Proofs of two conjectures on the dimensions of binary codes

Junhua Wu

Received: 18 June 2011 / Revised: 15 April 2012 / Accepted: 19 April 2012 / Published online: 6 May 2012
© Springer Science+Business Media, LLC 2012

Abstract Let \( L \) and \( L_0 \) be the binary codes generated by the column \( \mathbb{F}_2 \)-null spaces of the incidence matrices of external points versus passant lines and internal points versus secant lines with respect to a conic in \( \text{PG}(2, q) \), respectively. We confirm the conjectures on the dimensions of \( L \) and \( L_0 \) using methods from both finite geometry and modular representation theory.

Keywords Block idempotent · Brauer’s theory · Character · Conic · General linear group · Incidence matrix · Low-density parity-checkcode · Module · 2-Rank

Mathematics Subject Classification 51E20 · 20C20

1 Introduction

Let \( \mathbb{F}_q \) be the finite field of order \( q \), where \( q = p^e \), \( p \) is a prime and \( e \geq 1 \) is an integer. Let \( \text{PG}(2, q) \) denote the classical projective plane of order \( q \) represented via homogeneous coordinates. Namely, a point \( P \) of \( \text{PG}(2, q) \) can be written as \( (a_0, a_1, a_2) \), where \( (a_0, a_1, a_2) \) is a nonzero vector of \( V \), and a line \( \ell \) as \( [b_0, b_1, b_2] \), where \( b_0, b_1, b_2 \) are not all zeros. The point \( P = (a_0, a_1, a_2) \) lies on the line \( \ell = [b_0, b_1, b_2] \) if and only if

\[
a_0b_0 + a_1b_1 + a_2b_2 = 0.
\]

A nondegenerate conic in \( \text{PG}(2, q) \) is the set of points satisfying a nondegenerate quadratic form. It is well known that the set of points

\[
\mathcal{O} = \{(1, t, t^2) \mid t \in \mathbb{F}_q \} \cup \{(0, 0, 1)\},
\]

(1.1)

Communicated by Q. Xiang.

J. Wu (✉)
Department of Mathematics, Lane College, Jackson, TN 38301, USA
e-mail: jwu@lanecollege.edu
which is also the set of projective solutions of the nondegenerate quadratic form

\[ Q(X_0, X_1, X_2) = X_1^2 - X_0X_2 \]  

(1.2)

ger over \( \mathbb{F}_q \), gives rise to a standard example of a nondegenerate conic in PG(2, \( q \)). It can be shown that every nondegenerate conic must have \( q + 1 \) points, no three of which are collinear, which we call an oval (see [7, p. 157]). In the case where \( q \) is odd, Segre [15] proved that an oval in PG(2, \( q \)) must be a nondegenerate conic. In this paper, \( q = p^\ell \) is always assumed to be an odd prime power. For convenience, we fix the conic in (1.1) as the “standard” conic. A line \( \ell \) is passant, tangent, or secant accordingly as \( |\ell \cap \mathcal{O}| = 0, 1, \) or 2, respectively. It is clear that every line of PG(2, \( q \)) must be in one of these classes. A point \( P \) is an internal, absolute, or external point depending on whether it lies on 0, 1, or 2 tangent lines to \( \mathcal{O} \).

The sets of secant, tangent, and passant lines are denoted by \( Se \), \( T \) and \( Pa \), respectively; the sets of external and internal points are denoted by \( E \) and \( I \), respectively. The sizes of these sets are \(|Se| = |E| = \frac{q(q+1)}{2} \), \(|Pa| = |I| = \frac{q(q-1)}{2} \), and \(|T| = q + 1 \) (see (2.2)). Moreover, it can be shown that the quadratic form \( Q \) in (1.1) induces a polarity \( \sigma \), a correlation of order 2, under which \( E \) and \( Se \), \( O \) and \( T \), and \( I \) and \( Pa \) are in one-to-one correspondence with each other, respectively.

Let \( C \) be a 0–1 matrix; that is, \( C \) is a matrix whose entries are either 0 or 1. Note that \( C \) can be viewed as a matrix over any ring with 1. The \( p \)-rank of \( C \), denoted by rank\(_p\)(\( C \)), is defined to be the dimension of the column space of \( C \) over a field \( F \) of characteristic \( p \). The column null space of \( C \) over \( F \) determines a linear code whose dimension is defined to be the dimension of the corresponding column null space of \( C \) over \( F \).

Let \( A \) be the \((q^2 + q + 1) \times (q^2 + q + 1)\) point-line incidence matrix of PG(2, \( q \)); namely, \( A \) is a 0–1 matrix and the rows and columns of \( A \) are labeled by the points and lines of PG(2, \( q \)), respectively, and the \((P, \ell)\)-entry of \( A \) is 1 if and only if \( P \in \ell \). It can be shown that the 2-rank of \( A \) is \( q^2 + q \) [8] and the \( p \)-rank of \( A \) is \( \left(\frac{p+1}{2}\right)^e \) [1], where \( q = p^\ell \). The binary linear code generated by the column \( \mathbb{F}_2 \)-null space of \( A \) has dimension 1. Therefore, it is not useful for any practical purpose.

In [4], Droms et al. partitioned \( A \) into the following 9 submatrices:

\[
\begin{pmatrix}
A_{11} & A_{12} & A_{13} \\
A_{21} & A_{22} & A_{23} \\
A_{31} & A_{32} & A_{33}
\end{pmatrix}
\]  

(1.3)

where the block of rows for \((A_{11}, A_{21}, A_{31})\) are labeled by the absolute, internal, and external points, respectively, and the block of columns for \((A_{11}, A_{12}, A_{13})\) are labeled by the tangent, passant, and secant lines, respectively. They used the column null spaces of the submatrices \( A_{i,j} \) for \( 2 \leq i, j \leq 3 \) over \( \mathbb{F}_2 \) to construct four low-density parity-check (LDPC) codes. Based on computational evidence, they made a conjecture on the dimensions of these codes. For convenience, we denote \( A_{33} \) and \( A_{32} \) by \( B_0 \) and \( B \), respectively. From (1.3), it follows that \( B_0 \) and \( B \) are the incidence matrices of internal points versus secant lines and external points versus passant lines, respectively. Note that \( B \) is a \( \frac{q(q+1)}{2} \times \frac{q(q-1)}{2} \) matrix and \( B_0 \) is a \( \frac{q(q-1)}{2} \times \frac{q(q+1)}{2} \) matrix. The purpose of this article is to confirm the following conjecture on the dimensions of the LDPC codes \( \mathcal{L} \) and \( \mathcal{L}_0 \) arising from the column \( \mathbb{F}_2 \)-null spaces of \( B \) and \( B_0 \), respectively.

**Conjecture 1.1** ([4]) Let \( \mathcal{L} \) and \( \mathcal{L}_0 \) be the \( \mathbb{F}_2 \)-null spaces of \( B \) and \( B_0 \), respectively. Then

\[
\dim_{\mathbb{F}_2}(\mathcal{L}) = \begin{cases} 
\frac{q^2-1}{4} - q, & \text{if } q \equiv 1 \pmod{4}, \\
\frac{q^2-1}{4} - q + 1, & \text{if } q \equiv 3 \pmod{4};
\end{cases}
\]
Let \( F \) be the algebraic closure of \( \mathbb{F}_2 \). Let \( F^I \) and \( F^E \) be the free \( F \)-modules whose standard bases consist of the characteristic column vectors of \( I \) and those of \( E \), respectively. The actions of \( H \) on \( I \) and \( E \) make the free \( F \)-modules \( F^I \) and \( F^E \) into \( FH \)-permutation modules. We define a map

\[
\phi_B : F^I \rightarrow F^E
\]

as follows: specify the images of the basis elements of \( F^I \) under \( \phi_B \) first, i.e.

\[
\phi_B(\mathcal{P}) = \sum_{Q \in B^+ \cap E} \chi_Q
\]

for each \( \mathcal{P} \in I \), and then extend \( \phi_B \) linearly to \( F^I \), where \( \perp \) is the polarity induced by the quadratic form \( Q, G_p \) and \( \chi_Q \) are the characteristic column vectors of the internal point \( P \) with respect to \( I \) and the external point \( Q \) with respect to \( E \), respectively. The matrix of \( \phi_B \) is a 0-1 matrix of size \( |E| \times |I| \). Up to permutations of the rows and columns, \( B \) regarded as a matrix over \( F \), is the matrix of \( \phi_B \) with respect to the standard bases of \( F^I \) and \( F^E \). Moreover, \( \phi_B(x) = Bx \) for \( x \in F^I \). It can be shown that \( \phi_B \) is an \( FH \)-homomorphism. Hence, the column space of \( B \) over \( F \) is equal to \( \text{Im}(\phi_B) \), which is also an \( FH \)-submodule of \( F^E \).

This point of view enables us to use results from modular representation of \( H \) to determine the dimension of \( \text{Im}(\phi_B) \) and thus the 2-rank of \( B \). We remark that in the calculation of the 2-rank of \( A_{33} \) the authors of [16] view \( A_{33} \) as the matrix of an \( FH \)-homomorphism \( \phi \) from \( F^E \) to \( F^E \) under which the characteristic vector of an external point \( P \) is mapped to the sum of the characteristic vectors of the external points on \( P^\perp \).

Our idea of calculating \( \dim_F(\text{Im}(\phi_B)) \) is to find a decomposition of \( \text{Im}(\phi_B) \) into a direct sum of its submodules whose dimensions can be computed easily. To this end, we apply Brauer’s theory and compute the decomposition of \( \text{Im}(\phi_B) \) into blocks. A similar idea was used in [16] to compute the decomposition of \( \text{Ker}(\phi) \) into blocks as well as \( \dim_F(\text{Ker}(\phi)) \).

Nevertheless, there are two major differences between the current article and [16]: (1) the geometric results used to compute the decomposition of \( \text{Im}(\phi_B) \) into blocks are essentially different from those used to compute the decomposition of \( \text{Ker}(\phi) \); (2) the summands of
Im(φ_B) in its block decomposition are more complicated than those of Ker(φ), requiring more effort to find dim_F(Im(φ_B)).

In the following we will give a brief overview of this article. In Sect. 2, we first review the basic facts about \( \mathcal{O} \) and then prove several crucial geometric results. From them, in Sect. 5, we show that the 2-rank of the incidence matrix \( \mathbf{D} \) of external points and \( N_{P_a,\ell}(\mathbf{P}) \) for \( \mathbf{P} \in I \) (the set of external points on the passant lines through \( \mathbf{P} \)) is either \( q \) or \( q - 1 \), depending on \( q \). The character of the complex permutation module \( \mathbb{C}^I \) and its decomposition into a sum of the irreducible ordinary characters of \( H \) were calculated in [18]; the decomposition of the characters of \( H \) into 2-blocks was given by Burkhardt [3] and Landrock [12]. From them we see that \( \mathbb{C}^I \) is a direct sum of \( \mathbb{C}H \)-modules consisting of one simple module from each block of defect zero, and some summands from blocks of positive defect. According to Brauer’s theory, Im(φ_B) is the direct sum

\[
\text{Im}(\phi_B) = \bigoplus_B \text{Im}(\phi_B)e_B
\]

(1.5)

where \( e_B \) is a primitive idempotent in the center of \( FH \). The block idempotents \( e_B \) are elements of \( FH \) and were computed in [16]. In order to compute \( \text{Im}(\phi_B)e_B \) for each 2-block \( B \), we need detailed information concerning the action of group elements in various conjugacy classes on various geometric objects and on the intersections of certain special subsets of \( H \) with various conjugacy classes of \( H \). These computations are made in Sects. 3 and 4. This information also tells us that (i) \( \text{Im}(\phi_B)e_{B_0} \) is equal to the column space of \( \mathbf{D} \) over \( F \), or this space plus an additional trivial module, depending on \( q \), where \( B_0 \) is the principal 2-block of \( H \), and (ii) block idempotents associated with nonprincipal 2-blocks of positive defect annihilate \( \text{Im}(\phi_B) \) (Lemma 6.2). Since the \( B \)-component of \( F^I \) is the mod 2 reduction of the \( B \)-component of \( \mathbb{C}^I \), using (i) and (ii), and the block decomposition of \( \mathbb{C}^I \), we show that \( \text{Im}(\phi_B) \) is equal to the direct sum of the column space of \( \mathbf{D} \) and the simple modules lying in the 2-blocks of defect 0, or this sum plus an additional trivial module, depending on \( q \). The dimension formula of \( \text{Im}(\phi_B) \) follows as a corollary.

