Journal of Combinatorial Theory, Series A 157 (2018) 461–499

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Characterization of intersecting families of maximum size in $PSL(2, q)$

Ling Long[a,1], Rafael Plaza[b], Peter Sin[c,2], Qing Xiang[b,3]

[a] *Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, USA*
[b] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*
[c] *Department of Mathematics, University of Florida, Gainesville, FL 32611, USA*

ARTICLE INFO

Article history:
Received 25 August 2016
Available online xxxx

Keywords:
Character table
Erdős–Ko–Rado theorem
Hypergeometric function over finite field
Intersecting family
Legendre sum
Soto-Andrade sum

ABSTRACT

We consider the action of the 2-dimensional projective special linear group $PSL(2, q)$ on the projective line $PG(1, q)$ over the finite field $\mathbb{F}_q$, where q is an odd prime power. 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 an element $x \in PG(1, q)$ such that $x^{g_1} = x^{g_2}$. It is known that the maximum size of an intersecting family in $PSL(2, q)$ is $q(q-1)/2$. We prove that all intersecting families of maximum size are cosets of point stabilizers for all odd prime powers $q > 3$.

1. Introduction

Let n, k be positive integers such that $k \leq n$ and let $[n] = \{1, 2, \ldots, n\}$. A family of k-subsets of $[n]$ is said to be *intersecting* if the intersection of any two k-subsets in

E-mail addresses: llong@lsu.edu (L. Long), plaza@udel.edu (R. Plaza), sin@ufl.edu (P. Sin), qxiang@udel.edu (Q. Xiang).

[1] Research partially supported by NSF grants DMS-1303292 and DMS-1602047.
[2] Research partially supported by a grant from the Simons Foundation (#204181 to Peter Sin).
[3] Research partially supported by an NSF grant DMS-1600850.

https://doi.org/10.1016/j.jcta.2018.03.006
0097-3165/

the family is non-empty. The Erdős–Ko–Rado (EKR) theorem is a classical result in extremal set theory. It states that when $k < n/2$ any intersecting family of k-subsets has size at most $\binom{n-1}{k-1}$; equality holds if and only if the family consists of all k-subsets of $[n]$ containing a fixed element of $[n]$ (cf. [9]). In this paper, we focus on EKR type problems for permutation groups. In particular, for any odd prime power q, we consider the natural right action of $PSL(2, q)$, the 2-dimensional projective special linear group over the finite field $\mathbb{F}_q$, on the set of points of $PG(1, q)$, the projective line over $\mathbb{F}_q$.

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 any $g_1, g_2 \in S$ there exists an element $x \in X$ such that $x^{g_1} = x^{g_2}$, i.e., $g_1 g_2^{-1}$ stabilizes some $x \in X$. In the context of EKR-type theorems, the following problems about intersecting families in G are of interest:

I (Upper Bound) What is the maximum size of an intersecting family?
II (Characterization) What is the structure of intersecting families of maximum size?

Extensive research has been done to solve the above problems for different groups. In 1977, Deza and Frankl [10] solved Problem I for the symmetric group S_n acting on $[n]$. They proved that any intersecting family of S_n has size at most $(n-1)!$. In fact, this upper bound is tight because any coset of a point stabilizer in S_n is an intersecting family of size precisely $(n-1)!$. They conjectured these sets are the only intersecting families of size $(n-1)!$. This conjecture was proved to be true, independently, by Cameron and Ku [6] and Larose and Malvenuto [17].

In [20], Meagher and Spiga studied Problem 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 [21], they went one step further to solve Problem I and II for the group $PGL(3, q)$ acting on the set of points of the projective plane $PG(2, q)$.

In this paper we study Problem II for the group $PSL(2, q)$ acting on $PG(1, q)$, where q is an odd prime power. Here we only consider the q odd case since if q is a power of two, we have $PSL(2, q) = PGL(2, q)$, and both Problem I and II were solved in [20]. It is known, from the combined results of [3,20], that the maximum size of an intersecting family in $PSL(2, q)$ is $q(q-1)/2$. (In fact, in a recent paper [22], it is proved that if $G \leq S_n$ is a 2-transitive group, then the maximum size of an intersecting family in G is $|G|/n$. That is, the maximum size of an intersecting family is the cardinality of a point stabilizer.) However, it is only a conjecture that all intersecting families of maximum size are cosets of point stabilizers when $q > 3$. (See the second part of Conjecture 1 in [20].) In this paper, we prove that the second part of Conjecture 1 in [20] is true for all odd prime powers $q > 3$.

Theorem 1. *Let S be an intersecting family in $PSL(2, q)$ of maximum size, where $q > 3$ is an odd prime power. Then S is a coset of a point stabilizer.*

Note that when $q = 3$, we have $PSL(2, q) \cong A_4$, and the action of $PSL(2, q)$ on the projective line $PG(1, q)$ is equivalent to the (natural) action of A_4 on $\{1, 2, 3, 4\}$; in this case, it was pointed out in [16] that the set $S = \{(1), (123), (234)\}$ (we are using cycle notation for permutations), is an intersecting family of maximum size in A_4, but S is not a coset of any point stabilizer. To prove Theorem 1 we apply a general method for solving Problem II for some 2-transitive groups. This technique was described 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 which we define below.

Definition 2. 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 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 point stabilizers are the only intersecting families of maximum size for the symmetric group [12], the alternating group [2], $PGL(2, q)$ [20], and many other groups [3].

Thus, in order to prove Theorem 1 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 1 follows directly from the next theorem.

Theorem 3. *Let M be the derangement matrix of $PSL(2, q)$ acting on $PG(1, q)$, where $q > 3$ is an odd prime power. Then the $\mathbb{C}$-rank of M is $q(q - 1)$.*

Exactly the same statement for $PGL(2, q)$ is proved in [20, Prop. 9], so we must first examine why the proof does not immediately carry over to $PSL(2, q)$. In [20] 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 2.4). This is not a surprise; it is well known that these sums appear in connection with the complex representation theory of $PGL(2, q)$ [14]. To prove that these character sums are not equal to zero the following facts will be crucial:

(1) The Legendre and Soto-Andrade sums (see Definitions 7 and 8) on $\mathbb{F}_q$ form an orthogonal basis in the inner product space $\ell_2(\mathbb{F}_q, m)$ [14], where m is the measure assigning mass $q + 1$ to the points ± 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 2.3). These functions were introduced by Greene in [13] and Katz in [15] and since that time they have been extensively studied [1,11,14].

The rest of this paper is organized as follows. In Section 2, we provide some basic results about the character table of $PGL(2, q)$, Legendre and Soto-Andrade sums, and hypergeometric functions over finite fields. In Section 3, 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 4, we find some formulas to express those character sums over $PGL(2, q)$ in terms of Legendre and Soto-Andrade sums. In Section 5, we prove Theorem 3. In Section 6, we conclude with some remarks and open problems.

2. Background

We start by recalling standard facts about the groups $PGL(2, q)$ and $PSL(2, q)$ and their complex characters, introducing our notation in the process. We shall assume that the reader is familiar with the general terminology and basic results from the representation theory of finite groups over the complex field, as can be found in many textbooks, and we shall use [26] for specific references when necessary.

