmatrix} n \\ r-1 \end{bmatrix}$.

### 7.2.2 Proof of Theorem 75

In this section we prove Theorem 75. Our approach will be similar to the one used in the proof of Theorem 65. However, because we do not have a $q$-analogue of Bier basis for $M_q^r$ we will apply the results from representation theory that were introduced in the previous sections.

For $\pi \in P(n-r,r)$, define the *leading term* of $\pi$ to be the number of $E$ moves before the first $S$ move. We denote by $S(r)^<$ the set of paths in $S(r)$ whose leading term is strictly less than $r$ and by $S(r)^\geq$ the set of paths in $S(r)$ whose leading term is greater than or equal to $r$. Thus by definition we have that

$$S(r) = (S(r)^<) \cup \left(S(r)^\geq\right).$$

**Lemma 83.** *If $K$ is a field of characteristic coprime to $q$ containing a primitive $p$-th root of unity then*

$$U_{r-1} \cap \bigoplus_{\pi \in S(r)^\geq} M_q^r(\pi) = \{0\}.$$

*Proof.* Consider the inner product over $M_q^r$ defined in the statement of Theorem 77. A straightforward application of the Submodule Theorem implies that $U_{r-1}$ is contained in the orthogonal complement of the Specht module $S^{(n-r,r)}$. Thus, for every $z \in S^{(n-r,r)}$ and $v \in U_{r-1}$ we have that $\langle z, v\rangle = 0$.

It follows from Definition 81 that every $r$-dimensional subspace $L$ of $\mathbb{F}_q^n$ with $\pi(L) \in S(r)^\geq$ is a good subspace. Therefore, if $\pi \in S(r)^\geq$ then the set of vectors $\{e_L : L \text{ good and } \pi(L) = \pi\}$ is a basis of $M_q^r(\pi)$. Combining this fact with Theorem 82, we conclude that the Specht module $S^{(n-r,r)}$ contains a vector $w_L$, for every $L$ with $\pi(L) \in S(r)^\geq$ such that $top(w_L) = L$.

Given any vector $v \in M_q^r$ we can use the canonical basis of $M_q^r$ to represent $v$ as a column vector. We arrange the canonical basis with respect to the reverse lexicographic order, therefore, on the top we have the subspaces related to the paths in $S(r)^\geq$, then the subspaces whose associated path is an element of $S(r)^<$, and finally the ones associated with paths in $P(n-r,r) \setminus S(r)$.

Now, given an arbitrary basis of $U_{r-1}$, we consider its representation as column vectors with respect to the canonical basis. Applying column operations on this basis we can get a new basis of $U_{r-1}$ in reduced echelon form such that the leading ones appear from left to right and from the bottom to the top.

We claim that no leading one of this basis appears on a row indexed by a subspace $L$ with $\pi(L) \in S(r)^{\geq}$. Note that this is enough to prove Lemma 83.

To prove our claim we proceed by contradiction. Suppose that after column operations one of the basis elements $v'$ of $U_{r-1}$ has a leading one in an entry indexed by a subspace $L$ with $\pi(L) \in S(r)^{\geq}$. Therefore, $\langle v', w_L \rangle = 1$ which is a contradiction because $U_{r-1} \subseteq (S^{(n-r,r)})^{\perp}$.

□

Now we prove a vector space analogue of Lemma 72. To state this result we introduce some notation. For any $g \in GL(n,q)$ and any family $\mathcal{F}$ of $r$-subspaces of $\mathbb{F}_q^n$ we denote by $g(\mathcal{F})$ the family of $r$-subspaces $\{g(X) : X \in \mathcal{F}\}$. Furthermore, consider the following set of $r$-dimensional vector subspaces of $\mathbb{F}_q^n$:

$$S(r)_q^{\geq} = \left\{ X \in \begin{bmatrix} \mathbb{F}_q^n \\ r \end{bmatrix} : \pi(X) \in S(r)^{\geq} \right\}.$$

Thus, $S(r)_q^{\geq}$ is the set of $r$-subspaces of $\mathbb{F}_q^n$ whose associated path is in $S(r)$ and has leading term greater than or equal to $r$.