2 Geometric results

Recall that a collineation of PG(2, \( q \)) is an automorphism of PG(2, \( q \)), which is a bijection from the set of all points and all lines of PG(2, \( q \)) to itself that maps a point to a point and a line to a line, and preserves incidence. It is well known that each element of GL(3, \( q \)), the group of all 3 \( \times \) 3 nonsingular matrices over \( \mathbb{F}_q \), induces a collineation of PG(2, \( q \)). The proof of the following lemma is straightforward.

**Lemma 2.1** Let \( \mathbf{P} = (a_0, a_1, a_2)(\text{respectively,} \ \ell = [b_0, b_1, b_2]) \) be a point (respectively, a line) of PG(2, \( q \)). Suppose that \( \theta \) is a collineation of PG(2, \( q \)) that is induced by \( \mathbf{D} \in GL(3, q) \). If we use \( \mathbf{P}^\theta \) and \( \ell^\theta \) to denote the images of \( \mathbf{P} \) and \( \ell \) under \( \theta \), respectively, then

\[
\mathbf{P}^\theta = (a_0, a_1, a_2)^\theta = (a_0, a_1, a_2)\mathbf{D}
\]

and

\[
\ell^\theta = [b_0, b_1, b_2]^\theta = [c_0, c_1, c_2],
\]

where \( c_0, c_1, c_2 \) correspond to the first, the second, and the third coordinate of the vector \( \mathbf{D}^{-1}(b_0, b_1, b_2)^\top \), respectively.
A correlation of $\text{PG}(2, q)$ is a bijection from the set of points to the set of lines as well as the set of lines to the set of points that reverses inclusion. A polarity of $\text{PG}(2, q)$ is a correlation of order 2. The image of a point $P$ under a correlation $\sigma$ is denoted by $P^\sigma$, and that of a line $\ell$ is denoted by $\ell^\sigma$. It can be shown [7, p. 181] that the nondegenerate quadratic form $Q(X_0, X_1, X_2) = X_1^2 - X_0X_2$ induces a polarity $\sigma$ (or $\perp$) of $\text{PG}(2, q)$, which can be represented by the matrix

$$
M = \begin{pmatrix}
0 & 0 & -\frac{1}{2} \\
0 & 1 & 0 \\
-\frac{1}{2} & 0 & 0
\end{pmatrix}.
$$

(2.1)

**Lemma 2.2** ([9, p. 47]) Let $P = (a_0, a_1, a_2)$ (respectively, $\ell = [b_0, b_1, b_2]$) be a point (respectively, a line) of $\text{PG}(2, q)$. If $\sigma$ is the polarity represented by the above nonsingular symmetric matrix $M$, then

$$
P^\sigma = (a_0, a_1, a_2)^\sigma = [c_0, c_1, c_2]
$$

and

$$
\ell^\sigma = [b_0, b_1, b_2]^\sigma = (b_0, b_1, b_2)M^{-1},
$$

where $c_0, c_1, c_2$ correspond to the first, the second, the third coordinate of the column vector $M(a_0, a_1, a_2)^\top$, respectively.

For example, if $P = (x, y, z)$ is a point of $\text{PG}(2, q)$, then its image under $\sigma$ is $P^\sigma = [z, -2y, x]$. For convenience, $\xi$ is a fixed primitive element of $\mathbb{F}_q$, we will denote the set of all nonzero squares of $\mathbb{F}_q$ by $\square_q$, and the set of nonsquares by $\square_q$. Also, $\mathbb{F}_q^*$ is the set of nonzero elements of $\mathbb{F}_q$.

**Lemma 2.3** ([7, pp. 181–182]) Assume that $q$ is odd.

(i) The polarity $\sigma$ above defines three bijections; that is, $\sigma : I \to Pa$, $\sigma : E \to Se$, and $\sigma : O \to T$ are all bijections.

(ii) A line $[b_0, b_1, b_2]$ of $\text{PG}(2, q)$ is a passant, a tangent, or a secant to $O$ if and only if $b_1^2 - 4b_0b_2 \in \square_q, b_1^2 - 4b_0b_2 = 0,$ or $b_1^2 - 4b_0b_2 \in \square_q$, respectively.

(iii) A point $(a_0, a_1, a_2)$ of $\text{PG}(2, q)$ is internal, absolute, or external if and only if $a_1^2 - a_0a_2 \in \square_q, a_1^2 - a_0a_2 = 0,$ or $a_1^2 - a_0a_2 \in \square_q$, respectively.

The results in the following lemma can be obtained by simple counting; see [7] for more details and related results.

**Lemma 2.4** ([7, p. 170]) Using the above notation, we have

$$
|T| = |O| = q + 1, \ |Pa| = |I| = \frac{q(q - 1)}{2}, \ \text{and} \ |Se| = |E| = \frac{q(q + 1)}{2}.
$$

(2.2)

Also, we have the following tables:

2.1 More geometric results

Let $G$ be the automorphism group of $O$ in $\text{PGL}(3, q)$ (i.e. the subgroup of $\text{PGL}(3, q)$ fixing $O$ setwise). Then $G$ is the image in $\text{PGL}(3, q)$ of $\text{O}(3, q) = \text{SO}(3, q) \times \langle -1 \rangle$, hence also
the image of SO(3, q), to which it is isomorphic. For our computations, we will describe $G$
 in a slightly different way. The map $\tau : \text{GL}(2, q) \rightarrow \text{GL}(3, q)$ sending the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to
\[
\begin{pmatrix}
  a^2 & ab & b^2 \\
  2ac & ad + bc & 2bd \\
  c^2 & cd & d^2
\end{pmatrix}
\]
(2.3)
is a group homomorphism. The image of $\tau(G)$ in PGL(3, q) lies in $G$. Now, whether
or not the group $\tau(\text{GL}(2, q))$ contains SO(3, q) depends on $q$. Nevertheless, $\tau(\text{GL}(2, q))$
always contains a subgroup of index 2 in O(3, q) whose image in PGL(3, q) is $G$. Thus,
the induced homomorphism $\overline{\tau} : \text{PGL}(2, q) \rightarrow \text{PGL}(3, q)$ maps PGL(2, q) isomorphically
onto $G$.

Let $H = \tau(\text{SL}(2, q))$, the group of matrices of the form (2.3) such that $ad - bc = 1$.
Since the kernel of $\tau$ is $\langle -I_2 \rangle$, it follows that $H \cong \text{PSL}(2, q)$ and that $H$
is isomorphic to its image $\overline{H}$ in PGL(3, q). In fact, we have $H = \Omega(3, q)$.

Since
\[
\text{PGL}(2, q) = \text{PSL}(2, q) \cup \begin{pmatrix} 1 & 0 \\ 0 & \xi^{-1} \end{pmatrix} \cdot \text{PSL}(2, q),
\]
our discussion shows that
\[
H \cup d(1, \xi^{-1}, \xi^{-2}) \cdot H
\]
(2.4)
is a full set of representative matrices for the elements of $G$. In our computations, it will often
be convenient to refer to elements of $G$ by means of their representatives in the set (2.4).

Additionally, a group element in (2.3) has the inverse equal to
\[
\begin{pmatrix}
  d^2 & -bd & b^2 \\
  -2cd & ad + bc & -2ab \\
  c^2 & -ac & a^2
\end{pmatrix}
\]
(2.5)
Moreover, the following holds.

**Lemma 2.5** [6] The group $G$ acts transitively on $I$ and $Pa$ as well as on $E$ and $Se$.

We will refer to this lemma frequently in the rest of this section.

**Lemma 2.6** [16, Lemma 2.9] Let $P$ be a point not on $O$, $\ell$ a nontangent line, and $P \in \ell$.
Using the above notation, we have the following.

(i) If $P \in I$ and $\ell \in Pa$, then $P^{\perp} \cap \ell \in E$ if $q \equiv 1$ (mod 4), and $P^{\perp} \cap \ell \in I$
if $q \equiv 3$ (mod 4).

(ii) If $P \in I$ and $\ell \in Se$, then $P^{\perp} \cap \ell \in I$ if $q \equiv 1$ (mod 4), and $P^{\perp} \cap \ell \in E$
if $q \equiv 3$ (mod 4).

(iii) If $P \in E$ and $\ell \in Pa$, then $P^{\perp} \cap \ell \in I$ if $q \equiv 1$ (mod 4), and $P^{\perp} \cap \ell \in E$
if $q \equiv 3$ (mod 4).

(iv) If $P \in E$ and $\ell \in Se$, then $P^{\perp} \cap \ell \in E$ if $q \equiv 1$ (mod 4), and $P^{\perp} \cap \ell \in I$
if $q \equiv 3$ (mod 4).

Next we define $\Box_q - 1 := \{s - 1 \mid s \in \Box_q\}$ and $\varnothing_q - 1 := \{s - 1 \mid s \in \varnothing_q\}$.

**Lemma 2.7** [17] Using the above notation,

(i) if $q \equiv 1$ (mod 4), then $|(\Box_q - 1) \cap \Box_q| = \frac{q - 5}{4}$ and $|(\Box_q - 1) \cap \varnothing_q| =
|(\varnothing_q - 1) \cap \Box_q| = |(\varnothing_q - 1) \cap \varnothing_q| = \frac{q - 1}{4}$.

\[\square\] Springer
Table 1 Number of points on lines of various types

| Name            | Absolute points | External points | Internal points |
|-----------------|-----------------|-----------------|-----------------|
| Tangent lines   | 1               | $q$             | 0               |
| Secant lines    | 2               | $\frac{q-1}{2}$ | $\frac{q-1}{2}$ |
| Passant lines   | 0               | $\frac{q+1}{2}$ | $\frac{q+1}{2}$ |

Table 2 Number of lines through points of various types

| Name            | Tangent lines | Secant lines | Passant lines |
|-----------------|---------------|--------------|---------------|
| Absolute points | 1             | $q$          | 0             |
| External points | 2             | $\frac{q-1}{2}$ | $\frac{q-1}{2}$ |
| Internal points | 0             | $\frac{q+1}{2}$ | $\frac{q+1}{2}$ |

(ii) if $q \equiv 3 \pmod{4}$, then $|((\varnothing_q q - 1) \cap \varnothing_q | = \frac{q+1}{4}$ and $|((\varnothing_q q - 1) \cap \varnothing_q | = |((\varnothing_q q - 1) \cap \varnothing_q | = \frac{q-3}{4}$.

Definition 2.8 Let $P$ be a point not on $O$ and $\ell$ a line. We define $E_\ell$ (respectively, $I_\ell$) to be the set of external (respectively, internal) points on $\ell$, $Pap$ (respectively, $Sep$) the set of passant (respectively, secant) lines through $P$, and $T_P$ the set of tangent lines through $P$. Also, $N_{Pa,E}(P)$ (respectively, $N_{Se,E}(P)$) is defined to be the set of external points on the passant (respectively, secant) lines through $P$.

In the following lemma, we list the sizes of the above defined sets as well as the action of $G$ on these sets. Also, we adopt standard notation from permutation group theory. For instance, if $W \subseteq I$, then $W^g := \{ w^g | w \in W \}$, $G_P$ is the stabilizer of $P$ in $G$, and for $M \subseteq G$, $M^g$ is the conjugate of $M$ under $g$.