2.1. 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 2×2 matrices over $\mathbb{F}_q$ and $SL(2,q)$ the subgroup of all invertible 2×2 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 $PSL(2,q) = SL(2,q)/\left(SL(2,q) \cap Z(GL(2,q))\right)$. 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.

2.2. The character table of $PGL(2,q)$

We assume in this section and throughout this paper that q is an odd prime power. We briefly describe the character table of $PGL(2,q)$. We refer the reader to [23] 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 2×2 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 conjugate 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 $x = -1$. 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 $r \in \mathbb{F}_{q^2}^* \setminus (\mathbb{F}_q^* \cup i\mathbb{F}_q^*)$ and $q(q-1)/2$ if $r \in i\mathbb{F}_q^*$, where i is an element of $\mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ such that $i^2 \in \mathbb{F}_q^*$.

The complex irreducible characters of $PGL(2,q)$ are described in Table 1. They also come in four families. First the characters λ_1 and λ_{-1} correspond to representations of degree 1. Here λ_1 is the principal character and the values of λ_{-1} depend on a function δ 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.

Secondly, the characters ψ_1 and ψ_{-1} correspond to representations of degree q. The character ψ_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 ψ_{-1} depend on the function δ defined above.

The third 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 β in Table 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 β corresponds to a unique multiplicative character of $\mathbb{F}_{q^2}$ which is trivial on $\mathbb{F}_q^*$.

Finally, the fourth 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 values depend on multiplicative characters of $\mathbb{F}_q$. In fact, the label γ in Table 1 runs through all the homomorphism $\gamma : \mathbb{F}_q^* \to \mathbb{C}^*$ of order greater than 2 up to inversion.

Throughout this paper we denote by Γ and B a fixed selection of characters γ and β, 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 $\{\nu_\gamma\}_{\gamma\in\Gamma}$ and $\{\eta_\beta\}_{\beta\in B}$, respectively.

Table 1
Character table of $PGL(2,q)$.

	I	u	d_x	d_{-1}	v_r	v_i
λ_1	1	1	1	1	1	1
λ_{-1}	1	1	$\delta(x)$	$\delta(-1)$	$\delta(r)$	$\delta(i)$
ψ_1	q	0	1	1	-1	-1
ψ_{-1}	q	0	$\delta(x)$	$\delta(-1)$	$-\delta(r)$	$-\delta(i)$
η_β	$q-1$	-1	0	0	$-\beta(r)-\beta(r^q)$	$-2\beta(i)$
ν_γ	$q+1$	1	$\gamma(x)+\gamma(x^{-1})$	$2\gamma(-1)$	0	0

2.3. 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. For details, see [4].

Hypergeometric functions over finite fields were introduced independently by John Greene [13] and Nicholas Katz [15]. Note that the two definitions differ only in a normalizing factor for cases related to our discussion.

In this section and throughout this paper we denote by ϵ and ϕ the trivial and quadratic multiplicative characters of $\mathbb{F}_q$, respectively. Also throughout this paper we adopt the convention of extending multiplicative characters by declaring them to be zero at $0 \in \mathbb{F}_q$. For any multiplicative character γ, we use $\overline{\gamma}$ to denote its complex conjugation. A Gauss sum of γ is defined by $g(\gamma) := \sum_{x\in\mathbb{F}_q}\gamma(x)\theta(x)$ where θ is any nontrivial additive character of $\mathbb{F}_q$. 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

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

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 paper.

Following Greene [13], 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

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

See §4.4 of [11] for a comparison among different versions of finite field hypergeometric functions.

The following lemma is a generalization of Lemma 2.2 in [1].

Lemma 4. *For any non-trivial multiplicative character γ of $\mathbb{F}_q$,*

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

where $\phi(\cdot)$ denotes the quadratic character of $\mathbb{F}_q$.

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

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

Now replacing xy by z,

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

Letting $w=1/x$ and using (1) we get,

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

Like their classical counterparts hypergeometric functions over finite fields satisfy many transformation formulas [11,13]. In particular, the next one will be useful for our purpose.

Lemma 5. *(Greene, [13]) For $x \in \mathbb{F}_q$ with $x \neq 0$ we have,*

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

Proposition 6. *Let $n = 2, 3, 4$ or 6, $\mathbb{F}_q$ be any finite field of size q that is congruent to* 1 mod n, *and γ be any order n multiplicative character of $\mathbb{F}_q$. Then*

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

Proof. This proposition is a corollary of Theorem 2 of [19]. The background is about character sums in the perspective of hypergeometric motives [5,15,25] and we will only point out how to obtain our claim. Under the assumption on n, the choice of γ is unique up to complex conjugation and $\gamma(-1)$ is independent of the choice of γ. For each n, let $\boldsymbol{\alpha} = \{\frac{1}{n}, \frac{n-1}{n}, \frac{1}{2}, \frac{1}{2}\}$ and $\boldsymbol{\beta} = \{1, 1, 1, 1\}$ and ω be any order $(q-1)$ multiplicative character of $\mathbb{F}_q$. Thus either γ or γ^{-1} is $\omega^{(q-1)/n}$. The normalized Katz version of hypergeometric sum is defined as (see Definition 1.1 of [5])

$$ H_q(\boldsymbol{\alpha}, \boldsymbol{\beta}; \lambda) := \frac{1}{1-q} \sum_{k=0}^{q-2} \prod_{\alpha \in \boldsymbol{\alpha}} \frac{g(\omega^{k+(q-1)\alpha})}{g(\omega^{(q-1)\alpha})} \prod_{\beta \in \boldsymbol{\beta}} \frac{g(\omega^{-k-(q-1)\beta})}{g(\omega^{-(q-1)\beta})}\, \omega^k\big((-1)^m \lambda\big). \tag{2} $$

We take $\lambda = 1$ here. Then the conversion between Greene and the normalized Katz versions of hypergeometric finite sums says

$$ -q^3 \cdot {}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix};\ 1; q\right] = H_q(\boldsymbol{\alpha}, \boldsymbol{\beta}; 1), \tag{3} $$

independent of the choice of γ. Then Theorem 2 in [19] implies that there are two imaginary quadratic algebraic integers $A_{1,q}$ and $A_{2,q}$ (depending on both n and q) both of complex absolute values $q^{3/2}$ such that $H_q(\boldsymbol{\alpha}, \boldsymbol{\beta}; 1) = \phi(-1)\gamma(-1)q + A_{1,q} + A_{2,q}$. Thus

$$ \left| q^3 \cdot {}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix};\ 1; q\right] + \phi(-1)\gamma(-1)q \right| = |A_{1,q} + A_{2,q}| \le 2q^{3/2}. $$

The proof is now complete. □

2.4. 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

$$\langle f_1, f_2\rangle := \sum_{x\in\mathbb{F}_q} f_1(x)\overline{f_2(x)}m(x).$$

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

Definition 7. For any multiplicative character γ of $\mathbb{F}_q$, the *Legendre sum* with respect to γ 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 8. For any multiplicative character β of $\mathbb{F}_{q^2}$, the *Soto-Andrade sum* with respect to β 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 $PGL(2,q)$ [14]. 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 9. *(Kable, [14]) The set*

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

is an orthogonal basis for the space $\ell^2(\mathbb{F}_q, m)$, where Γ and B were defined in the end of Section 2.2 with $|\Gamma| = \frac{q-3}{2}$ and $|B| = \frac{q-1}{2}$. The square norm of the elements of this basis are as follows:

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

If we normalize the basis given by Lemma 9 then we can easily obtain an orthonormal basis of $\ell^2(\mathbb{F}_q, m)$. We denote the elements of this orthonormal basis by $\{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in \Gamma, \beta \in B\}$.