**Lemma 84.** *Suppose $0 \leq s < r \leq n/2$. Let $\mathcal{F}$ be a family of $r$-dimensional subspaces of $\mathbb{F}_q^n$ and $K$ a field with $char(K) \neq p$. If there exists $g \in GL(n,q)$ such that $g(\mathcal{F}^c) \subseteq S(r)_q^{\geq}$ then*

$$rank_K(W_{r,s}^{\mathcal{F}}(q)) = rank_K(W_{r,s}(q)).$$

*Proof.* Note that without loss of generality we can assume that $K$ contains a primitive $p$-th root of unity. Indeed, if $K$ does not contain a primitive $p$-th root of unity then we can extend $K$ to a larger field and this does not change the rank of the matrices $W_{r,s}(q)$ or $W_{r,s}(q)^{\mathcal{F}}$.

First, assume that $\mathcal{F}^c \subseteq S(r)_q^{\geq}$. Consider the following subspaces of $M_q^s$,

$$W_j = \varphi_{0,s}(M_q^0) + \varphi_{1,s}(M_q^1) + \cdots + \varphi_{j,s}(M_q^j). \tag{7.3}$$

for $j$ from 0 to $s$. It is clear that

$$W_0 \subset W_1 \subset \cdots \subset W_s. \tag{7.4}$$

Furthermore, Frumkin and Yakir proved that the dimension of $W_j$ over $K$ is $\begin{bmatrix} n \\ j \end{bmatrix}$. Therefore, it follows from equations (7.3) and (7.4) that $M_q^s$ has a basis with the following property: for all $j$ from 0 to $s$, $\begin{bmatrix} n \\ j \end{bmatrix} - \begin{bmatrix} n \\ j-1 \end{bmatrix}$ of the elements of the basis are of the form $\langle X \rangle_s$ with $X \in \begin{bmatrix} \mathbb{F}_q \\ j \end{bmatrix}$. For every $j$ from 0 to $s$, we denote by $B_j$ a set of $j$-dimensional subspaces of $\mathbb{F}_q^n$ with cardinality $\begin{bmatrix} n \\ j \end{bmatrix} - \begin{bmatrix} n \\ j-1 \end{bmatrix}$ chosen in such a way that

$$\bigcup_{j=0}^{s} \{\langle X \rangle_s : X \in B_j\}$$

is a basis of $M_q^s$.

The definition of $\varphi_{s,r}$ implies that

$$\varphi_{s,r}(\langle X \rangle_s) = \begin{bmatrix} r-j \\ s-j \end{bmatrix} \langle X \rangle_r \tag{7.5}$$

for all $X \in B_j$ with $j$ from 0 to $s$.

Let $Y = \{j : 0 \leq j \leq s \text{ such that } \begin{bmatrix} r-j \\ s-j \end{bmatrix} \neq 0\}$ and $Z = \{j : 0 \leq j \leq s \text{ such that } \begin{bmatrix} r-j \\ s-j \end{bmatrix} = 0\}$. Equations (7.2) and (7.5) imply that the set

$$\bigcup_{j \in Z} \{\langle X \rangle_s : X \in B_j\}$$

forms a basis of the kernel of $\varphi_{s,r}$. Therefore, the set

$$\bigcup_{j \in Y} \{\langle X \rangle_r : X \in B_j\} \tag{7.6}$$

forms a basis for the image of $\varphi_{s,r}$ so in particular these vectors are linearly independent in $M_q^r$.

Now, we proceed in the same way as in the proof of Lemma 72. Consider the following linear transformation from $M_q^s$ to $M_q^r$

$$\varphi_{s,r}^{\mathcal{F}^c}(S) = \sum_{S \subseteq R} R - \sum_{T \in \mathcal{F}^c, S \subseteq T} T,$$

where $R$ runs over all $r$-dimensional subspaces of $\mathbb{F}_q^n$ containing $S$, and $T$ runs over all $r$-dimensional subspaces of $\mathbb{F}_q^n$ containing $S$ such that $T \in \mathcal{F}^c$. It is clear from definition that $\dim_K(\mathrm{im}\varphi_{s,r}^{\mathcal{F}^c}) = \mathrm{rank}_K W_{r,s}^{\mathcal{F}}(q)$. Furthermore, note that for every $X \in B_j$ with $0 \leq j \leq s$ we have that,

$$\varphi_{s,r}^{\mathcal{F}^c}(\langle X \rangle_s) = \begin{bmatrix} r-j \\ s-j \end{bmatrix} \langle X \rangle_r - \sum_{T \in \mathcal{F}^c, X \subseteq T} \begin{bmatrix} r-j \\ s-j \end{bmatrix} T.$$