Lemma 2.9 Using the above notation, if $P \in I$, we have

(i) $|E_P \perp | = |Sep| = \frac{q+1}{2}$,
(ii) $|I_P \perp | = |Pap| = \frac{q+1}{2}$,
(iii) $|N_{Pa,E}(P)| = \frac{(q+1)^2}{4}$ and $|N_{Se,E}(P)| = \frac{(q-1)(q+1)}{4}$; moreover, if $P$ is not a point on $O$, $\ell$ is a nontangent line, and $g \in G$, we have
(iv) $I_{\ell \perp}^g = I_{\ell \perp}$ and $Pap_P^g = Pap_P$,
(v) $E_{\ell \perp}^g = E_{\ell \perp}$ and $Sep_P^g = Sep_P$,
(vi) $H_P^g = H_P$,
(vii) $N_{Pa,E}^g(P) = N_{Pa,E}(P^g)$ and $N_{Se,E}^g(P) = N_{Se,E}(P^g)$,
(viii) $(P \perp)^g = (P^g) \perp$, where $\perp$ is the polarity of $PG(2, q)$ defined as above.

Proof The above (i) – (iii) follow from from Tables 1 and 2 and simple counting, and (iv) – (viii) follow from the fact that $G$ preserves incidence. \hfill $\square$

By the definition of $G$, it is clear that the following two lemmas are true.

Lemma 2.10 Let $P$ be a point of $PG(2, q)$. Then the polarity $\perp$ defines a bijection between $I_P \perp$ and $Pap$, and also a bijection between $E_P \perp$ and $Sep$. \hfill $\square$
Lemma 2.11 Let $W$ be a subgroup of $G$. Suppose that $g \in G$ and $P$ is a point of $\text{PG}(2, q)$. Then

$$(W^g)_{P^g} = W^g_P.$$  

Proposition 2.12 Let $P$ be a point not on $\mathcal{O}$ and set $K = G_P$. Then $K$ is transitive on each of $I_P^\perp$, $E_P^\perp$, $P_P$, and $\text{Sep}$. Moreover, if $P \in E$, then $K$ is also transitive on $T_P$.

Proof The case where $P \in I$ is Proposition 2.11 in [18]; the case where $P \in E$ or $\mathcal{O}$ is Lemma 2.11(iii) in [16].

Lemma 2.13 [16, Corollary 2.16] Let $P$ be a point of $\text{PG}(2, q)$ and let $\perp$ be the polarity of $\text{PG}(2, q)$ defined above. Then for $g \in G_P$ we have $P^\perp = (P^\perp)^g$. Consequently, $P^\perp$ is fixed setwise by $G_P$. Moreover, $G_{P^\perp} = G_P$.

Lemma 2.14 Assume that $P \in I$ and $\ell = P^\perp$. Let $Q \in E_\ell$ and $\ell^* \in T_Q$. Suppose that $P_1$ and $P_2$ are two distinct external points on $\ell^*$ and let $\ell_1$ and $\ell_2$ be the tangent lines different from $\ell^*$ through $P_1$ and $P_2$, respectively. Then $\ell_1$ and $\ell_2$ meet in an external point on a secant line through $P$ if and only if one of the following two cases occurs:

(i) $P_1$ and $P_2$ are on two passant lines through $P$;

(ii) $P_1$ and $P_2$ are on two secant lines through $P$.

Proof Since $G$ is transitive on $I$ and preserves incidence, without loss of generality, we may assume that $P = (1, 0, −ξ)$, and thus $\ell = [1, 0, −ξ^{-1}]$. Since $K := G_P$ is transitive on $E_\ell$ by Proposition 2.12, we can assume that $Q = (0, 1, 0)$. Let $\ell^* = [1, 0, 0]$ be a tangent line through $Q$. It is clear that

$$E_{\ell^*} = \{(0, 1, m) \mid m \in \mathbb{F}_q\}.$$  

Let $P_1 = (0, 1, m_1)$ and $P_2 = (0, 1, m_2)$ be two distinct external points on $\ell^*$. Then the tangent lines through $P_1$ and $P_2$ different from $\ell^*$ are $\ell_1 = [m_1^2, −4m_1, 4]$ and $\ell_2 = [m_2^2, −4m_2, 4]$, respectively. So we have that $P_3 := \ell_1 \cap \ell_2 = (1, \frac{m_1 + m_2}{4}, \frac{m_1m_2}{4}) \in E$. Thus the line through $P$ and $P_3$ is

$$\ell_{P, P_3} = \left[ m_1 + m_2, −4\left(\frac{m_1m_2}{4ξ} + 1\right), \frac{m_1 + m_2}{ξ} \right],$$

which is a secant line if and only if

$$16\left(\frac{m_1m_2}{4ξ} + 1\right)^2 − \frac{4(m_1 + m_2)^2}{ξ} = \frac{(m_1^2 − 4ξ)(m_2^2 − 4ξ)}{ξ^2} \in \mathbb{F}_q$$

if and only if either $m_i^2 − 4ξ \not\in \mathbb{F}_q$ for $i = 1, 2$ or $m_i^2 − 4ξ \not\in \mathbb{F}_q$ for $i = 1, 2$. Since the line through $P$ and $P_i$ ($i = 1$ or 2) is $\ell_{P, P_i} = [1, −\frac{m_i}{ξ}, \frac{1}{ξ}]$, and its discriminant is $\frac{m_i^2 − 4ξ}{ξ^2}$, we conclude that $\ell_{P, P_3}$ is a secant line if and only if either (i) $P_1$ and $P_2$ are on two passant lines through $P$ or (ii) $P_1$ and $P_2$ are on two secant lines through $P$.

Definition 2.15 Let $N \subseteq E$. We define $\chi_N$ to be the characteristic (column) vector of $N$ with respect to $E$; that is, $\chi_N$ is a column vector of length $|E|$ whose entries are indexed by the external points such that if $P \in N$ then the entry of $\chi_N$ indexed by $P$ is 1, 0 otherwise. For a line $\ell$, if no confusion occurs, we use $\chi_\ell$ to replace $\chi_{E\ell}$. Also, if $N = \{P\}$ is a singleton set, we will frequently use $\chi_P$ to replace $\chi_{[P]}$.  

Springer
Remark 2.16 In the rest of this section, \( \chi_N \) for \( N \subseteq E \) will be always viewed as a column vector over \( \mathbb{Z} \), the ring of integers.

Corollary 2.17 Let \( P \in I \). Using the above notation, we have
\[
\chi_{NP_a,E}(P) \equiv \sum_{\ell' \in T(P, \ell(P))} \chi_{\ell'} \pmod{2},
\]
where \( \ell(P) \) is a tangent line through an external point on \( P^\perp \), \( T(P, \ell(P)) \) is the set of tangent lines distinct from \( \ell(P) \) through the external points that are on both \( \ell(P) \) and the passant lines through \( P \), and the congruence means entrywise congruence.

Proof It is clear that \( |T(P, \ell(P))| = \frac{q+1}{2} \) since there are \( \frac{q+1}{2} \) passant lines through \( P \) and each of them meets \( \ell(P) \) in an external point. Let \( \ell' \in T(P, \ell(P)) \). Then by Lemma 2.14, any tangent line other than \( \ell' \) in \( T(P, \ell(P)) \) meets \( \ell' \) in an external point on a secant line through \( P \), and if we use \( IE(\ell', \ell(P)) \) to denote their intersections with \( \ell' \) then the points in \( E_{\ell'} \setminus IE(\ell', \ell(P)) \) must be on the passant lines through \( P \). Since
\[
(E_{\ell_1} \setminus IE(\ell_1, \ell(P))) \cap (E_{\ell_2} \setminus IE(\ell_2, \ell(P))) = \emptyset
\]
for two distinct lines \( \ell_1, \ell_2 \in T(P, \ell(P)) \) and
\[
|E_{\ell'} \setminus IE(\ell', \ell(P))| = q - \frac{q-1}{2} = \frac{q+1}{2},
\]
it follows that
\[
\sum_{\ell' \in T(P, \ell(P))} |E_{\ell'} \setminus IE(\ell', \ell(P))| = \sum_{\ell' \in T(P, \ell(P))} \frac{q+1}{2} = \frac{(q+1)^2}{4}
\]
which is the same as the size of \( NP_a,E(P) \) by Lemma 2.9(iii). Consequently, we must have
\[
\bigcup_{\ell' \in T(P, \ell(P))} E_{\ell'} \setminus IE(\ell', \ell(P)) = \bigcup_{\ell' \in P_{\text{ap}}} E_{\ell'} = NP_a,E(P).
\]
Moreover, since each point in \( IE(\ell', \ell(P)) \) lies on exactly two lines in \( T(P, \ell(P)) \) and each point in \( E_{\ell'} \setminus IE(\ell', \ell(P)) \) lies on no other line than \( \ell' \) in \( T(P, \ell(P)) \), the result follows. \( \square \)

Lemma 2.18 Assume that \( q \equiv 1 \pmod{4} \). Let \( P \in \mathcal{O} \). Then there exits a set \( \mathcal{M}(P) \) consisting of an odd number of internal points such that, for each external point \( Q \in P^\perp \), the number of passant lines through \( Q \) and the points in \( \mathcal{M}(P) \), counted with multiplicity, is odd.

Remark 2.19 In this lemma, it is possible that \( Q, Q_1, ..., Q_k \) are on the same passant line \( \ell \), where \( Q \in E_{P^\perp} \) and \( Q_i \in \mathcal{M}(P) \) for \( 1 \leq i \leq k \). If this circumstance occurs, then the line \( \ell \) should be counted \( k \) times.

Proof Without loss of generality, we may assume that \( P = (0, 0, 1) \), and so \( \ell := P^\perp = [1, 0, 0] \). Using Lemma 2.1 and (2.5), we have
\[
K := H_{\ell} = \left\{ \begin{pmatrix} d^2 - bd & b^2 \\ 0 & 1 & -\frac{2b}{d} \\ 0 & 0 & \frac{d}{d^2} \end{pmatrix} \middle| d \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}.
\]
Since
\[
\begin{pmatrix}
1 -b & b^2 \\
0 & 1 & -2b \\
0 & 0 & 1
\end{pmatrix}^k = \begin{pmatrix}
1 -kb & (kb)^2 \\
0 & 1 & -2kb \\
0 & 0 & 1
\end{pmatrix}
\]
for any positive integer \(k\), it is obvious that
\[
\left\{ \begin{pmatrix}
1 -b & b^2 \\
0 & 1 & -2b \\
0 & 0 & 1
\end{pmatrix} \mid b \in \mathbb{F}_q \right\}
\]
is a collineation subgroup of order \(q\) in \(K\), which we denote by \(T\).

For \((0, 1, u_1), (0, 1, u_2)\) where \(u_1, u_2 \in \mathbb{F}_q\) and \(u_1 \neq u_2\), we have
\[
(0, 1, u_1) \begin{pmatrix}
1 -u_1-u_2 \\
0 & 1 & -(u_1-u_2) \\
0 & 0 & 1
\end{pmatrix} = (0, 1, u_2);
\]
this implies that \(T\) is transitive on \(E_\ell = \{(0, 1, u) \mid u \in \mathbb{F}_q\}\).

Now let \(P_1 = (1, 0, -\xi) \in I\), set \(\mathcal{M}(P) := \{P_1^g \mid g \in T\}\) which is the \(T\)-orbit of \(P_1\), and let \(Q = (0, 1, u) \in \ell\). Then
\[
\mathcal{M}(P) = \{(1, -b, b^2 - \xi) \mid b \in \mathbb{F}_q\}
\]
and the lines through both \(Q\) and the points in \(\mathcal{M}(P)\) form the multiset
\[
L(Q) = \{[b^2 + ub - \xi, u, -1] \mid b \in \mathbb{F}_q\}.
\]
Note that a line \([b^2 + ub - \xi, u, -1] \in L(Q)\) is passant if and only if \(\frac{(u+2b)^2}{4b} - 1 \in \mathbb{F}_q\).

Since the number of \(t \in \mathbb{F}_q\) satisfying \(t - 1 \in \mathbb{F}_q\) is \(|\{t \in \mathbb{F}_q \mid t - 1 \in \mathbb{F}_q\}| = \frac{q-1}{4}\) by Lemma 2.18(i), it follows that the number of \(b \in \mathbb{F}_q \setminus \{-\frac{3}{2}\}\) satisfying \(\frac{(u+2b)^2}{4b} - 1 \in \mathbb{F}_q\) is \(2(\frac{q-1}{4}) = \frac{q-1}{2}\). Moreover, when \(b = -\frac{u}{2}\), \(\frac{(u+2b)^2}{4b} - 1 = -1 \in \mathbb{F}_q\) as \(q \equiv 1 \pmod{4}\).