The next lemmas list some elementary properties of the Legendre and Soto-Andrade sums that we will need later. Lemma 10 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 11 shows that the Legendre and Soto-Andrade sums are easy to evaluate at ±1.

Lemma 10. *The values of the Legendre sum with respect to ϵ 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 11. *Let γ and β be characters from the sets Γ 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 $i \in \mathbb{F}^*_{q^2} \setminus \mathbb{F}_q$ such that $i^2 \in \mathbb{F}^*_q$.

Lemma 12. *The values of the Legendre and Soto-Andrade sums are real numbers. Moreover, for every $\gamma \in \Gamma$, $\beta \in B$ 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 establishes a relation between Legendre sums and hypergeometric sums over finite fields. This fact will be crucial later in this paper.

Lemma 13. *(Kable, [14]) If γ is a nontrivial character of $\mathbb{F}_q$ and $a \in \mathbb{F}_q \setminus \{\pm 1\}$ then*

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

3. 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.

3.1. 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 ∞ 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 14. Let Ω 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 Ω; 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 $\operatorname{rank}_{\mathbb{C}}(M) = \operatorname{rank}_{\mathbb{C}}(N)$. The next lemma gives information about the entries of N.

Lemma 15. *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) $N_{(a,b),(b,a)} = \begin{cases} 0, & \text{if } q \equiv 1 \ mod\ 4, \\ (q-1)/2, & \text{if } q \equiv 3 \ mod\ 4, \end{cases} \quad \forall (a,b) \in \Omega.$

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

(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

$$N_{(a,b),(c,d)} = N_{(a^g,b^g),(c^g,d^g)}, \tag{4}$$

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 15 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 Equation (4) 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 Equation (4) we can assume without loss of generality that $a = 0$ and $b = \infty$. The elements $g_\lambda \in PSL(2,q)$ sending 0 to ∞ and ∞ 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_λ and $g_{-\lambda}$ represent the same element of $PSL(2,q)$. Let ξ 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 ∞ and ∞ to 0.

  Recall that g_λ is a derangement if and only if its eigenvalues are not in $\mathbb{F}_q$. Thus, g_λ 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 $\mathbb{F}_q$. Thus, $p_\lambda(t)$ 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 $\lambda \in \mathbb{F}_q^*$. Therefore, $N_{(a,b),(b,a)} = N_{(0,\infty),(\infty,0)} = (q-1)/2$.

- **Case 4**.

  Every element of $PSL(2,q)$ sending 0 to ∞ 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_λ and $g_{-\lambda}$ represent the same element of $PSL(2,q)$. The matrix g_λ 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 λ 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 λ such that g_λ has eigenvalues $\{x,x^{-1}\}$, then they have to satisfy the following quadratic equation

$$\lambda^2-(x+x^{-1})\lambda+d=0. \tag{5}$$

– **Case 4 (a)**:

If we assume $d=0$ then $\lambda=0$ is a solution of Equation (5), however, that solution is not admissible by the definition of g_λ. 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 λ. In fact, we can relate to each set $\{x,x^{-1}\}$ a unique value of λ.

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 λ. Thus, the number of values of λ 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 λ. Thus, the number of values for λ 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 Equation (5) in $\mathbb{F}_q$ is given by $1+\phi((x+x^{-1})^2-4d)$. In this case, x and x^{-1} leads to the same value of λ. 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 $d \neq 0, 1, \infty$,

$$\begin{aligned}
&N_{(0,\infty),(1,d)}\\
&= \frac{1}{2}\left\{(q-1) - \left[2(1+\phi(1-d)) + \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_q^*\\ x\neq 1,-1}} (1+\phi((x+x^{-1})^2-4d))\right]\right\}\\
&= \frac{q-3}{4} - \frac{\phi(1-d)}{2} - \frac{1}{4}\sum_{\substack{x\in\mathbb{F}_q^*\\ x\neq 1,-1}} \phi((x+x^{-1})^2-4d)
\end{aligned}$$

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

Corollary 16. *Let $d \in \mathbb{F}_q$, $d \neq 0, 1$. The number of derangements of $PSL(2,q)$ sending 0 to ∞ and 1 to d can be expressed in terms of the Legendre sum with respect to ϕ. Specifically,*

$$N_{(0,\infty),(1,d)} = \frac{q-1}{4} - \frac{\phi(1-d)}{2} - \frac{q}{4}P_\phi(2d-1). \tag{6}$$

Proof. To prove this corollary, we compute

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

Next we replace x^2 by y. If $y \in \mathbb{F}_q^*$ is not a square, then $1+\phi(y)=0$; on the other hand, if $y \in \mathbb{F}_q^*$ is a square, then $x^2=y$ has $1+\phi(y)=2$ solutions. It follows that

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

Applying Theorem 5.48 from [18] it follows that,

$$\sum_{y\in\mathbb{F}_q}\phi(y^2-2(2d-1)y+1)=-1.$$

Thus, the above computations imply that

$$\sum_{x\in\mathbb{F}_q^*}\phi((x+x^{-1})^2-4d)=-2+qP_\phi(2d-1). \tag{7}$$

Now, Corollary 16 follows from part 4(b) of Lemma 15 and Equation (7). □

3.2. 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 Ω 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 $\{e_\omega\}_{\omega\in\Omega}$. 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_{ψ_1} each irreducible module of $PGL(2,q)$ appears exactly once.

Let (χ,ψ) denote the inner product of the characters χ and ψ of $PGL(2,q)$ (see [26, Section 2.3]).

Lemma 17. *Let V_χ denote an irreducible module of $PGL(2,q)$ with character χ. Then the decomposition of V into irreducible constituents is given by,*

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

Proof. Let π 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 π has an easy description given by the following table

	1	u	d_x	v_r
π	$q(q+1)$	0	2	0

.