Note that Claim 73 and Lemma 83 imply that the vectors

$$\bigcup_{j \in Y} \{\varphi_{s,r}^{\mathcal{F}^c}(\langle X \rangle_s) : X \in B_j\}$$

are linearly independent in $M_q^r$. Therefore,

$$\sum_{j \in Y} \begin{bmatrix} n \\ j \end{bmatrix} - \begin{bmatrix} n \\ j-1 \end{bmatrix} \leq \dim_K(\mathrm{im}\varphi_{s,r}^{\mathcal{F}^c}).$$

Hence, Lemma 84 follows from the trivial upper bound $\mathrm{rank}_K W_{r,s}^{\mathcal{F}}(q) \leq \mathrm{rank}_K W_{r,s}(q)$ and the $q$-analogue of Wilson's rank formula for $W_{r,s}(q)$.

Now, if $\mathcal{F}^c \not\subseteq S(r)_q^{\geq}$ then by assumption there exists $g \in GL(n,q)$ such that $g(\mathcal{F}^c) \subseteq S(r)_q^{\geq}$. Like in the proof of Lemma 72, we can use $g$ to define the following invertible linear transformations,

$$\Phi_r^g : \begin{array}{ccc} M_q^r & \to & M_q^r \\ R & \mapsto & g(R) \end{array}, \qquad \Phi_s^g : \begin{array}{ccc} M_q^s & \to & M_q^s \\ S & \mapsto & g(S) \end{array}.$$

From the above definitions, it follows that

$$\varphi_{s,r}^{\mathcal{F}^c} = (\Phi_r^g)^{-1} \circ \varphi_{s,r}^{g(\mathcal{F}^c)} \circ \Phi_s^g.$$

Hence, $\dim_K(\mathrm{im}\varphi_{s,r}^{\mathcal{F}^c}) = \dim_K(\mathrm{im}\varphi_{s,r}^{g(\mathcal{F}^c)})$ which implies Lemma 84.

□

In the statement of the next corollary, given a $r$-dimensional subspace $X$, we denote also by $\pi(X)$ the unique subset of $[n]$ corresponding to the path associated with $X$.

**Corollary 85.** *Suppose that* $0 \leq s < r \leq n/2$. *Let* $\mathcal{F}$ *be a family of* $r$*-subspaces of* $\mathbb{F}_q^n$. *If the family* $\mathcal{F}$ *satisfies that*

$$\left| \bigcup_{X \in \mathcal{F}^c} \pi(X) \right| \leq n - r \tag{7.7}$$

*then* $rank_K(W_{r,s}^{\mathcal{F}}(q)) = rank_K(W_{r,s}(q))$.

*Proof.* Lemma 84 implies that is enough to show that there exists $g \in GL(n,q)$ such that $g(\mathcal{F}^c) \subseteq S(r)_q^{\geq}$. Recall that every $r$-dimensional subspace of $\mathbb{F}_q^n$ can be represented by a unique $r$ by $n$ matrix in reduced echelon form. The condition $\left|\bigcup_{X \in \mathcal{F}^c} \pi(X)\right| \leq n-r$ implies that there are at least $r$ columns that do not contain a leading one for any of the subspaces in $\mathcal{F}^c$. Let $i_1 < i_2 < \cdots < i_l$ be the indices of the columns corresponding to the leading ones of all subspaces in $\mathcal{F}^c$. By assumption we have that $l \leq n - r$ so there exists a permutation sending $i_l \to n, i_{l-1} \to n-1, \ldots, i_1 \to n-l+1$ where $n - l + 1 > r$.

This implies that there exists a linear transformation $g$ sending every $X \in \mathcal{F}^c$ to a subspace $g(X)$ such that none of the leading ones of the reduced echelon form of $g(X)$ appears on the first $r$ columns, therefore, $g(X) \in S(r)_q^{\geq}$ for every $X \in \mathcal{F}^c$. □

Theorem 75 is an immediate consequence of Corollary 85 because every family of $r$-subspaces $\mathcal{F}$ satisfying that $|\mathcal{F}^c| \leq \frac{n}{r} - 1$ also satisfies inequality (7.7).