Hence, the number of \(b \in \mathbb{F}_q\) satisfying \(\frac{(u+2b)^2}{4b} - 1 \in \mathbb{F}_q\) is \(\frac{q-1}{2} + 1 = \frac{q+1}{2}\). Thus, counted with multiplicity, there are \(\frac{q+1}{2}\) passant lines in \(L(Q)\). Therefore, there are an odd number of internal points (precisely \(\frac{q+1}{2}\)) in \(\mathcal{M}(P)\) connecting \(Q\) by a passant line as \(q \equiv 1 \pmod{4}\).

Since \(T\) is transitive on both \(\mathcal{M}(P)\) and \(E_\ell\) and preserves incidence, we conclude that the number of passant lines through an external point on \(P_1\) and the points in \(\mathcal{M}(P)\), counted with multiplicity, must be odd.

**Remark 2.20** Let \(P \in O\). In the rest of this article, without being further mentioned, \(\mathcal{M}(P)\) always denotes a set of internal points associated with \(P\) satisfying the conditions in Lemma 2.18.

**Corollary 2.21** Assume that \(q \equiv 1 \pmod{4}\). Let \(\ell\) be a tangent line. Then
\[
\chi_\ell = \sum_{P \in \mathcal{M}(P)} \sum_{P \cap \ell} \chi_\ell
\]
\[
= \sum_{P \in \mathcal{M}(P)} \chi_{N_{P_0,E}(P)} \pmod{2}
\]
where the congruence is entrywise congruence.

\(\square\) Springer
Proof Let \( P \in \mathcal{M}(\ell^\perp) \). Then from Corollary 2.17, it follows that

\[
\chi_{N_{\text{Pa}, \mathcal{E}}}(P) = \sum_{\ell' \in \text{Pa}P} \chi_{\ell'}
\]

\[
\equiv \sum_{\ell' \in T(\ell, \ell(P))} \chi_{\ell'} \quad (\text{mod } 2),
\]

(2.9)

where \( \ell(P) \) is a tangent line through an external point on \( P^\perp \) and \( T(\ell, \ell(P)) \) is the set of tangent lines different from \( \ell(P) \) through the external points that are both \( \ell(P) \) and the passant lines through \( P \).

Further, if we take \( \ell(P) = \ell \) for each \( P \in \mathcal{M}(\ell^\perp) \) and set \( W(P) := \{ \ell \cap \ell_1 | \ell_1 \in P_{\text{Pa}} \} \), then

\[
\sum_{P \in \mathcal{M}(\ell^\perp)} \sum_{\ell' \in \text{Pa}P} \chi_{\ell'} \equiv \sum_{\ell \in \mathcal{M}(\ell^\perp)} \sum_{\ell' \in T(\ell, \ell(P))} \sum_{Q \in W(P)} \chi_{\ell'}
\]

\[
= \sum_{Q \in E_\ell} \sum_{\ell' \in T_Q \setminus \{ \ell \}} \sum_{Q \in W(P)} \chi_{\ell'}
\]

\[
= \sum_{\ell' \in T \setminus \{ \ell \}} \sum_{Q \in W(P)} \chi_{\ell'}
\]

\[
\equiv \sum_{\ell' \in T \setminus \{ \ell \}} \chi_{\ell'} \quad (\text{mod } 2),
\]

(2.10)

where \( a_{\ell'} \) for \( \ell' \in T \setminus \{ \ell \} \) are odd. In (2.10), the second equality follows from the definition of \( T(\ell, \ell(P)) \) and the third equality holds since the multiset

\[
\bigcup_{Q \in E_\ell} \bigcup_{L(Q)} T_Q \setminus \{ \ell \},
\]

(2.11)

where \( L(Q) := \{ \ell_{P_1, Q} \in \text{Pa} | P_1 \in \mathcal{M}(\ell^\perp) \} \), is the same as the multiset

\[
\bigcup_{P \in \mathcal{M}(\ell^\perp)} \bigcup_{Q \in \mathcal{W}(P)} T_Q \setminus \{ \ell \},
\]

and the tangent line \( \ell' \) other than \( \ell \) through an external point \( Q \) on \( \ell \) occurs an odd number of times in (2.11) by Lemma 2.18.

Since \( \sum_{\ell' \in T} \chi_{\ell'} \equiv 0 \mod 2 \), it follows that

\[
\sum_{P \in \mathcal{M}(\ell^\perp)} \sum_{\ell' \in \text{Pa}P} \chi_{\ell'} \equiv \sum_{P \in \mathcal{M}(\ell^\perp)} \chi_{N_{\text{Pa}, \mathcal{E}}}(P)
\]

\[
\equiv \sum_{\ell' \in T \setminus \{ \ell \}} \chi_{\ell'}
\]
\[ \equiv \chi_\ell + \sum_{\ell' \in T} \chi_{\ell'} \]
\[ \equiv \chi_\ell \pmod{2}. \]

Lemma 2.22 Let \( P \in E \) and let \( T_1 \) and \( T_2 \) be the two tangent lines through \( P \). Assume that 
\[ Z \subseteq (E_{T_1} \cup E_{T_2}) \setminus \{ P \}. \]
Then there is a set \( M(P) \) consisting of an even number of internal points such that, for any point \( Q \in Z \), the number of passant lines through \( Q \) and the points \( M(P) \), counted with multiplicity, is odd, and the number of passant lines through \( P \) and the points in \( M(P) \), counted with multiplicity, is even.

Proof Since \( G \) is transitive on \( E \), without loss of generality, we may assume that \( P = (0, 1, 0) \), and thus \( T_1 = [1, 0, 0] \) and \( T_2 = [0, 0, 1] \) are two tangent lines through \( P \). Let 
\[ K := G_P \] 
be the stabilizer of \( P \) in \( G \). Using (2.4), we have
\[ K = \left\{ d \begin{pmatrix} d^2, 1, \frac{1}{d^2} \end{pmatrix} \left| d^2 \in \square_q \right\} \cup \left\{ ad \begin{pmatrix} \frac{1}{d^2}, -1, c^2 \end{pmatrix} \left| c^2 \in \square_q \right\} \right. \]
\[ \cup \left\{ d \begin{pmatrix} d^2, 1, \frac{1}{d^2} \end{pmatrix} \left| d^2 \in \square_q \right\} \cup \left\{ ad \begin{pmatrix} \frac{1}{d^2}, -1, c^2 \end{pmatrix} \left| c^2 \in \square_q \right\} \right. \]
(2.12)

Let \( P_1 = (1, 1, x) \), where \( x \in \square_q \) (respectively, \( x \in \square_q \)) and \( 1 - x \in \square_q \), be an internal point for \( q \equiv 3 \pmod{4} \) (respectively, \( q \equiv 1 \pmod{4} \)). (Note that such an \( x \) in the last coordinate of \( P_1 \) exists in \( F_q \).) Then the \( K \)-orbit of \( P_1 \) is
\[ O_{P_1} = \left\{ \begin{pmatrix} 1, \frac{1}{d^2}, \frac{x}{d^4} \end{pmatrix} \left| d^2 \in \square_q \right\} \cup \left\{ \begin{pmatrix} 1, \frac{1}{d^2}, \frac{x}{d^2} \end{pmatrix} \left| d^2 \in \square_q \right\} \right. \]
To prove the first part of the lemma, we need only show that it holds for
\[ Z = (E_{T_1} \cup E_{T_2}) \setminus \{ P \}. \]
Let \( Q = (0, 1, 1) \in Z \). Using (2.12), we have that \( K \) only contains the identity collineation.
So \( K \) is transitive on \( Z \) as \( |Z| = |K| = 2(q - 1) \). The lines through \( Q \) and the points in \( O_{P_1} \) form the multiset
\[ L(Q) = \{ [x - d^2, d^4, -d^4] \mid d^2 \in \square_q \} \cup \{ [x - d^2, d^4, -d^4] \mid d^2 \in \square_q \}. \]
A line in \( L(Q) \) is passant if and only if
\[ \frac{(d^2 - 2)^2}{4(1 - x)} - 1 \in \square_q \]
or
\[ \frac{(d^2\xi - 2)^2}{4(1 - x)} - 1 \in \square_q, \]
where \( d^2 \in \square_q \). The number of \( d^2 \) satisfying either of the above two equations is equal to that of \( t \in F_q^* \) satisfying \( \frac{(t-2)^2}{4(1-t)} - 1 \in \square_q \) since \( F_q^* = \square_q \cup \square_q \xi \), where \( \square_q \xi = \{ d^2 \xi \mid d^2 \in \square_q \} \). For the case where \( q \equiv 3 \pmod{4} \), since the number of \( t \in F_q \) satisfying \( \frac{(t-2)^2}{4(1-t)} - 1 \in \square_q \) is equal to \( 2(|\square_q - 1| \cap \square_q| = 2(\frac{q+1}{4}) = q+1 \) by Lemma 2.9(ii) and \( t = 0 \) is one of them, we see that the number of passant lines in \( L(Q) \), counted with multiplicity, is \( \frac{q-1}{2} \) which is odd since \( q \equiv 3 \pmod{4} \). For the case where \( q \equiv 1 \pmod{4} \), since the number of \( t \in F_q \setminus \{ 2 \} \) satisfying \( \frac{(t-2)^2}{4(1-t)} - 1 \in \square_q \) is equal to \( 2(|\square_q - 1| \cap \square_q| = 2(\frac{q-1}{4}) = \frac{q-1}{2} \) Springer
by Lemma 2.9(i), \( t = 0 \) is not one of the solutions and \( t = 2 \) also satisfies \( \frac{(t-2)^2}{4(1-x)} - 1 \in \square q \), we see that the number of passant lines in \( L(Q) \), counted with multiplicity, is even, which is odd as \( q \equiv 1 \pmod{4} \). Now we set \( \mathcal{M}'(P) := \mathcal{O}_{P_1} \), and so \( |\mathcal{M}'(P)| = q - 1 \) is even. Since \( K \) is transitive on both \( Z = (E_{T_1} \cup E_{T_2}) \setminus \{P\} \) and the points in \( \mathcal{M}'(P) \), the number of passant lines through a point in \( Z \) and the points in \( \mathcal{M}'(P) \), counted with multiplicity, must be odd.

The lines through \( P \) and the points in \( \mathcal{M}'(P) \) form the multiset

\[
\left\{ \left[ 1, 0, -\frac{d^4}{x} \right] \Bigg| d^2 \in \square q \right\} \cup \left\{ \left[ 1, 0, -\frac{d^4q^2}{x} \right] \Bigg| d^2 \in \square q \right\},
\]

each or none of which is a passant line accordingly as \( q \equiv 3 \pmod{4} \) or \( q \equiv 1 \pmod{4} \). Hence, we conclude that the number of passant lines through \( P \) and the points in \( \mathcal{M}(P) \), counted with multiplicity, is even.

\[ \square \]

Remark 2.23 Let \( P \in E \). In the following discussion, without being further mentioned, \( \mathcal{M}'(P) \) will always denote a set consisting of an even number of internal points that satisfy the conditions with \( Z = E_{T_1} \setminus \{P\} \) in the above lemma, where \( T_1 \) is one of the two tangent lines through \( P \).

Corollary 2.24 Let \( P \in E \) and let \( T_1 \) and \( T_2 \) be the two tangent lines through \( P \). Then

\[
\chi_{T_1} + \chi_{T_2} \equiv \sum_{Q \in \mathcal{M}'(P)} \sum_{\ell \in \mathrm{Seq}_Q} \chi_{\ell} \equiv \sum_{Q \in \mathcal{M}'(P)} \chi_{N_{Se,E}(Q)} \pmod{2},
\]

where the congruence means entrywise congruence.