Now let V_χ be an irreducible representation of $PGL(2,q)$ and χ its irreducible character. It is known ([26, Chapter 2, Theorem 4]) that the multiplicity of V_χ in V is equal to the character inner product (π, χ). Thus, the lemma follows by direct calculation using the character table of $PGL(2,q)$. □

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

$$l_{a,b} := \sum_{\substack{p \in PG(1,q) \\ p \neq a,b}} (e_{(a,p)} - e_{(b,p)}) + e_{(a,b)} - e_{(b,a)}, \tag{8}$$

$$r_{a,b} := \sum_{\substack{p \in PG(1,q) \\ p \neq a,b}} (e_{(p,a)} - e_{(p,b)}) + e_{(b,a)} - e_{(a,b)}. \tag{9}$$

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

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

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

Lemma 18. *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 Equations (8) and (9) 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 see 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

$$v = \sum_{\substack{p \in PG(1,q)\\ p \neq a}} \alpha_p l_{a,p} = \sum_{\substack{p \in PG(1,q)\\ p \neq a}} \beta_p r_{a,p} \tag{10}$$

where not all α_p and β_p are equal to zero.

For a fixed $b \in PG(1,q)$, the vector $l_{a,b}$ is the only one in the set $\{l_{a,p}\}_{p \in PG(1,q), p \neq a}$ that contains $e_{(b,a)}$. On the other hand, every vector of the form $r_{a,p}$ with $p \neq a$ contains $e_{(b,a)}$. Therefore, using Equation (10) we get

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

which implies that the values of the coefficients α_p in Equation (10) are all the same. Analogously, we can show that the values β_p in Equation (10) are the same. Thus, we can rewrite Equation (10) as follows,

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

where $\alpha = \sum_{p \neq a} \beta_p$ and $\beta = \sum_{p \neq a} \alpha_p$. This implies that $\alpha = q\beta = q^2\alpha$, a contradiction, because q is not equal to one.

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 θ 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 θ to all elements of V_1 linearly. Now, from the definition of θ 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, θ is a $PGL(2,q)$-module isomorphism. This completes the proof of part (4). □

Lemma 19. *The submodules V_1 and V_2 are isomorphic to V_{ψ_1}.*

Proof. This result follows directly from Lemmas 17 and 18. If we consider the decomposition of V into irreducible constituents, we note that each irreducible representation appears only once, except for V_{ψ_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 20. *The linear transformation T_N defined above is a $PGL(2,q)$-module homomorphism from V to V.*

Proof. To prove the lemma we have to show that the linear transformation T_N respects the action of $PGL(2,q)$ on V; that is, for each $g \in PGL(2,q)$ and each $(a,b) \in \Omega$,

$$T_N(e_{(a,b)} \cdot g) = T_N(e_{(a,b)}) \cdot g. \tag{11}$$

First, consider the left hand side of Equation (11). From the definition of T_N it follows that

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

Now, note that the right hand side of Equation (11) can be written as

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

Furthermore, recall that $N_{(a,b),(c,d)} = N_{(a^g,b^g),(c^g,d^g)}$ for all $g \in PGL(2,q)$. Therefore,

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

which implies that Equation (11) holds. This completes the proof of the lemma. □

3.3. 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 20) 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 21. *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 Ω. 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 fixed $a \in PG(1,q)$ 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 19 and 21, 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 χ 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_χ is zero or is equal to the dimension of V_χ. Hence, to study the image of V_χ under T_N for any $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta \in B}, \{\nu_\gamma\}_{\gamma \in \Gamma}\}$ we proceed in the following way:

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

(2) Project $e_{(0,\infty)}$ onto V_χ 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_χ 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 ∞ 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:

$$T_{N,\chi} := T_N(E_\chi(e_{(0,\infty)}))_{(0,\infty)} = \sum_{(a,b)\in\Omega}\left[\sum_{0^g=a,\infty^g=b}\chi(g^{-1})\right]N_{(0,\infty),(a,b)}, \tag{12}$$

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

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

$$\sum_\chi \dim(V_\chi) \le \operatorname{rank}(M), \tag{13}$$

where χ in the sum on the left hand side of (13) runs through $\{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in\Gamma}\}$ such that $T_{N,\chi} \neq 0$. In particular, if $T_{N,\chi}$ is not zero for all $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in\Gamma}\}$ then the rank of the derangement matrix M is equal to $q(q-1)$. We conclude that to prove Theorem 3, it is enough to show that the values of the character sums $T_{N,\chi}$ with $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in\Gamma}\}$ are not equal to zero. This will be our objective in the next two sections.

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

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 a and ∞ to b for any $a, b \in PG(1,q)$. Therefore, we can compute (12) 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 15 to obtain the last equality. Thus, from the analysis given in Section 3.3 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 $\chi \in \{\psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in\Gamma}\}$ which will be helpful to write Equation (12) in terms of character sums over finite fields.

Lemma 22. *Let χ be any irreducible character of $PGL(2,q)$ from the set $\{\psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in\Gamma}\}$. Let h be the unique element of $PGL(2,q)$ sending 0 to 0, 1 to ∞, and ∞ to 1. If $q \equiv 1$ mod 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 $q \equiv 3$ *mod* 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. We start by presenting some results on character sums over $PGL(2,q)$ that we will need.

We denote by $PGL(2,q)_{0,\infty}$ the subgroup of $PGL(2,q)$ fixing 0 and ∞. Analogously, $PGL(2,q)_0$ denotes the subgroup of $PGL(2,q)$ fixing 0. Applying the Frobenius Reciprocity Theorem [26, Chapter 7, Theorem 13], we have:

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

where π is the permutation character defined in the proof of Lemma 17 and 1 is the trivial character of the groups $PGL(2,q)_{0,\infty}$ and $PGL(2,q)_0$, respectively. Using these equalities and the decomposition of π in terms of irreducible characters (which was given in Lemma 17), we evaluate the following character sums:

$$\sum_{0^g=0,\infty^g=\infty} \chi(g^{-1}) = (q-1)(\mathrm{Res}(\chi),1)_{PGL(2,q)_{0,\infty}} = (q-1)(\chi,\pi)_{PGL(2,q)} = q-1,$$

and

$$\sum_{0^g=0} \chi(g^{-1}) = q(q-1)(\mathrm{Res}(\chi),1)_{PGL(2,q)_0} = q(q-1)(\chi,\lambda_1+\psi_1)_{PGL(2,q)} = 0.$$

Note that $\chi(kgk^{-1}) = \chi(g)$ for any $k \in PGL(2,q)$ since χ is a character, hence a class function. This fact implies many relations between character sums over $PGL(2,q)$. In particular,

$$\sum_{a^g=b} \chi(g^{-1}) = \sum_{(a^k)^g=(b^k)^g} \chi(g^{-1}), \tag{14}$$

and

$$\sum_{a^g=b,c^g=d} \chi(g^{-1}) = \sum_{(a^k)^g=b^k,(c^k)^g=d^k} \chi(g^{-1}). \tag{15}$$

We claim that $\sum_{0^g=\infty} \chi(g^{-1}) = 0$. To prove this claim, recall that χ is a non-trivial character of $PGL(2,q)$. Therefore,

$$0 = \sum_{g\in PGL(2,q)} \chi(g^{-1}) = \sum_{0^g=0} \chi(g^{-1}) + \sum_{\substack{a\in PG(1,q)\\ a\neq 0}} \sum_{0^g=a} \chi(g^{-1}).$$

Since $\sum_{0^g=0} \chi(g^{-1}) = 0$, we conclude that

$$0 = \sum_{\substack{a\in PG(1,q)\\ a\neq 0}} \sum_{0^g=a} \chi(g^{-1}) = q \sum_{0^g=\infty} \chi(g^{-1}),$$

where Equation (14) is used to obtain the last equality.