# Chapter 8

# OPEN PROBLEMS

In this chapter we raise some problems related to the work we have done in this thesis.

In Chapter 4 we prove that extremal families in $PGL(2,q)$ are not only unique, but also stable: any intersecting family in $PGL(2,q)$ of size close to $q(q-1)$ must be close in structure to a coset of a point stabilizer. Actually, Theorem 41 implies that for $q$ sufficiently large the cosets of point stablizers are the only extremal families in $PGL(2,q)$. This result was already proven by Meagher and Spiga [45] using different methods.

It is possible to apply the ideas used in this thesis to prove similar results for some 3-transitive groups. Let $G$ be a finite group acting 3-transitively on a finite set $X$. Suppose that this action satisfies the following conditions:

1. The maximum size of an intersecting family in $G$ is $|G|/|X|$ (note that this number is equal to the size of a coset of a point stabilizer in $G$).

2. The standard character is the unique irreducible character affording the minimum eigenvalue of the derangement graph $Cay(G,D)$ where $D$ is the set of derangements in $G$ (recall that since $D$ is inverse-closed and conjugation-invariant there is a correspondence, given by Lemma 33, between the eigenvalues of $Cay(G,D)$ and the irreducible characters of $G$).

Thus, applying Hoffman's bound it follows that the characteristic vector of any intersecting family of maximum size lies in the vector subspace $\widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$ of $\mathbb{C}[G]$. Recall that $\widehat{V}_1$ and $\widehat{V}_{\chi_{std}}$ are the vector subspaces of complex-valued functions on $G$

whose Fourier transforms have support on the trivial and the standard representation, respectively.

Now, let $S \subset G$ be an intersecting family. If the size of $S$ is close to $|G|/|X|$ and the size of the gap between the smallest and the second-smallest eigenvalue of $Cay(G, D)$ is big enough then we can use analogues of Lemmas 42 and 43 to conclude that the characteristic function $1_S$ is close to $\widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$. Moreover, as was remarked in Section 4.2, the result of Ellis, Filmus and Friedgut in [16], for Boolean functions on $S_n$, can be generalized to any 3-transitive action of a finite group on a finite set. Thus, if $1_S$ is close to the vector space $\widehat{V}_1 \oplus \widehat{V}_{\chi_{std}}$ then it must be close in structure to some coset of a point stabilizer in $G$. Therefore, we can use these ideas to prove that extremal families in $G$ are unique and stable. In fact, the above analysis give more evidence to support the following conjecture.

**Conjecture 86.** (Meagher and Spiga, [45]) Let $G$ be a finite group acting 3-transitively on a finite set $X$. Every intersecting family of maximum size is a coset of a point stabilizer.

In this thesis we consider the natural right action of $PSL(2, q)$ on $PG(1, q)$, where $q$ is an odd prime power. Using the eigenvalue method, it was proved in [3, 45] that the maximum size of an intersecting family in $PSL(2, q)$ is $q(q-1)/2$. Meagher and Spiga [45] conjectured that the cosets of points stabilizers are the only intersecting families of maximum size in $PSL(2, q)$. Here, we prove their conjecture in the affirmative using tools from representation theory of $PGL(2, q)$ and deep results from number theory.

For future research, one could consider the stability problem concerning intersecting families of $PSL(2, q)$. The stability of intersecting families for permutation groups has been studied during the past few years (cf. [14, 22, 49]). We conjecture that extremal families in $PSL(2, q)$ are also stable. The precise statement is given below.

**Conjecture 87.** Let $S$ be an intersecting family in $PSL(2,q)$ with $q$ an odd prime power. Then there exists $\delta > 0$ such that if $|S| \geq (1-\delta)q(q-1)/2$ then $S$ is contained within a coset of a point stabilizer.