Proof Let \( Q \in \mathcal{M}'(P) \). Then Corollary 2.17 gives

\[
\chi_{NP_{a,E}(Q)} \equiv \sum_{\ell' \in P_{aQ}} \chi_{\ell'} \equiv \sum_{\ell' \in T(Q, \ell(Q))} \chi_{\ell'} \pmod{2},
\]

where \( \ell(Q) \) is a tangent line through an external point on \( Q^\perp \) and \( T(Q, \ell(Q)) \) is the set tangent lines through the external points that are on both \( \ell(Q) \) and the passant lines through \( Q \). Let \( \mathbf{1} \) be the all-one column vector of length \( |E| \). Since

\[
\mathbf{1} + \chi_{NP_{a,E}(Q)} \equiv \chi_{N_{Se,E}(Q)} \pmod{2}
\]

and \( |\mathcal{M}'(P)| \) is even, we have

\[
\sum_{Q \in \mathcal{M}'(P)} \sum_{\ell \in \mathrm{Seq}_Q} \chi_{\ell} \equiv \sum_{Q \in \mathcal{M}'(P)} (1 + \chi_{NP_{a,E}(Q)}) \equiv \sum_{Q \in \mathcal{M}'(P)} 1 + \sum_{Q \in \mathcal{M}'(P)} \chi_{NP_{a,E}(Q)} \equiv \sum_{Q \in \mathcal{M}'(P)} \chi_{NP_{a,E}(Q)} \equiv \sum_{Q \in \mathcal{M}'(P)} \sum_{\ell \in T(Q, \ell(Q))} \chi_{\ell} \pmod{2}.
\]

\[ \square \]
Further, if we set \( \ell(Q) := T_1 \) for each \( Q \in \mathcal{M}'(P) \) and set \( W'(Q) := \{ T_1 \cap \ell_1 \mid \ell_1 \in PaQ \} \), since the multiset
\[
\bigcup_{P_1 \in E'_{T_1}} \bigcup_{L'(P_1)} TP_1 \setminus \{T_1\},
\]
where \( L'(P_1) = \{ \ell_{P_1, P_2} \in Pa \mid P_2 \in \mathcal{M}(P) \} \), is the same as the multiset
\[
\bigcup_{Q \in \mathcal{M}'(P)} TP_1 \setminus \{T_1\},
\]
and the tangent line \( \ell \) other than \( T_1 \) through an external point \( P_1 \neq P \) (respectively, \( P_1 = P \)) on \( T_1 \) occurs an odd (respectively, even) number of times in (2.16) by Lemma 2.22, we obtain
\[
\sum_{Q \in \mathcal{M}'(P)} \sum_{\ell \in T(Q; \ell(Q))} \chi_{\ell} = \sum_{P_1 \in E'_{T_1}} \sum_{\ell \in T_{P_1} \setminus \{T_1\}} b_{\ell} \chi_{\ell} = b_{T_1} \chi_{T_2} + \sum_{\ell \in T \setminus \{T_1, T_2\}} b_{\ell} \chi_{\ell} = \sum_{\ell \in T \setminus \{T_1, T_2\}} \chi_{\ell} \pmod{2},
\]
where \( b_{\ell} \) for \( \ell \in T \setminus \{T_1, T_2\} \) are all odd integers and \( b_{T_2} \) is an even integer.

Using (2.15), (2.17), and the fact that \( \sum_{\ell \in T} \chi_{\ell} = 0 \pmod{2} \), we have
\[
\chi_{T_1} + \chi_{T_2} = \sum_{\ell \in T \setminus \{T_1, T_2\}} \chi_{\ell} = \sum_{Q \in \mathcal{M}'(P)} \sum_{\ell \in PaQ} \chi_{\ell} = \sum_{Q \in \mathcal{M}'(P)} \chi_{NPaE(Q)} \pmod{2}.
\]

3 The conjugacy classes and intersection parity

In this section, we review the conjugacy classes of \( H \) and study their intersections with some special subsets of \( H \).

3.1 Conjugacy classes

Recall that
\[
H = \left\{ \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix} \right\} \mid a, b, c, d \in \mathbb{F}_q, \ ad - bc = 1 \right\}
\]
is the subgroup of \( G \) that is isomorphic to \( \text{PSL}(2, q) \). If we define \( T := \text{tr}(g) + 1 \), where \( g \in H \) and \( \text{tr}(g) \) is the trace of \( g \), then the conjugacy classes of \( H \) can be read as follows.
Lemma 3.1 [16, Lemma 3.2] The conjugacy classes of $H$ are given as follows.

(i) $D = \{d(1, 1, 1)\}$;
(ii) $F^+ \cup F^−$, where $F^+ \cup F^− = \{g \in H \mid T(g) = 4, \ g \neq d(1, 1, 1)\}$;
(iii) $[\theta_i] = \{g \in H \mid T(g) = \theta_i, 1 \leq i \leq \frac{q - 5}{4} \text{ if } q \equiv 1 \pmod{4}, \text{ or } 1 \leq i \leq \frac{q - 3}{4} \text{ if } q \equiv 3 \pmod{4}, \text{ where } \theta_i \in \mathbb{Q}, \theta_i \neq 4, \text{ and } \theta_i - 4 \in \mathbb{Q}\}$;
(iv) $[0] = \{g \in H \mid T(g) = 0\}$;
(v) $[\pi_k] = \{g \in H \mid T(g) = \pi_k, 1 \leq k \leq \frac{q - 1}{4} \text{ if } q \equiv 1 \pmod{4}, \text{ or } 1 \leq k \leq \frac{q - 3}{4} \text{ if } q \equiv 3 \pmod{4}, \text{ where } \pi_i \in \mathbb{Q}, \pi_k \neq 4, \text{ and } \pi_k - 4 \in \mathbb{Q}\}$.

Remark 3.2 The set $F^+ \cup F^−$ forms one conjugacy class of $G$, and splits into two equal-sized classes $F^+$ and $F^−$ of $H$. For our purpose, we denote $F^+ \cup F^−$ by $[4]$. Also, each of $D, [\theta_i], [0]$, and $[\pi_k]$ forms a single conjugacy class of $G$. The class $[0]$ consists of all the elements of order 2 in $H$.

In the following, for convenience, we frequently use $C$ to denote any one of $D, [0], [4], [\theta_i]$, or $[\pi_k]$. That is,

$$C = D, [0], [4], [\theta_i], \text{ or } [\pi_k]. \quad (3.1)$$

3.2 Intersection properties

Definition 3.3 Let $P \in I, Q \in E, \ell \in Pa$. We define

$$\mathcal{H}_{P,Q} = \{h \in H \mid (P^\perp)^h \in PaQ\} \text{ and } S_{P,\ell} = \{h \in H \mid (P^\perp)^h = \ell\}.$$ 

That is, $\mathcal{H}_{P,Q}$ consists of all the elements of $H$ that map the passant line $P^\perp$ to a passant line through $Q$ and $S_{P,\ell}$ is the set of elements in $H$ that map $P^\perp$ to the passant line $\ell$.

Using the above notation, since $G$ preserves incidence, for $g \in G, P \in I$, and $\ell \in Pa$, we have

$$\mathcal{H}_{P,Q}^g = \mathcal{H}_{P^g,Q^g}, \ S_{P,\ell}^g = S_{P^g,\ell^g}. \quad (3.2)$$

The following corollary is apparent.

Corollary 3.4 Let $g \in G$ and $C$ be given in (3.1) and let $P$ and $Q$ be two external points. Then $(C \cap \mathcal{H}_{P,Q})^g = C \cap \mathcal{H}_{P^g,Q^g}.$

Next the size of the intersection of each conjugacy class of $H$ with $K$ which stabilizes an element of $I$ in $H$ is calculated.

Corollary 3.5 Let $P \in I$ and $K = H_P$. Then we have

(i) $|K \cap D| = 1$;
(ii) $|K \cap [4]| = 0$;
(iii) $|K \cap [\pi_k]| = 2$ for each $k$;
(iv) $|K \cap [\theta_i]| = 0$ for each $i$;
(v) $|K \cap [0]| = \frac{q + 1}{2}$ or $\frac{q - 1}{2}$ accordingly as $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$.

Proof Let $Q = (1, 0, -\xi)$ and $K_1 = H_Q$. Since $H$ is transitive on $I$, it follows $Q^g = P$ for some $g \in H$. By Lemma 2.11, we have $K_1^g = K$. Consequently,

$$|K \cap C| = |(K_1 \cap C)^g|.$$
Therefore, to prove the corollary, it is enough to consider $P = Q$. It is clear that $|D \cap K| = 1$. Let $g \in K \cap C$. Then the quadruples $(a, b, c, d)$ determining $g$ satisfy the following equations

\[
\begin{align*}
ab - cd\xi &= 0 \\
b^2 - d^2\xi &= -\xi(a^2 - c^2) \\
ad - bc &= 1 \\
a + d &= s,
\end{align*}
\]

(3.3)

where $s^2 = 0, 4, \pi_k, \theta_i$. The equations in (3.3) give (1) $a = d = \frac{s}{2}$, $c^2 = \frac{s^2 - 4}{4\xi}$, $b = \xi c$ and (2) $a = -d$, $s = 0$, $c^2\xi - 1 = a^2$, $b = -\xi c$. From Case (1), we see that $|K \cap [\pi_k]| = 2$ for each $[\pi_k]$ and $|K \cap C| = 0$ for $C = [\theta_i]$, [4]; moreover, if $q \equiv 3 \pmod{4}$, we obtain one group element $\text{ad}(-\xi, -1, \xi, -\xi) \in K \cap [0]$ in Case (1). Since the number of $t \in \mathbb{F}_q$ satisfying $t - 1 \in \mathbb{F}_q$ is $\frac{q-1}{2}$ or $\frac{q-3}{2}$ accordingly as $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$ by Lemma 2.9, the number of $c \in \mathbb{F}_q$ satisfying $c^2\xi - 1 \in \mathbb{F}_q$ is $2(\mathbb{F}_q - 1 \cap \mathbb{F}_q)$ which is $\frac{q-1}{2}$ or $\frac{q-3}{2}$ accordingly as $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$. When $q \equiv 1 \pmod{4}$, $c = 0$ also satisfies $c^2\xi - 1 \in \mathbb{F}_q$. Therefore, Case (1) and Case (2) give $\frac{q+1}{2}$ or $\frac{q-1}{2}$ different group elements in $K \cap [0]$ depending on $q$. Now the corollary is proved.

In the following lemma, we investigate the parity of $|H_{P, Q} \cap C|$ for each $C \neq [0]$ and $P \in I, Q \in E$. Recall that $\ell_{P, Q}$ is the line through $P$ and $Q$.

**Lemma 3.6** Assume that $q \equiv 1 \pmod{4}$. Let $P \in I$ and $Q \in E$. Suppose that $C = D$. [4], $[\pi_k](1 \leq k \leq \frac{q-1}{2})$, $[\theta_i](1 \leq i \leq \frac{q-5}{4})$.

(i) If $\ell_{P, Q} \in \text{Sep}$, then $|H_{P, Q} \cap C|$ is even for each $C$.

(ii) If $\ell_{P, Q} \in \mathbb{P}_P$ and $Q \not\in \mathbb{P}_P$, then $|H_{P, Q} \cap C|$ is odd if and only if if $C = D$.

(iii) If $\ell_{P, Q} \in \mathbb{P}_P$ and $Q \in \mathbb{P}_P$, for each class $[\pi_k]$ with $1 \leq k \leq \frac{q-1}{2}$, there are two different points $Q_1, Q_2 \in E_{P, Q}$ such that $|H_{P, Q} \cap C|$ is odd for $j = 1, 2$; moreover, the two points associated with one class $[\pi_{k_1}]$ are different from those associated with the other class $[\pi_{k_2}]$, where $[\pi_{k_1}] \neq [\pi_{k_2}]$.