Moreover, it follows from the above equations and the 2-transitivity of the action of $PGL(2,q)$ on $PG(1,q)$ that

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

Now, we are ready to prove Lemma 22. From Equation (12) and Lemma 15 we get,

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

First, assume that $q \equiv 1 \pmod 4$. From Lemma 15 it follows that

$$N_{(0,\infty),(\infty,b)} = N_{(0,\infty),(a,0)} = (q-1)/4$$

for all $a, b \in \mathbb{F}_q^*$, and

$$N_{(0,\infty),(\infty,0)} = 0.$$

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

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

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 (4) we conclude that $N_{(0,\infty),(a,b)} = N_{(0,\infty)(1,b^k)}$ where $k \in PGL(2, q)$ is the unique element sending 0 to 0, ∞ to ∞ and a to 1. Moreover, applying Equation (15) we obtain

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

Putting all these facts together we conclude that

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

Thus, Lemma 22 is proved for the case where $q \equiv 1 \bmod 4$. Similar computations work for the case when $q \equiv 3 \bmod 4$. □

It follows from Lemma 22 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 written in terms of character sums over finite fields for all $\chi \in \{\psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in\Gamma}\}$.

Lemma 23. *Let i be an element of $\mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ such that $i^2 \in \mathbb{F}_q^*$. Then,*

$$\sum_{0^g=\infty,\infty^g=0} \psi_{-1}(g^{-1}) = \phi(-1)(q-1),$$

$$\sum_{0^g=\infty,\infty^g=0} \nu_\gamma(g^{-1}) = \gamma(-1)(q-1) \quad \textit{for all } \gamma \in \Gamma,$$

$$\sum_{0^g=\infty,\infty^g=0} \eta_\beta(g^{-1}) = -\beta(i)(q-1) \quad \textit{for all } \beta \in B.$$

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

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

Note that the characteristic polynomial of g_λ is $p_\lambda(t) := t^2 - \lambda$.

To evaluate the character sums in this lemma we need to know to which conjugacy classes the elements g_λ belong.

First, recall that the eigenvalues of g_λ are defined up to multiplication by an element of $\mathbb{F}_q^*$. Now, if λ is a square in $\mathbb{F}_q^*$ then $p_\lambda(t)$ is reducible and g_λ has eigenvalues $\pm\sqrt{\lambda} \in \mathbb{F}_q^*$. This implies that g_λ lies in the conjugacy class d_{-1} whenever λ is a square. On the other hand, if λ 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 λ is not a square we see that g_λ 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 $PGL(2,q)$. □

Lemma 24. *For every $\gamma \in \Gamma$ 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 ∞ 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 α correspond to the same element g_λ in $PGL(2,q)$. Indeed, as was remarked earlier the eigenvalues of g_λ are defined up to scalar multiplication.

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

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

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_λ are $\{1, x\}$ for some $x \in \mathbb{F}_q^*$. This implies that g_λ is contained in the same conjugacy class as d_x (see Section 2.2). Here, we assume that d_x with $x = 1$ corresponds to the element $u \in PGL(2, q)$ defined in Section 2.2.

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 α such that g_λ has eigenvalues $\{1, x\}$. From the above analysis it is clear that d, x, α and λ 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 α satisfies the following quadratic equation,

$$d\alpha^2 - (x+1)\alpha + x = 0.$$

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_λ is conjugate to d_x is equal to

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

Now using the above remarks and the character table of $PGL(2, q)$ we get

$$\begin{aligned}\sum_{0^g=\infty,1^g=d} \nu_\gamma(g) = (1+\phi(1-d))\gamma(1) + \left(\frac{1+\phi(d)}{2}\right)(2\gamma(-1)) \\ +\frac{1}{2}\sum_{\substack{x\neq 1,-1\\ x\in\mathbb{F}_q^*}} (1+\phi((x+1)^2-4xd))(\gamma(x)+\gamma(x^{-1}))\end{aligned} \tag{16}$$

where the first two terms in the right hand side of Equation (16) corresponds to $x = 1$ and $x = -1$. Furthermore, note that we have included a factor $\frac{1}{2}$ in front of the last expression in Equation (16). This occurs because every element g_λ 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 λ. Simplifying the right hand side of Equation (16),

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

Finally, applying basic properties of characters and Lemma 12 we obtain

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

The proof is now complete. □

Lemma 25. *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 all the elements in $PGL(2,q)$ sending 0 to ∞ and 1 to d 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 2.2).

We know that if $r \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ is an eigenvalue of g_λ then g_λ 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_λ then this implies that g_λ 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 α such that g_λ has eigenvalues $\{r, r^q\}$. From the characteristic polynomial of g_λ 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

$$d\alpha^2 - (r + r^q)\alpha + r^{q+1} = 0. \tag{17}$$

Distinct solutions of Equation (17) generate distinct values of λ unless $r \in i\mathbb{F}_q$ where i is an element of $\mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ such 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_λ 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_λ 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 values of λ for every $a \in \mathbb{F}_q^*$. Therefore,

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

Now, the lemma follows from Definition 8 and Lemma 12. □

Lemma 26. *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

$$\psi_{-1}(g) = \begin{cases} 0, & \text{if } g \in u,\\ 1, & \text{if } g \in d_x \text{ and } d_x \subset PSL(2,q),\\ -1, & \text{if } g \in d_x \text{ and } d_x \subset PGL(2,q)\setminus PSL(2,q),\\ -1, & \text{if } g \in v_r \text{ and } v_r \subset PSL(2,q),\\ 1, & \text{if } g \in v_r \text{ and } v_r \subset PGL(2,q)\setminus PSL(2,q). \end{cases} \tag{18}$$

Thus, to evaluate the sum $\sum_g \psi_{-1}(g)$ we need to know: how many elements sending 0 to ∞ and 1 to d belong to each of the five categories considered in (18). In fact, these counting problems follow from the proof of Case (4) of Lemma 15.

For the sake of clarity, we recall some simple facts. There are $q-1$ elements in $PGL(2,q)$ sending 0 to ∞ and 1 to d, and half of them are in $PSL(2,q)$. It was proved by Meagher and Spiga [20] 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 ∞ and 1 to d into three categories:

- 2 elements, each fixing exactly one point.
- $\displaystyle\frac{1}{4}\sum_{x\in\mathbb{F}_q^*,x\neq 1,-1}(1+\phi((x+x^{-1})^2-4d))$ elements, each fixing exactly two points.
- $\displaystyle\frac{q-5}{4}-\frac{1}{4}\sum_{x\in\mathbb{F}_q^*}\phi((x+x^{-1})^2-4d)$ elements 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 ∞ and 1 to d,

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

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

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

Here the last equality above follows from Equation (7).