In this thesis, Theorem 5 proved by Keevash in [38] was generalized in two directions. First, we showed that the rank of the matrix $W_{r,s}$ is resilient over any field, i.e. if the size of a family $\mathcal{F}$ of $r$-subsets of $[n]$ is close enough to $\binom{n}{r}$ then $\text{rank}_K(W_{r,s}) = \text{rank}_K(W_{r,s}^{\mathcal{F}})$ for any field $K$. Note that a better result was proved in [29] under the additional assumption that $K$ is a field of characteristic zero. In fact, under this assumption it is known that $\text{rank}_K(W_{r,s}) = \text{rank}_K(W_{r,s}^{\mathcal{F}})$ for every family of $r$-subsets $\mathcal{F}$ satisfying that $|\mathcal{F}^c| < \binom{n-s}{r-s}$ (when $n$ is big enough) and this bound is the best possible over fields of characteristic zero. We conjecture that, similar to the case of characteristic zero, the rank of the matrix $W_{r,s}$ is resilient to the deletion of $O(n^{r-s})$ rows over any field.

**Conjecture 88.** Assume that $0 \leq s < r \leq n/2$. Let $\mathcal{F}$ be a family of $r$-subsets of $[n]$. If $n$ is big enough and $|\mathcal{F}^c| < \binom{n-s}{r-s}$ then $\text{rank}_K(W_{r,s}) = \text{rank}_K(W_{r,s}^{\mathcal{F}})$ for every field $K$.

Note that over fields of positive characteristic is it not known if $\binom{n-s}{r-s}$ is the best upper bound.

On the other hand, we proved a $q$-analogue of Theorem 5. Indeed, if the size of a family $\mathcal{F}$ of $r$-subspaces of $\mathbb{F}_q^n$ is close enough to $\begin{bmatrix} n \\ r \end{bmatrix}$ then $\text{rank}_K(W_{r,s}(q)) = \text{rank}_K(W_{r,s}^{\mathcal{F}}(q))$ for any field $K$ whose characteristic is not equal to $p$, where $q = p^t$.

The condition in Theorem 75 on the size of $\mathcal{F}^c$ seems too restrictive. In fact the striking similarities between the $K$-rank formulas of the matrices $W_{r,s}$ and $W_{r,s}(q)$ together with the results of Theorems 65 and 75 is enough evidence for us to make the following conjecture.

**Conjecture 89.** Assume that $0 \leq s < r \leq n/2$. Let $\mathcal{F}$ be a family of $r$-subspaces of $\mathbb{F}_q^n$ and $K$ a field with $\text{char}(K) \neq p$. If $n$ is big enough and $|\mathcal{F}^c| < \begin{bmatrix} n-s \\ r-s \end{bmatrix}$ then $\text{rank}_K(W_{r,s}(q)) = \text{rank}_K(W_{r,s}^{\mathcal{F}}(q))$.

Note that over fields of characteristic zero $\begin{bmatrix} n-s \\ r-s \end{bmatrix}$ is the best upper bound, however, this has not be proven for fields of positive characteristic.

## REFERENCES


[1] N. Alon, I. Dinur, E. Friedgut and B. Sudakov. Graph products, Fourier analysis and spectral techniques. *Geometric and Functional Analysis*, **14** (2004), 913-940.

[2] S. Ahlgren and K. Ono, A Gaussian hypergeometric series evaluation and Apery number congruences *J. Reine Angew. Math.* **518** (2000), 187-212.

[3] B. Ahmadi and K. Meagher. The Erdös-Ko-Rado property for some 2-transitive groups. *Ann. Combin.* **19** (2015), 621-640.

[4] B. Ahmadi and K. Meagher. A new proof for the Erdös-Ko-Rado Theorem for the alternating group. *Disc. Math.* **324** (2014), 28–40.

[5] G.E. Andrews, George, R. Askey, and R. Roy, *Special functions. Encyclopedia of Mathematics and its Applications 71*, Cambridge University Press, Cambridge, 1999.

[6] L. Babai. Spectra of Cayley graphs. *Journal of Combinatorial Theory, Series B*, **27** (1979), 180-189.

[7] V. Batyrev and D. van Straten. Generalized hypergeometric functions and rational curves on Calabi-Yau complete intersections in toric varieties. *Comm. Math. Phys.* **168** (1995), 493–533.

[8] F. Beukers, H. Cohen, and A. Mellit. Finite hypergeometric functions. `arXiv: 1505.02900`.

[9] T. Bier. Remarks on Recent Formulas of Wilson and Frankl. *Europ. J. Combinatorics*, **14** (1993), 1-8.

[10] M. Brandt, R. Dipper, G. James and S. Lyle. Rank polynomials, *Proc. London Math. Soc.*, **98** (2009), 1-18.