**Proof** Since $G$ acts transitively on $I$ and preserves incidence, without loss of generality, we may assume that $P = (1, 0, -\xi)$. From (2.4), it follow that

\[
K := G_P = \left\{ \begin{array}{l} \\
\left( \begin{array}{c} d^2 \\ 2cd \\
2c^2 \\
-dc \\
-c^2 \\
-cd \\
d \\
d \\
d \\
d \\
-dc \\
-c \\
-c \\
-c \end{array} \right) \mid d, c \in \mathbb{F}_q, d^2 - c^2 = 1 \right\}
\]

(3.4)

Since $K$ is transitive on both $P_{\mathbb{P}_P}$ and $\text{Sep}$ by Proposition 2.12 and

$$|H_{P, Q} \cap C| = |(H_{P, Q} \cap C)^2| = |H_{P, Q} \cap C|$$

by Corollary 3.4, we may assume that $Q$ is on either $\ell_1$ or $\ell_2$, where $\ell_1 = [1, 0, \xi^{-1}] \in P_{\mathbb{P}_P}$ and $\ell_2 = [0, 1, 0] \in \text{Sep}$.
Case I. \( Q \in \ell_1 \) and \( Q \notin P^\perp \).

In this case, \( Q = (1, x, -\xi) \) for some \( x \in \mathbb{F}_q^* \) and \( x^2 + \xi \in \mathbb{D}_q \), and

\[
P_{aQ} = \{[1, s, (1 + sx)\xi^{-1}] \mid s \in \mathbb{F}_q, s^2 - 4(1 + sx)\xi^{-1} \in \mathbb{Z}_q \}.
\]

Using (3.4), we obtain that

\[
K_Q = \{d(1, 1, 1), ad(1, -\xi^{-1}, \xi^{-2})\}.
\]

It is apparent that \( d(1, 1, 1) \) fixes each line in \( P_{aQ} \). From

\[
ad(1, -\xi^{-1}, \xi^{-2})^{-1}(1, s, (1 + sx)\xi^{-1})^T = ((1 + sx)\xi, -s\xi, 1)^T,
\]

it follows that \( [1, s, (1 + sx)\xi^{-1}] \in P_{aQ} \) is fixed by \( K_Q \) if and only if \( s = 0 \) or \( s = -2x^{-1} \). Therefore, \( K_Q \) has two orbits of length 1 on \( P_{aQ} \), i.e. \( \{\ell_1 = [1, 0, \xi^{-1}]\} \) and \( \{\ell_3 = [1, -2x^{-1}, -\xi^{-1}]\} \), and all other orbits, whose representatives are \( R_{1} \), have length 2. From

\[
\dim_{\mathbb{F}_2} \mathcal{N}_{P, Q} \cap C = |\mathcal{S}_{P, \ell_1} \cap C| + |\mathcal{S}_{P, \ell_3} \cap C| + 2 \sum_{\ell \in R_{1}} |\mathcal{S}_{P, \ell} \cap C|,
\]

it follows that the parity of \( \dim_{\mathbb{F}_2} \mathcal{N}_{P, Q} \cap C \) is determined by that of \( |\mathcal{S}_{P, \ell_1} \cap C| + |\mathcal{S}_{P, \ell_3} \cap C| \).

Here we used the fact that \( |\mathcal{S}_{P, \ell} \cap C| = |\mathcal{S}_{P, \ell'} \cap C| \) if \( \{\ell, \ell'\} \) is an orbit of \( K_P \) on \( P_{aQ} \). It is clear that \( |\mathcal{S}_{P, \ell} \cap D| = |\mathcal{S}_{P, \ell_3} \cap D| = 0 \).

Note that the quadruples \((a, b, c, d)\) that determine group elements in \( \mathcal{S}_{P, \ell_1} \cap C \) satisfy the following equations

\[
-2cd + 2ab\xi^{-1} = 0,
\]

\[
c^2 - a^2\xi^{-1} = (d^2 - b^2\xi^{-1})\xi^{-1}
\]

\[
a + d = s
\]

\[
ad - bc = 1
\]

(3.5)

where \( s^2 = 4, \pi_k, \theta_i \). The first two equations in (3.5) give \( c = \pm \sqrt{-1}b\xi^{-1} \) and \( a = \pm \sqrt{-1}d \). Combining them with the last two equations in (3.5), we obtain 0, 4 or 8 quadruples \((a, b, c, d)\) satisfying the above equations, among which, both \((a, b, c, d)\) and \((-a, -b, -c, -d)\) do appear at the same time. Therefore, \( |\mathcal{S}_{P, \ell_1} \cap C| \) is 0, 2, or 4. Particularly, in \([0] \), there might be only 2 elements satisfying the above conditions.

Similarly, the quadruples \((a, b, c, d)\) that determine a group element in \( \mathcal{S}_{P, \ell_3} \cap C \) satisfy the following equations

\[
-cd + ab\xi^{-1} = -x^{-1}(d^2 - b^2\xi^{-1})
\]

\[
c^2 - a^2\xi^{-1} = -\xi^{-1}(d^2 - b^2\xi^{-1})
\]

\[
a + d = s
\]

\[
ad - bc = 1
\]

(3.6)

where \( s^2 = 4, \pi_k, \theta_i \). In (3.6), after squaring both sides of the first equation and multiplying both sides of the second equation by \( d^2 - b^2\xi^{-1} \) and then subtracting both sides of the resulting equations, we obtain

\[
d^2 - b^2\xi^{-1} = \pm A,
\]

(3.7)
Combining \( |H|\), if (3.6) determines an odd number of group elements, then
\[ -(\pm 2A + 2 - s^2)\xi^{-1} \notin \mathbb{Q}_q. \]

Hence, if (3.6) determines an odd number of group elements, then
\[ -(\pm 2A + 2 - s^2)\xi^{-1} \notin \mathbb{Q}_q. \]

From (3.7), \( c^2 - a^2\xi^{-1} = \mp A\xi^{-1} \) and \( a^2 + d^2 = s^2 - 2 - 2bc \), it follows that
\[ (b\xi^{-1} + c)^2 = -(\pm 2A + 2 - s^2)\xi^{-1}. \]

Therefore, in this case, we have
\[ -(\pm 2A + 2 - s^2)\xi^{-1} \notin \mathbb{Q}_q. \]

If \( -(\pm 2A + 2 - s^2)\xi^{-1} \in \mathbb{Q}_q \), we set \( B_{(\pm)} := \sqrt{-(\pm 2A + 2 - s^2)\xi^{-1}} \). From \( c^2 - a^2\xi^{-1} = \pm A\xi^{-1} \) and \( d^2 - b^2\xi^{-1} = \mp A \), we have
\[ d = \frac{1}{2s}[s^2 + (\xi B^2_{(\pm)} - 2B_{(\pm)}b)] \quad (\text{or } d = \frac{1}{2s}[s^2 + (\xi B^2_{(\pm)} + 2B_{(\pm)}b)]) \]
and thus
\[ a = \frac{1}{2s}[s^2 - (\xi B^2_{(\pm)} - 2B_{(\pm)}b)] \quad (\text{or } a = \frac{1}{2s}[s^2 - (\xi B^2_{(\pm)} + 2B_{(\pm)}b)]). \]

Combining \( b = (\pm B_{(\pm)} - c)\xi \) and \( ad - bc = 1 \), we have
\[ \left(\xi - \frac{2B^2_{(\pm)}}{s^2}\right)c^2 + \left(\frac{\xi^2 B^3_{(\pm)}}{s^2} - B_{(\pm)}\xi\right)c + \left(\frac{s^2}{4} - \frac{\xi^2 B^4_{(\pm)}}{4s^2} - 1\right) = 0 \]
\[ \left(\xi - \frac{2B^2_{(\pm)}\xi^2}{s^2}\right)c^2 - \left(\frac{\xi^2 B^3_{(\pm)}}{s^2} - B_{(\pm)}\xi\right)c + \left(\frac{s^2}{4} - \frac{B^4_{(\pm)}}{4s^2} - 1\right) = 0. \]

The discriminant of (3.12) or (3.13) is
\[ \Delta = \left(\frac{\xi^2 B^2_{(\pm)} - \xi B_{(\pm)}}{s^2}\right)^2 - 4 \left(\xi - \frac{\xi^2 B^2_{(\pm)}}{s^2}\right) \left(\frac{s^2}{4} - \frac{\xi^2 B^4_{(\pm)}}{4s^2} - 1\right)
= \xi \left(1 - \frac{\xi B^2_{(\pm)}}{s^2}\right) \left(4 - s^2 + \xi B^2_{(\pm)}\right)
= \frac{4\xi^2 \xi}{x^2 + 4\xi^{-1}} \in \mathbb{Q}_q. \]

From (3.10), (3.11), (3.12), (3.13), and (3.14), it follows that (3.6) produces 2 or 4 group elements; that is, \(|S_{P_1, t} \cap C| = 2 \text{ or } 4\).

If \( -(\pm 2A + 2 - s^2)\xi^{-1} = 0 \), then \( s^2 \) can be only one of \( 2A + 2 \) and \(-2A + 2 \) since from (3.8)
\[ (2A + 2)(-2A + 2) = \frac{4\xi^2}{x^2 + \xi^{-1}} \in \mathbb{Q}_q. \]

Therefore, in this case, we have \(|s^2| \cap S_{P_1, t} = 1\). It is also clear that, for the same \([s^2]\),
\[ |[s^2] \cap S_{P_1, t}| \]
is odd, where \( P_1 = (1, -x, -\xi) \in E_{t\ell}. \) Moreover, when \( x \) runs over
\[ L := \{ x \in \mathbb{F}_q^n \mid x^2 + \xi \in \square_q \} \]

once, each \([\pi_k]\) with \(1 \leq k \leq \frac{q-1}{4}\) appears exactly twice in the multiset

\[
\left\{ 2 \sqrt{\frac{1}{(x^{-2} + \xi^{-1})\xi}} + 2 \right\} \cup \left\{ -2 \sqrt{\frac{1}{(x^{-2} + \xi^{-1})\xi}} + 2 \right\}.
\]

Note that

\[
\pm \frac{2}{\sqrt{(x^{-2} + \xi^{-1})\xi}} + 2 = \pm \frac{2}{\sqrt{(x^{-2} + \xi^{-1})\xi}} + 2
\]

if and only if \(x_1 = \pm x_2\). Therefore, for each class \([\pi_k]\) with \(1 \leq k \leq \frac{q-1}{4}\), there are two different points \(Q_1, Q_2 \in E_{\ell_4, Q}\) such that \([\pi_k] \cap \mathcal{H}_{\ell_4, Q}\) is odd for \(j = 1, 2\); further, the two points associated with one class \([\pi_k]\) are different from those associated with the other class \([\pi_{k_2}]\), where \([\pi_{k_1}] \neq [\pi_{k_2}]\). The proof of (iii) is completed.

**Case II.** \(Q = \ell_1 \cap P^\perp\).

In this case, \(Q = (0, 1, 0)\). From (3.4), it follows that

\[ K_Q = \{ d(1, 1, 1), \text{ad}(-1, 1, -1), d(-1, -\xi^{-1}, -\xi^{-2}), \text{ad}(1, -\xi^{-1}, \xi^{-2}) \}. \]

Since \(Pa_Q = \{(1, 0, -x) \mid x \in \square_q\}\), it follows that the passant lines through \(Q\) that are fixed by \(K_Q\) are \(\ell_1 = [1, 0, \xi^{-1}]\) and \(\ell_4 = [1, 0, -\xi^{-1}]\). Thus, \(K_Q\) has two orbits of length 1 on \(Pa_Q\) and all the other orbits, whose representatives are \(R_2\), have length 2. By

\[ |\mathcal{H}_{\ell_4, Q} \cap C| = |\mathcal{S}_{\ell_1, 1} \cap C| + |\mathcal{S}_{\ell_4, 1} \cap C| + 2 \sum_{\ell \in R_2} |\mathcal{S}_{\ell, 1} \cap C|, \]

we obtain that the parity of \(|\mathcal{H}_{\ell_4, Q} \cap C|\) is determined by that of \(|\mathcal{S}_{\ell_1, 1} \cap C| + |\mathcal{S}_{\ell_4, 1} \cap C|\).

From the discussions in **Case I**, we know that \(|\mathcal{S}_{\ell_1, 1} \cap C|\) always even. Since \(\ell_4 = P^\perp\) and \(G_P = G_{P^\perp}\) by Lemma 2.13, it follows from Corollary 3.5 that \(|\mathcal{S}_{\ell_4, 1} \cap C|\) is odd if and only if \(C = D\). The proof of (ii) is completed.