The case where $(1-d)$ is not a square can be treated by similar computations. We omit the details. □

5. The restriction of T_N onto $V_{\psi_{-1}}$, V_{ν_γ} and V_{η_β}

In this section, we study the restriction of T_N onto the irreducible constituents, $V_{\psi_{-1}}$, $\{V_{\nu_\gamma}\}_{\gamma\in\Gamma}$ and $\{V_{\eta_\beta}\}_{\beta\in B}$, of V. We start with a technical lemma that will be useful for studying the character sums $T_{N,\chi}$ with $\chi\in\{\psi_{-1},\{\eta_\beta\}_{\beta\in B},\{\nu_\gamma\}_{\gamma\in\Gamma}\}$. In the statement of the lemma below, h is the same as defined in Lemma 22.

Lemma 27. *Let i be an element of $\mathbb{F}_{q^2}^*\setminus\mathbb{F}_q^*$ such that $i^2\in\mathbb{F}_q^*$. Then for all $\gamma\in\Gamma$,*

$$T_{N,\nu_\gamma}=\frac{(q-1)}{4}\left[q^2-3q-(q+1)\,\gamma(-1)\phi(-1)-q^2\sum_{b\in\mathbb{F}_q^*,b\neq1}P_\gamma(2b^h-1)P_\phi(2b-1)\right].$$

Also, for all $\beta\in B$,

$$T_{N,\eta_\beta}=\frac{(q-1)}{4}\left[q^2+q+(q+1)\,\beta(i)\phi(-1)+q^2\sum_{b\in\mathbb{F}_q^*,b\neq1}R_\beta(2b^h-1)P_\phi(2b-1)\right],$$

and

$$T_{N,\psi_{-1}}=\frac{(q-1)}{4}\left[q^2-2q-3-q^2\sum_{b\in\mathbb{F}_q^*,b\neq1}P_\phi(2b^h-1)P_\phi(2b-1)\right].$$

Proof. We will prove that the expression for T_{N,ν_γ} holds for every $\gamma\in\Gamma$. The proofs for the characters sums T_{N,η_β} and $T_{N,\psi_{-1}}$ are similar; we omit those details.

First, assume that $q\equiv1 \bmod 4$. It follows from Lemma 22 that

$$\begin{aligned}T_{N,\nu_\gamma}&=\frac{(q-1)^3}{4}-\frac{q-1}{2}\sum_{0^g=\infty,\infty^g=0}\nu_\gamma(g^{-1})\\&\quad+(q-1)\sum_{\substack{b\in\mathbb{F}_q^*\\b\neq1}}\left[\sum_{0^g=\infty,1^g=b^h}\nu_\gamma(g^{-1})\right]N_{(0,\infty),(1,b)}\\&=\frac{(q-1)^3}{4}-\frac{(q-1)^2}{2}\gamma(-1)+(q-1)\sum_{\substack{b\in\mathbb{F}_q^*\\b\neq1}}\left[\sum_{0^g=\infty,1^g=b^h}\nu_\gamma(g^{-1})\right]N_{(0,\infty),(1,b)},\end{aligned}$$

where for the last equality we have applied Lemma 23. Also, recall that $h\in PGL(2,q)$ is the unique element sending 0 to 0, 1 to ∞ and ∞ to 1.

Let us define

$$S := \sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} \left[\sum_{0^g=\infty,1^g=b^h} \nu_\gamma(g^{-1}) \right] N_{(0,\infty),(1,b)}.$$

Applying Corollary 16 and Lemma 24 we obtain

$$\begin{aligned} S &= \sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} qP_\gamma(2b^h-1)\left(\frac{q-1}{4} - \frac{\phi(1-b)}{2} - \frac{1}{4}P_\phi(2b-1)\right) \\ &= \frac{q(q-1)}{4}\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} P_\gamma(2b^h-1) - \frac{q}{2}\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} \phi(1-b)P_\gamma(2b^h-1) \\ &\quad - \frac{q^2}{4}\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} P_\gamma(2b^h-1)P_\phi(2b-1). \end{aligned}$$

We now simplify the first two character sums in the above expression for S.

The following computation uses the connection between Legendre sums and hypergeometric sums given by Lemma 13. We have

$$\begin{aligned} \sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} P_\gamma(2b^h-1) &= \sum_{\substack{a\in\mathbb{F}_q\\ a\neq \pm 1}} P_\gamma(a) \\ &= \sum_{\substack{a\in\mathbb{F}_q\\ a\neq \pm 1}} {}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \epsilon\end{matrix};\ \frac{1-a}{2};q\right]. \end{aligned}$$

Now, using Greene's definition of hypergeometric sums given in Equation (21) we get

$$\begin{aligned} \sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} P_\gamma(2b^h-1) &= \frac{\gamma^{-1}(-1)}{q}\sum_{\substack{a\in\mathbb{F}_q\\ a\neq \pm 1}}\sum_{x\in\mathbb{F}_q} \gamma^{-1}(x)\gamma(1-x)\gamma^{-1}\left(1-\frac{1}{2}(1-a)x\right) \\ &= \frac{\gamma^{-1}(-1)}{q}\sum_{x\in\mathbb{F}_q^*} \gamma^{-1}(x)\gamma(1-x)\sum_{\substack{a\in\mathbb{F}_q\\ a\neq \pm 1}} \gamma^{-1}\left(1-\frac{1}{2}(1-a)x\right) \\ &= \frac{\gamma^{-1}(-1)}{q}\sum_{x\in\mathbb{F}_q^*} \gamma^{-1}(x)\gamma(1-x)(-1-\gamma^{-1}(1-x)) \\ &= \frac{1}{q}(1+\gamma(-1)). \end{aligned}$$

On the other hand, to compute the second sum we use the definition of Legendre sums given in Definition 7 and noting that $\phi(-1) = 1$ when $q \equiv 1 \mod 4$,

$$\begin{aligned}\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} \phi(1-b)P_\gamma(2b^h-1) &= \frac{1}{q}\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}} \phi(1-b)\sum_{x\in\mathbb{F}_q^*}\gamma(x)\phi(1+(2-4b^h)x+x^2)\\ &= \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\gamma(x)\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}}\phi((x+1)^2-4b^hx)\phi(b-1)\\ &= \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\gamma(x)\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}}\phi((x-1)^2b-(x+1)^2)\\ &= \frac{1}{q}\sum_{x\in\mathbb{F}_q^*,x\neq 1}\gamma(x)\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}}\phi((x-1)^2b-(x+1)^2)+\frac{1}{q}\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}}\phi(-4)\\ &= \frac{1}{q}\sum_{x\in\mathbb{F}_q^*,x\neq 1}\gamma(x)(-\phi(-4x)-\phi(-(x+1)^2))+\frac{q-2}{q}\\ &= 1+\frac{1}{q}\gamma(-1).\end{aligned}$$

Putting all the above results together we have

$$S = -\frac{(q-1)}{4}+\frac{(q-3)}{4}\gamma(-1)-\frac{q^2}{4}\sum_{\substack{b\in\mathbb{F}_q^*\\ b\neq 1}}P_\gamma(2b^h-1)P_\phi(2b-1),$$

and plugging S into the expression for T_{N,ν_γ} we obtain

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

The computations for the case $q \equiv 3 \bmod 4$ are very similar. In fact, the following expression is obtained for T_{N,ν_γ} assuming that $q \equiv 3 \bmod 4$,

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

Finally, note that $\phi(-1) = 1$ when $q \equiv 1 \bmod 4$ and $\phi(-1) = -1$ when $q \equiv 3 \bmod 4$. This fact completes the proof of the Lemma. □

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_{η_β} is a $PGL(2,q)$-module isomorphism for every $\beta \in B$.