[11] P. J. Cameron and C. Y. Ku. Intersecting families of permutations. *European J. Combin.* **24** (2003), 881–890.

[12] P. Diaconis, M. Shahshahani. Generating a random permutation with random transpositions. *Probability Theory and Related Fields*, **57** (1981), 159-179.

[13] D. Ellis. Stability for $t$-intersecting families of permutations. *Journal of Combinatorial Theory, Series A*, **118** (2011), 208-227.

[14] D. Ellis. A Proof of the Cameron-Ku Conjecture. *J. London Math. Soc.* **85** (2012), 165-190.

[15] D. Elllis, Y. Filmus and E. Friedgut. Triangle-intersecting families of graphs. *Journal of the European Mathematical Society*, **14** (2012), 841-885.

[16] D. Ellis, Y. Filmus, and E. Friedgut. A quasi-stability result for dictatorships in $S_n$. *Combinatorica*, (2014),1-46.

[17] D. Ellis, Y. Filmus, and E. Friedgut. A stability result for balanced dictatorships in $S_n$. *Random Structures and Algorithms*, 2015.

[18] P. Erdös, C. Ko, R. Rado. Intersection theorems for systems of finite sets. *Quart. J. Math. Oxford* **12** (1961), 313-320.

[19] P. Frankl Erdös-Ko-Rado theorem with conditions on the maximal degree. *J. Combin. Theory Ser. A*, **46** (1987), 252-263.

[20] P. Frankl. Intersection theorems and mod p rank of inclusion matrices. *J. Combin. Theory Ser. A*, **54** (1990), 85-94.

[21] P. Frankl and M. Deza. On the maximum number of permutations with given maximal or minimal distance. *J. Combin. Theory Ser. A*, **22** (1977), 352-360.

[22] E. Friedgut, G. Kalai, A. Naor. Boolean functions whose Fourier transform is concentrated on the first two levels. *Advances in Applied Mathematics*, **29** (2002), 427-437.

[23] A. Frumkin and A. Yakir. Rank of inclusion matrices and modular representation theory. *Israel Journal of Mathematics*, **71** 1990, 309-320.

[24] J. G. Fuselier, L. Long, R. Ramakrishna, H. Swisher, and F. Tu. Hypergeometric functions over finite fields. `arxiv:1510.02575`

[25] J. Greene. Hypergeometric functions over finite fields. *Trans. Amer. Math. Soc.* **301** (1987), 77-101.

[26] C. Godsil and K. Meagher. A new proof of the Erdös-Ko-Rado theorem for intersecting families of permutations. *European J. Combin.* **30** (2009), 404-414.

[27] D. H. Gottlieb. A certain class of incidence matrices. *Proc. Amer. Math. Soc.*, **17** (1966), 1233-1237.

[28] F. Gouvêa and N. Yui. Rigid Calabi-Yau threefolds over $\mathbb{Q}$ are modular. *Expo. Math.* **29** (2011), 142-149.

[29] C. Grosu, Y. Person, and T. Szabó. On the rank of higher inclusion matrices. *Journal of the London Mathematical Society*, 2014.

[30] N. Hamada. The rank of the incidence matrix of points and $d$-flats in finite geometries. *J. Sci. Hiroshima Univ.* **32** (1968), 381-396.

[31] H. Hatami, M. Ghandehari. Fourier analysis and large independent sets in powers of complete graphs. *Journal of Combinatorial Theory, Series B*, **98** (2008):164-172.

[32] G. D. James. *Representations of general linear groups*, London Mathematical Society, Lecture Note Series 94, 1984.

[33] Stasys Jukna *Extremal Combinatorics*, 2nd edn. Springer, Berlin, 2011.

[34] A. Kable, Legendre sums, Soto- Andrade sums and Kloosterman sums. *Pacific J. Math.* **206** (2002), 139-157.

[35] G. Katona. A theorem of finite sets. *Theory of graphs (Proc. Colloq., Tihany, 1966)*, (1968), 187-207.

[36] W. M. Kantor. On incidence matrices of finite projective and affine spaces. *Math. Z.*, **124** (1972), 315-318.

[37] N. M. Katz. *Exponential Sums and Differential Equations.* Annals of Math Studies, 124, 1990.

[38] P. Keevash. Shadows and intersections: stability and new proofs. *Adv. Math.*, **218** (2008), 1695-1703.