**Case III.** \(Q \in \ell_2\).

In this case, \(Q = (1, 0, -y)\) for some \(y \in \square_q\). Using (3.4), we see that

\[ K_Q = \{ d(1, 1, 1), d(-1, 1, -1) \}. \]

Moreover, all the orbits of \(K_Q\) on \(Pa_Q = \{(1, s, y^{-1}) \mid s \in \mathbb{F}_q^*, s^2 - 4y^{-1} \in \square_q\}\) have length 2, then \(|\mathcal{H}_{\ell_4, Q} \cap C|\) is even for each \(C\). Part (i) is proved. \(\square\)

**Lemma 3.7** Assume that \(q \equiv 3 \pmod{4}\). Let \(P \in I\) and \(Q \in E\). Suppose that \(C = D[4]\), \([\pi_k](1 \leq k \leq \frac{q-3}{4})\), \([\theta_i](1 \leq i \leq \frac{q-3}{4})\).

(i) If \(\ell_4, Q \notin \text{Sep}\), for each class \([\theta_i]\) with \(1 \leq i \leq \frac{q-3}{4}\), there are two different points \(Q_1, Q_2 \in E_{\ell_4, Q}\) such that \([\theta_i] \cap \mathcal{H}_{\ell_4, Q}\) is odd for \(j = 1, 2\); moreover, the two points associated with one class \([\theta_i]\) are different from those associated with the other class \([\theta_{i_2}]\), where \([\theta_{i_1}] \neq [\theta_{i_2}]\).

(ii) If \(\ell_4, Q \notin \text{Sep}\) and \(Q \in P^\perp\), then \(|\mathcal{H}_{\ell_4, Q} \cap C|\) is odd if and only if \(C = D\).

(iii) If \(\ell_4, Q \in Pa_P\) and so \(|\mathcal{H}_{\ell_4, Q} \cap C|\) is even for each \(C\).

**Proof** The proof is essentially the same as the one of Lemma 3.6. We omit the details. \(\square\)
4 Group algebra $FH$

4.1 2-Blocks of $H$

In this section we recall several results on the 2-blocks of $H \cong PSL(2, q)$. We refer the reader to [13] or [2] for a general introduction on this subject.

Let $R$ be the ring of algebraic integers in the complex field $\mathbb{C}$. We choose a maximal ideal $M$ of $R$ containing $2R$. Let $F = R/M$ be the residue field of characteristic 2, and let $*: R \to F$ be the natural ring homomorphism. Define

$$S = \{ \frac{r}{s} \mid r \in R, \ s \in R \setminus M \}.$$  \hspace{1cm} (4.1)

Then it is clear that the map $*: S \to F$ defined by $(\frac{r}{s})^* = r^s(s^*)^{-1}$ is a ring homomorphism with kernel $\mathcal{P} = \{ \frac{r}{s} \mid r \in M, \ s \in R \setminus M \}$. In the rest of this article, $F$ will always be the field of characteristic 2 constructed as above. Note that $F$ is an algebraic closure of $\mathbb{F}_2$.

Let $Irr(H)$ and $IBr(H)$ be the set of irreducible ordinary characters and the set of irreducible Brauer characters of $H$, respectively. In the following, we deduce the 2-blocks of $H$ from the known results on the 2-blocks of $PSL(2, q)$. For basic results on blocks of finite groups, we refer the reader to Chapter 3 of [13].

The character tables of $PSL(2, q)$ were obtained by Jordan and Schur independently; see [10, 11], or [14] for the detailed discussions. The irreducible characters of $H$ can be read off from the character tables of $PSL(2, q)$ as follows.

**Lemma 4.1** ([10, 11, 14]) The irreducible ordinary characters of $H$ are:

(i) $1 = \chi_0, \gamma, \chi_1, ... , \chi_{\frac{q-1}{4}}, \beta_1, \beta_2, \phi_1, ..., \phi_{\frac{q-5}{4}}$ if $q \equiv 1 \pmod{4}$, where $1 = \chi_0$ is the trivial character, $\gamma$ is the character of degree $q$, $\chi_s$ for $1 \leq s \leq \frac{q-1}{4}$ are the characters of degree $q - 1, \phi_r$ for $1 \leq r \leq \frac{q-5}{4}$ are the characters of degree $q + 1$, and $\beta_i$ for $i = 1, 2$ are the characters of degree $\frac{q+1}{2}$;

(ii) $1 = \chi_0, \chi_1, ... , \chi_{\frac{q-1}{4}}, \beta_1, \eta_1, \eta_2, ... , \eta_{\frac{q-3}{4}}$ if $q \equiv 3 \pmod{4}$, where $1 = \chi_0$ is the trivial character, $\gamma$ is the character of degree $q$, $\chi_s$ for $1 \leq s \leq \frac{q-3}{4}$ are the characters of degree $q - 1, \phi_r$ for $1 \leq r \leq \frac{q-3}{4}$ are the characters of degree $q + 1$, and $\eta_i$ for $i = 1, 2$ are the characters of degree $\frac{q-1}{2}$;

The following lemma tells us how the irreducible ordinary characters of $H$ are partitioned into 2-blocks.

**Lemma 4.2** [16, Lemma 4.1] First assume that $q \equiv 1 \pmod{4}$ and $q - 1 = m2^n$, where $2 \nmid m$.

(i) The principal block $B_0$ of $H$ contains $2^{n-2} + 3$ irreducible characters $\chi_0 = 1, \gamma, \beta_1, \beta_2, \phi_0, \phi_{\frac{q^2-2-1}{1}}$.

where $\chi_0 = 1$ is the trivial character of $H$, $\gamma$ is the irreducible character of degree $q$ of $H$, $\beta_1$ and $\beta_2$ are the two irreducible characters of degree $\frac{q+1}{2}$, and $\phi_0$ for $1 \leq k \leq 2^{n-2} - 1$ are distinct irreducible characters of degree $q + 1$ of $H$.

(ii) $H$ has $\frac{q-1}{4}$ blocks $B_s$ of defect 0 for $1 \leq s \leq \frac{q-1}{4}$, each of which contains an irreducible ordinary character $\chi_s$ of degree $q - 1$. 

\[ \text{Springer} \]
(iii) If \( m \geq 3 \), then \( H \) has \( \frac{m - 1}{2} \) blocks \( B_t \) of defect \( n - 1 \) for \( 1 \leq t \leq \frac{m - 1}{2} \), each of which contains \( 2^{n - 1} \) irreducible ordinary characters \( \phi_j \) for \( 1 \leq j \leq 2^{n - 1} \).

Now assume that \( q \equiv 3 \pmod{4} \) and \( q + 1 = m2^n \), where \( 2 \nmid m \).

(iv) The principal block \( B_0 \) of \( H \) contains \( 2^{n - 2} + 3 \) irreducible characters

\[
\chi_0 = 1, \; \gamma, \; \eta_1, \; \eta_2, \; \chi_{01}, \ldots, \chi_{0(e^{2n-2} - 1)},
\]

where \( \chi_0 = 1 \) is the trivial character of \( H \), \( \gamma \) is the irreducible character of degree \( q \) of \( H \), \( \eta_1 \) and \( \eta_2 \) are the two irreducible characters of degree \( \frac{q - 1}{2} \), and \( \chi_k \) for \( 1 \leq k \leq 2^{n - 2} - 1 \) are distinct irreducible characters of degree \( q - 1 \) of \( H \).

(v) \( H \) has \( \frac{q^3 - 3}{4} \) blocks \( B_r \) of defect 0 for \( 1 \leq r \leq \frac{q^3 - 3}{4} \), each of which contains an irreducible ordinary character \( \phi_r \) of degree \( q + 1 \).

(vi) If \( m \geq 3 \), then \( H \) has \( \frac{m - 1}{2} \) blocks \( B_t \) of defect \( n - 1 \) for \( 1 \leq t \leq \frac{m - 1}{2} \), each of which contains \( 2^{n - 1} \) irreducible ordinary characters \( \chi_j \) for \( 1 \leq j \leq 2^{n - 1} \).

Moreover, the above blocks form all the 2-blocks of \( H \).

Remark 4.3 Parts (i) and (iv) are from Theorem 1.3 in [12] and their proofs can be found in Chapter 7 of III in [2]. Parts (iii) and (vi) are proved in Sects. II and VIII of [3].

4.2 Block idempotents

Let \( Bl(H) \) be the set of 2-blocks of \( H \). If \( B \in Bl(H) \), we write

\[
f_B = \sum_{\chi \in Irr(B)} e_{\chi},
\]

where \( e_{\chi} = \frac{\chi(1)}{|H|} \sum_{g \in H} \chi(g^{-1})g \) is a central primitive idempotent of \( \mathbb{Z}C(H) \) and \( Irr(B) = Irr(H) \cap B \). For future use, we define \( IBr(B) = IBr(H) \cap B \). Since \( f_B \) is an element of \( \mathbb{Z}C(H) \), we may write

\[
f_B = \sum_{C \in cl(H)} f_B(\hat{C})\hat{C},
\]

where \( cl(H) \) is the set of conjugacy classes of \( H \), \( \hat{C} \) is the sum of elements in the class \( C \), and

\[
f_B(\hat{C}) = \frac{1}{|H|} \sum_{\chi \in Irr(B)} \chi(1)\chi(x_C^{-1})
\]

(4.2)

with a fixed element \( x_C \in C \).

Theorem 4.4 Let \( B \in Bl(H) \). Then \( f_B \in \mathbb{Z}(SH) \). In other words, \( f_B(\hat{C}) \in S \) for each block of \( H \).

Proof It follows from Corollary 3.8 in [13].

We extend the ring homomorphism \( * : S \rightarrow F \) to a ring homomorphism \( * : SH \rightarrow FH \) by setting \( \sum_{g \in H} s g \) \( * = \sum_{g \in H} s^* g \). Note that * maps \( \mathbb{Z}(SH) \) onto \( \mathbb{Z}(FH) \) via \( \sum_{C \in cl(H)} s^* \hat{C} \). Now we define

\[
e_B = (f_B)^* \in \mathbb{Z}(FH),
\]

which is the block idempotent of \( B \). Note that \( e_B e_{B'} = \delta_{BB'} e_B \) for \( B, B' \in Bl(H) \), where \( \delta_{BB'} \) equals 1 if \( B = B' \), 0 otherwise. Also \( 1 = \sum_{B \in Bl(H)} e_B \).

\( \square \) Springer
All the block idempotents of the 2-blocks of $H$ are given in the following lemma; see [16] for the detailed calculations.

**Lemma 4.5** [16, Lemma 4.4] First assume that $q \equiv 1 \pmod{4}$ and $q - 1 = m2^n$ with $2 \nmid m$.

1. Let $B_0$ be the principal block of $H$. Then
   
   (a) $e_{B_0}(D) = 1$.
   (b) $e_{B_0}(F^+ +) = e_{B_0}(F^- -) \in F$.
   (c) $e_{B_0}([\theta_1]) \in F$, $e_{B_0}([0]) = 0$.
   (d) $e_{B_0}([\pi_k]) = 1$.

2. Let $B_s$ be any block of defect 0 of $H$. Then
   
   (a) $e_{B_s}(D) = 0$.
   (b) $e_{B_s}(F^+ +) = e_{B_s}(F^- -) = 1$.
   (c) $e_{B_s}([\theta_1]) \in F$, $e_{B_s}([0]) = 0$.
   (d) $e_{B_s}([\pi_k]) = 0$.

Suppose $m \geq 3$ and let $B'_t$ be any block of defect $n - 1$ of $H$. Then

3. Now assume that $q \equiv 3 \pmod{4}$. Suppose that $q + 1 = m2^n$ with $2 \nmid m$.

4. Let $B_0$ be the principal block of $H$. Then
   
   (a) $e_{B_0}(D) = 1$.
   (b) $e_{B_0}(F^+ +) = e_{B_0}(F^- -) \in F$.
   (c) $e_{B_0}([\theta_1]) \in F$.
   (d) $e_{B_0}([0]) = 0$, $e_{B_0}([\pi_k]) \in F$.