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_ϕ,

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

where we have used Lemma 9 in the last equality.

Theorem 28. *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 $\beta \in B$. From Lemma 27 it follows that

$$T_{N,\eta_\beta} = \frac{(q-1)}{4}\left[q^2 + q + (q+1)\,\beta(i)\phi(-1) + q^2 \sum_{b\in\mathbb{F}_q^*, b\neq 1} R_\beta(2b^h - 1)P_\phi(2b-1)\right], \tag{19}$$

where $i \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ such that $i^2 \in \mathbb{F}_q^*$. We will show that the expression on the right hand side of Equation (19) is not equal to zero.

We claim that the character sum

$$\sum_{b\in\mathbb{F}_q^*, b\neq 1} R_\beta(2b^h - 1)P_\phi(2b-1) \tag{20}$$

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 ∞ and ∞ 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 (20) 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 13 and the transformation formula in Lemma 5, the following expression for $P_\phi(2b^h-1)$ is obtained

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

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 $\mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ such that $i^2 \in \mathbb{F}_q^*$. Therefore, plugging in the above expression into Equation (19), we can also express T_{N,η_β} in terms of the function f,

$$T_{N,\eta_\beta} = \frac{q^2(q-1)}{4}\left[1+\frac{1}{q}+\phi(2)\left(1+\frac{1}{q}\right)^{1/2}\langle f, R'_\beta\rangle\right]. \tag{21}$$

Note that Equation (21) implies that if $|\langle f, R'_\beta\rangle| \le 1$ then $T_{N,\eta_\beta} \neq 0$. We claim that $|\langle f, R'_\beta\rangle| \le 1$ for every $\beta \in B$; note that the theorem follows from the validity of this claim.

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

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

Analogously, the squared norm of f can also be expressed in terms of this orthonormal basis,

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

where we have used the fact the coefficients in the expansion of f are all real (cf. Lemma 12).

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 $g \in$

$\{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in \Gamma, \beta \in B\}$. In particular, $\langle f, R'_\beta\rangle^2 \le 1 - 1/q - 2/q^2$ for all $\beta \in B$. Thus, our claim is proved. □

Unfortunately, the argument used in the proof of Theorem 28 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 [14].

Lemma 29. *Let γ 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 Lemmas 4 and 13 we obtain,

$$\begin{aligned}\phi(2)q^2\langle f, P_\gamma\rangle &= \phi(2)q^2\sum_{\substack{x\in\mathbb{F}_q\\ x\neq\pm1}}\phi(1-x)P_\phi(x)P_\gamma(x) + q^2P_\phi(-1)P_\gamma(-1)m(-1)\\ &= q^2\sum_{\substack{y\in\mathbb{F}_q^*\\ y\neq1}}\phi(y){}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix};\ y; q\right]{}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \epsilon\end{matrix};\ y; q\right] + \phi(-1)\gamma(-1)(q+1)\\ &= q^2\sum_{y\in\mathbb{F}_q}\phi(y){}_2\mathbb{F}_1\left[\begin{matrix}\phi & \phi \\ & \epsilon\end{matrix};\ y; q\right]{}_2\mathbb{F}_1\left[\begin{matrix}\gamma & \gamma^{-1} \\ & \epsilon\end{matrix};\ y; q\right] + \phi(-1)\gamma(-1)q\\ &= q^3{}_4\mathbb{F}_3\left[\begin{matrix}\gamma & \gamma^{-1} & \phi & \phi \\ & \epsilon & \epsilon & \epsilon\end{matrix};\ 1; q\right] + \phi(-1)\gamma(-1)q. \quad \square\end{aligned}$$

Theorem 30. *If $q \ge 7$ then,*

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

Proof. It suffices to show that $T_{N,\psi_{-1}} \neq 0$. It follows from Lemma 27 that

$$T_{N,\psi_{-1}} = \frac{(q-1)}{4}\left[q^2 - 2q - 3 - q^2\sum_{b\in\mathbb{F}_q^*, b\neq1}P_\phi(2b^h-1)P_\phi(2b-1)\right].$$

Let f be the function in $\ell^2(\mathbb{F}_q, m)$ defined before the statement of Theorem 28. By Lemmas 5 and 13 we see that the sum

$$\sum_{b\in\mathbb{F}_q^*, b\neq1}P_\phi(2b^h-1)P_\phi(2b-1)$$

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:

$$T_{N,\psi_{-1}} = \frac{(q-1)}{4}\left[q^2-q-2-\phi(2)q^2\langle f,P_\phi\rangle\right]. \tag{22}$$

We claim that $\phi(2)q^2\langle f,P_\phi\rangle \leq 2q^{3/2}$. This claim together with Equation (22) 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 29,

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

Therefore, our claim follows directly from the final conclusion of Proposition 6. □

To study the restriction of T_N onto V_{ν_γ} we consider two cases. First, if γ 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 28 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 γ has order three, four or six. The next theorem deals with these cases.

Theorem 31. *Assume that $q\geq 11$. If $\gamma\in\Gamma$ then*

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

Proof. We proceed as we did in the proof of Theorem 28. Thus, to prove this theorem it is enough to show that $T_{N,\nu_\gamma}\neq 0$. It follows from Lemma 27 that

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

Applying Lemmas 5 and 13 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

$$T_{N,\nu_\gamma} = \frac{q^2(q-1)}{4}\left[1 - \frac{3}{q} - \phi(2)\left(1-\frac{1}{q}\right)^{1/2}\langle f, P'_\gamma\rangle\right]. \tag{23}$$

Recall that

$$\|f\|^2 = \langle f, P'_\epsilon\rangle^2 + \langle f, P'_\phi\rangle^2 + \sum_\gamma \langle f, P_\gamma\rangle^2 + \sum_\beta \langle f, R'_\beta\rangle^2 = 1 - \frac{1}{q} - \frac{2}{q^2}, \tag{24}$$

where $\{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in \Gamma, \beta \in B\}$ is an orthonormal basis of $\ell^2(\mathbb{F}_q, m)$. Equation (24) implies that at most one of the coefficients $\langle f, g\rangle$ with $g \in \{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in \Gamma, \beta \in B\}$ can be close to 1. On the other hand, it is clear from (23) 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 $\gamma \in \Gamma$ such that $T_{N,\nu_\gamma} = 0$. Hence, it follows from equation (23) that

$$\langle f, P'_\gamma\rangle^2 = 1 - \frac{5}{q} + \frac{4}{q(q-1)}. \tag{25}$$

Let $\mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$ be the Galois group where ζ_{q-1} is a primitive $(q-1)$-th root of the unity. If γ 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 σ to both sides of (25) 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 $g \in \{P'_\epsilon, P'_\phi, P'_\gamma, R'_\beta : \gamma \in \Gamma, \beta \in B\}$ can be close to 1. Assume now $\gamma \in \Gamma$ is a character of order 3, 4 or 6. From equation (23) we get the following expression for T_{N,ν_γ},

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

By Lemma 29,

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

Now applying Proposition 6, we conclude that $T_{N\nu_\gamma} \neq 0$. □

Finally, we are ready to prove Theorem 3.