[39] J. B. Kruskal. The number of simplices in a complex. *Mathematical optimization techniques*, (1963), 251-278.

[40] The L-function and modular forms database, http://www.lmfdb.org

[41] B. Larose and C. Malvenuto. Stable sets of maximal size in Kneser-type graphs. *Europ. J. Combin.* **25** (2004), 657-673.

[42] N. Linial and B. L. Rothschild, Incidence matrices of subsets - A rank formula, *SIAM J. Algebraic Discrete Meth.*, **2** (1981), 333-340.

[43] L. Lovász. On the Shannon Capacity of a Graph. *IEEE Transactions on Information Theory*, IT-25, 1979.

[44] L. Lovász. em Combinatorial Problems and Exercises. North-Holland, Amsterdam, 1993.

[45] K. Meagher and P. Spiga. An Erdös-Ko-Rado theorem for the derangement graph of $PGL(2, q)$ acting on the projective line. *J. Combin. Theory Ser. A*, **118** (2011), 532-544.

[46] K. Meagher and P. Spiga. An Erdös-Ko-Rado theorem for the derangement graph of $PGL_3(q)$ acting on the projective plane. *SIAM J. Disc. Math.* **28** (2014), 918-941.

[47] K. Ono. Values of gaussian hypergeometric series. *Trans. Amer. Math. Soc.* **350** (1998), 1205-1223.

[48] I. Piatetski-Shapiro. *Complex Representations of $GL(2, K)$ for finite fields $K$.* Contemporary mathematics, 1983.

[49] R. Plaza, Stability for Intersecting Families in $PGL(2, q)$. *Electron. J. Combin.* **22** (2015).

[50] P. Reteln, On the Spectrum of the Derangement Graph, *Electron. J. Combin.* **14** (2007).

[51] F. Rodriguez-Villegas. Hypergeometric families of Calabi-Yau manifolds. *Fields Inst. Commun., 38, Calabi-Yau varieties and mirror symmetry*, (2003), 223-231.

[52] F. Rodriguez-Villegas. *Hypergeometric motives*. Lecture notes.

[53] J. P. Serre. *Linear Representations of Finite Groups.* Graduate Texts in Mathematics, Springer, 1977.

[54] J. P. Serre. *Abelian l-adic representations and elliptic curves.* With the collaboration of Willem Kuyk and John Labute. Revised reprint of the 1968 original. Research Notes in Mathematics, 7. A K Peters, Ltd., Wellesley, MA, 1998. 199 pp. ISBN: 1-56881-077-6

[55] B. van Geemen and N. Nygaard. On the geometry and arithmetic of some Siegel modular threefolds. *J. Number Theory* **53** (1995), 45-87.

[56] H.A. Verrill, The L-series of certain rigid Calabi-Yau threefolds. *J. Number Theory* **81** (2000), 310-334.

[57] R. M. Wilson. The exact bound in the Erdös-Ko-Rado theorem. *Combinatorica* **4** (1984), 247-257.

[58] R. M. Wilson. A diagonal form for the incidence matrices of $t$-subsets v. $k$-subsets. *Europ. J. Combinatorics*, **11** (1990), 609-615.

[59] N. Yui. Update on the modularity of Calabi-Yau varieties. With an appendix by Helena Verrill. Fields Inst. Commun., 38, *Calabi-Yau varieties and mirror symmetry*, (2003), 307-362.

# Appendix

## PERMISSIONS

The work presented in Chapter 4 of this thesis was published at the Electronic Journal of Combinatorics [49]. The following is the permission notice given by the Electronic Journal of Combinatorics to present that work in this document.

**Copyright Notice**

The copyright of published papers remains with the authors. We only require your agreement that we publish it, as described in the following publication release agreement:

- This is an agreement between the Electronic Journal of Combinatorics (the "Journal"), and the copyright owner (the "Owner") of a work (the "Work") to be published in the Journal.
- The Owner warrants that s/he has the full power and authority to enter into this Agreement and to grant the rights granted in this Agreement.
- The Owner hereby grants to the Journal a worldwide, irrevocable, royalty free license to publish or distribute the Work, to enter into arrangements with others to publish or distribute the Work, and to archive the Work.
- The Owner agrees that further publication of the Work, with the same or substantially the same content as appears in the Journal, will include an acknowledgement of prior publication in the Journal.