Proof of Theorem 3. Recall that in Section 3.3 we proved the following lower and upper bounds on the rank of the derangement matrix M of $PSL(2,q)$ acting on $PG(1,q)$,

$$\sum_{\{\chi : T_{N,\chi} \neq 0\}} \dim(V_\chi) \leq \operatorname{rank}(M) \leq q(q-1). \tag{26}$$

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

If $q \geq 11$ then it follows from Theorems 28, 30 and 31 that $T_{N,\chi} \neq 0$ for all $\chi \in \{\lambda_1, \psi_{-1}, \{\eta_\beta\}_{\beta\in B}, \{\nu_\gamma\}_{\gamma\in\Gamma}\}$. Furthermore, for each odd prime power q, $3 < q < 11$, we use a computer to check that the rank of M is exactly $q(q-1)$. □

6. Conclusions

In this paper 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 [20,3] that the maximum size of an intersecting family in $PSL(2,q)$ is $q(q-1)/2$. Meagher and Spiga [20] conjectured that the cosets of point stabilizers are the only intersecting families of maximum size in $PSL(2,q)$, when $q > 3$ is an odd prime power. 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 $PSL(2,q)$. To present this problem we introduce the notion of stability.

Let X be a finite set and G a finite group acting on X. Recall that a subset S of G is said to be an intersecting family if for any $g_1, g_2 \in S$ there exists an element $x \in X$ such that $x^{g_1} = x^{g_2}$. We will refer to intersecting families of maximum size as *extremal families*. Moreover, intersecting families whose sizes are close to the maximum are called *almost extremal families*. We say that the extremal families of a group G acting on X are *stable* if almost extremal families are similar in structure to the extremal ones.

The stability of intersecting families has been studied during the past few years (cf. [7,8,24]). Consider the action of S_n on $[n]$. As was remarked in the introduction, the size of extremal families in S_n is $(n-1)!$ and every extremal family is a coset of a point stabilizer. Furthermore, the stability of extremal families in S_n was established by Ellis [7], 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. Analogously, the same problems were solved for the group $PGL(2,q)$ acting on $PG(1,q)$. In fact, the size of extremal families in $PGL(2,q)$ is $q(q-1)$ and every extremal family is a coset of a point stabilizer. Recently, in [24] it was proved that the extremal families in $PGL(2,q)$ are stable.

We conjecture that the extremal families in $PSL(2,q)$ are also stable. The precise statement is given below.

Conjecture 32. Let S be an intersecting family in $PSL(2, q)$ with $q > 3$ 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.

Acknowledgments

The authors would like to thank the reviewers for their helpful comments.

References

[1] S. Ahlgren, K. Ono, A Gaussian hypergeometric series evaluation and Apery number congruences, J. Reine Angew. Math. 518 (2000) 187–212.
[2] B. Ahmadi, K. Meagher, A new proof for the Erdős–Ko–Rado Theorem for the alternating group, Discrete Math. 324 (2014) 28–40.
[3] B. Ahmadi, K. Meagher, The Erdős–Ko–Rado property for some 2-transitive groups, Ann. Comb. 19 (2015) 621–640.
[4] George E. Andrews, R. Askey, R. Roy, Special Functions, Encyclopedia Math. Appl., vol. 71, Cambridge University Press, Cambridge, 1999, xvi+664 pp.
[5] F. Beukers, H. Cohen, A. Mellit, Finite hypergeometric functions, Pure Appl. Math. Q. 11 (2015) 559–589.
[6] P.J. Cameron, C.Y. Ku, Intersecting families of permutations, European J. Combin. 24 (2003) 881–890.
[7] D. Ellis, A proof of the Cameron–Ku conjecture, J. Lond. Math. Soc. 85 (2012) 165–190.
[8] D. Ellis, E. Friedgut, Y. Filmus, A quasi-stability result for dictatorships in S_n, Combinatorica 35 (2015) 573–618.
[9] P. Erdős, C. Ko, R. Rado, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. (2) 12 (1961) 313–320.
[10] P. Frankl, M. Deza, On the maximum number of permutations with given maximal or minimal distance, J. Combin. Theory Ser. A 22 (1977) 352–360.
[11] J.G. Fuselier, L. Long, R. Ramakrishna, H. Swisher, F. Tu, Hypergeometric functions over finite fields, arXiv:1510.02575.
[12] C. Godsil, K. Meagher, A new proof of the Erdős–Ko–Rado theorem for intersecting families of permutations, European J. Combin. 30 (2009) 404–414.
[13] J. Greene, Hypergeometric functions over finite fields, Trans. Amer. Math. Soc. 301 (1987) 77–101.
[14] A. Kable, Legendre sums, Soto-Andrade sums and Kloosterman sums, Pacific J. Math. 206 (2002) 139–157.
[15] N.M. Katz, Exponential Sums and Differential Equations, Ann. of Math. Stud., vol. 124, 1990.
[16] C.Y. Ku, T.W.H. Wong, Intersecting families in the alternating group and direct product of symmetric groups, Electron. J. Combin. 14 (2007) R25.
[17] B. Larose, C. Malvenuto, Stable sets of maximal size in Kneser-type graphs, European J. Combin. 25 (2004) 657–673.
[18] R. Lidl, H. Niederreiter, Finite Fileds, Encyclopedia Math. Appl., 1997.
[19] L. Long, F.T. Tu, N. Yui, W. Zudilin, Supercongruences for rigid hypergeometric Calabi–Yau threefolds, arXiv:1705.01663.
[20] K. Meagher, P. Spiga, An Erdős–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.
[21] K. Meagher, P. Spiga, An Erdős–Ko–Rado theorem for the derangement graph of $PGL_3(q)$ acting on the projective plane, SIAM J. Discrete Math. 28 (2014) 918–941.
[22] K. Meagher, P. Spiga, P.H. Tiep, An Erdős–Ko–Rado theorem for finite 2-transitive groups, European J. Combin. 55 (2016) 100–118.
[23] I. Piatetski-Shapiro, Complex Representations of $GL(2, K)$ for finite fields K, Contemp. Math. (1983).
[24] R. Plaza, Stability for Intersecting Families in $PGL(2, q)$, Electron. J. Combin. 22 (4) (2015) 4.41, 14pp.
[25] F. Rodriguez-Villegas, Hypergeometric motives, Lecture notes.
[26] J.P. Serre, Linear Representations of Finite Groups, Grad. Texts in Math., Springer, 1977.