5. Let $B_r$ be any block of defect 0 of $H$. Then
   
   (a) $e_{B_r}(D) = 0$.
   (b) $e_{B_r}(F^+ +) = e_{B_r}(F^- -) = 1$.
   (c) $e_{B_r}([\theta_1]) = 0$.
   (d) $e_{B_r}([\pi_k]) \in F$.

6. Suppose that $m \geq 3$ and let $B'_t$ be any block of defect $n - 1$ of $H$. Then
   
   (a) $e_{B'_t}(D) = 0$.
   (b) $e_{B'_t}(F^+ +) = e_{B'_t}(F^- -) = 1$.
   (c) $e_{B'_t}([\theta_1]) = 0$.
   (d) $e_{B'_t}([0]) = 0$, $e_{B'_t}([\pi_k]) \in F$.

The following corollary will be used in the proof of Lemma 6.2.

**Corollary 4.6** Let $B_s(1 \leq s \leq \frac{q-1}{4})$ or $B_r(1 \leq r \leq \frac{q-3}{4})$ be the blocks of defect 0 of $H$ depending on whether $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$. Using the above notation,
(i) if $q \equiv 1 \pmod{4}$, for each $B_s$, there is a class $[\pi_k]$ such that $e_{B_s}([\pi_k]) \neq 0$;
(ii) if $q \equiv 3 \pmod{4}$, for each $B_r$, there is a class $[\theta_l]$ such that $e_{B_r}([\theta_l]) \neq 0$.

Proof First we assume that $q \equiv 1 \pmod{4}$. From Theorem 8.9 in [11], we have $\chi_s(g_k) = -\delta^{(2k)s} - \delta^{-(2k)s}$ for $1 \leq k \leq \frac{q-1}{4}$, where $\chi_s$ is the irreducible ordinary character lying in $B_s$, $g_k \in [\pi_k]$, and $\delta$ is a primitive $(q+1)$-th root of unit in $\mathbb{C}$. Note that

$$f_{B_s}([\pi_k]) = \frac{1}{|H|} \sum_{\chi_s \in B_s} \chi_s(1) \chi_s(g_k^{-1})$$

$$= \frac{q-1}{|H|} \left( \delta^{(2k)s} + \delta^{-(2k)s} \right).$$

Since

$$\sum_{k=1}^{(q-1)/4} e_{B_s}([\pi_k]) = \left( \frac{q-1}{|H|} \sum_{k=1}^{(q-1)/4} \delta^{(2k)s} + \delta^{-(2k)s} \right)^*$$

$$= \left( \frac{\delta^{2s} - \delta^{\frac{q+1}{2}s}}{1 - \delta^{2s}} + \frac{\delta^{-2s} - \delta^{\frac{q+1}{2}s}}{1 - \delta^{-2s}} \right)^*$$

$$= \left( \frac{\delta^{2s} - \delta^{\frac{q+1}{2}s}}{1 - \delta^{2s}} + \frac{\delta^{-2s} - \delta^{-\frac{q+1}{2}s}}{1 - \delta^{-2s}} \right)$$

$$= \left( \frac{\delta^{2s} - \delta^{\frac{q+1}{2}s}}{1 - \delta^{2s}} + \frac{1 - \delta^{\frac{q+3}{2}s}}{\delta^{2s} - 1} \right)^*$$

$$= 1,$$

we conclude that $e_{B_s}([\pi_k]) \neq 0$ for some $k$. Part (i) is proved.

Part (ii) can be proved in the same fashion using Theorem 8.11 in [11]; we omit the details.

Let $M$ be an $SH$-module. We denote the reduction $M/PM$, which is an $FH$-module, by $\overline{M}$. Then the following lemma is apparent.

Lemma 4.7 Let $M$ be an $SH$-module and $B \in Bl(H)$. Using the above notation, we have $\overline{f_B M} = e_B \overline{M}$, i.e. reduction commutes with projection onto a block $B$.

5 Linear maps and their matrices

Let $F$ be the algebraic closure of $\mathbb{F}_2$ defined in Sect. 4. From now on, $\chi_N$ for $N \subseteq E$ will be always regarded as a vector over $F$. Recall that for $P \in I$, $N_{Pa,E}(P)$ (respectively, $N_{se,E}(P)$) is the set of external points on the passant (respectively, secant) lines through $P$. We define $D$ (respectively, $D'$) to be the incidence matrix of $E$ and $N_{Pa,E}(P)$ (respectively, $N_{se,E}(P)$) for $P \in I$. Namely, the columns of $D$ and $D'$ can be viewed as the characteristic vectors of $N_{Pa,E}(P)$ and $N_{se,E}(P)$, respectively. In the following, we always regard both $D$ and $D'$ as matrices over $F$. 

\[ \text{Springer} \]
Definition 5.1 For $P \in I$, we define $G_P$ to be the column characteristic vector of $P$ with respect to $I$, i.e. $G_P$ is a 0-1 column vector of length $|I|$ with entries indexed by the internal points; the entry of $G_P$ is 1 if and only if $P$ is indexed by $I$.

Let $k$ be the complex field $\mathbb{C}$, the algebraic closure $F$ of $\mathbb{F}_2$, or the ring $S$ in (4.1). Let $k^I$ and $h^E$ be the free $k$-modules with the bases $\{G_P \mid P \in I\}$ and $\{\chi_P \mid P \in E\}$, respectively. If we extend the actions of $H$ on the bases of $k^I$ and $h^E$, which are defined by $\chi \cdot h = \chi_P h$ and $G_Q \cdot h = G_{Qh}$ for $P \in I$, $Q \in E$, and $h \in H$, linearly to $k^I$ and $h^E$ respectively, then both $k^I$ and $h^E$ are $kH$-permutation modules. Since $H$ is transitive on $I$, we have

$$k^I = \text{Ind}_k^I (1_k),$$

where $K$ is the stabilizer of an element of $I$ in $H$ and $\text{Ind}_k^H (1_k)$ is the $kH$-module induced by $1_k$.

The decomposition of $1 \uparrow_k^H$, the character of $\text{Ind}_k^H (1_k)$ where $k$ is the field of complex numbers, into a sum of the irreducible ordinary characters of degree $q$ is given as follows.

Lemma 5.2 [18, Lemma 5.2] Let $K$ be the stabilizer of an internal point in $H$.

Assume that $q \equiv 1 \pmod{4}$. Let $\chi_s$, $1 \leq s \leq \frac{q-1}{4}$, be the irreducible ordinary characters of degree $q-1$, $\phi_r$, $1 \leq r \leq \frac{q-3}{4}$, irreducible ordinary characters of degree $q+1$, $\gamma$ the irreducible of degree $q$, and $\beta_j$, $1 \leq j \leq 2$, irreducible ordinary characters of degree $\frac{q+1}{2}$.

(i) If $q \equiv 1 \pmod{8}$, then

$$1 \uparrow_k^H = 1 + \sum_{s=1}^{(q-1)/4} \chi_s + \gamma + \beta_1 + \beta_2 + \sum_{j=1}^{(q-5)/4} \phi_{r_j},$$

where $\phi_{r_j}$, $1 \leq j \leq \frac{q-9}{4}$, may not be distinct.

(ii) If $q \equiv 5 \pmod{8}$, then

$$1 \uparrow_k^H = 1 + \sum_{s=1}^{(q-1)/4} \chi_s + \gamma + \sum_{j=1}^{(q-5)/4} \phi_{r_j},$$

where $\phi_{r_j}$, $1 \leq j \leq \frac{q-5}{4}$, may not be distinct.

Next assume that $q \equiv 3 \pmod{4}$. Let $\chi_s$, $1 \leq s \leq \frac{q-3}{4}$, be the irreducible ordinary characters of degree $q-1$, $\phi_r$, $1 \leq r \leq \frac{q-3}{4}$, the irreducible ordinary characters of degree $q+1$, $\gamma$ the irreducible character of degree $q$, and $\eta_j$, $1 \leq j \leq 2$, the irreducible ordinary characters of degree $\frac{q-1}{2}$.

(iii) If $q \equiv 3 \pmod{8}$, then

$$1 \uparrow_k^H = 1 + \sum_{r=1}^{(q-3)/4} \phi_r + \sum_{j=1}^{(q-3)/4} \chi_{s_j},$$

where $\chi_{s_j}$, $1 \leq j \leq \frac{q-3}{4}$, may not be distinct.

(iv) If $q \equiv 7 \pmod{8}$, then

$$1 \uparrow_k^H = 1 + \sum_{r=1}^{(q-3)/4} \phi_r + \sum_{j=1}^{(q+1)/4} \chi_{s_j},$$

where $\chi_{s_j}$, $1 \leq j \leq \frac{q+1}{4}$, may not be distinct.
Corollary 5.3 Using the above notation,

(i) if \( q \equiv 1 \pmod{4} \), then the character of \( \text{Ind}_{K}^{H}(1) \cdot f_{B_{s}} \) is \( \chi_{s} \) for each block \( B_{s} \) of defect 0;

(ii) if \( q \equiv 3 \pmod{4} \), then the character of \( \text{Ind}_{K}^{H}(1) \cdot f_{B_{r}} \) is \( \phi_{r} \) for each block \( B_{r} \) of defect 0.

Proof The corollary follows from Lemma 4.2 and Lemma 5.2.

Since \( H \) preserves incidence, the following corollary is obvious.

Corollary 5.4 Let \( P \in I \). Using the above notation, we have

\[
\chi_{N_{P_{a},E}(P)} \cdot h = \chi_{N_{P_{a},E}(P^h)} \cdot h = \chi_{N_{S_{e},E}(P^h)}
\]

for \( h \in H \).

In the rest of the article, we always view \( G_{P} \) as a vector over \( F \). Consider the maps \( \phi_{B}, \phi_{D}, \) and \( \phi_{D'} \) from \( F^{I} \) to \( F^{E} \) defined by extending

\[
G_{P} \mapsto \chi_{P^\perp}, G_{P} \mapsto \chi_{N_{P_{a},E}(P)}, G_{P} \mapsto \chi_{N_{S_{e},E}(P)}
\]

linearly to \( F^{I} \), respectively. Then it is clear that as \( F \)-linear maps, the matrices of \( \phi_{B}, \phi_{D}, \) and \( \phi_{D'} \) are \( B, D, \) and \( D' \), respectively, and for \( x \in F^{I}, \phi_{B}(x) = Bx, \phi_{D}(x) = Dx \) and \( \phi_{D'}(x) = D'x \). Moreover, we have the following result.

Lemma 5.5 The maps \( \phi_{B}, \phi_{D}, \) and \( \phi_{D'} \) are all \( F H \)-module homomorphisms from \( F^{I} \) to \( F^{E} \).

Proof Let \( G_{P} \) be a basis element of \( F^{I} \). Then \( \phi(G_{P}) \cdot h = \phi(G_{P}) \cdot h \) since

\[
\phi_{B}(G_{P} \cdot h) = \chi_{(P^h)^\perp} = \chi_{P^\perp} \cdot h = \phi_{B}(G_{P}) \cdot h.
\]

By linearity of \( \phi_{B}, \) we have \( \phi_{B}(x) \cdot h = \phi_{B}(x \cdot h) \) for each \( x \in F^{I} \). The proof of the map \( \phi_{B} \) being \( FH \)-homomorphism is completed.

The proofs of the other two maps’ being homomorphisms are similar since

\[
\chi_{N_{P_{a},E}(P)} \cdot h = \chi_{N_{P_{a},E}(P^h)} \cdot h = \chi_{N_{S_{e},E}(P^h)}
\]

for \( h \in H \) and \( P \in I \) by Corollary 5.4. We omit the details.

For convenience, we use \( \text{col}_{F}(C) \) to denote the column space of the matrix \( C \) over \( F \).

Corollary 5.6 Using the above notation, we have \( \text{Im}(\phi_{B}) = \text{col}_{F}(B), \text{Im}(\phi_{D}) = \text{col}_{F}(D), \) and \( \text{Im}(\phi_{D'}) = \text{col}_{F}(D') \).

Now we define \( M_{1} := \langle \chi_{\ell} \mid \ell \in T \rangle_{F} \) and \( M_{2} := \langle \chi_{\ell_{i}} + \chi_{\ell_{j}} \mid \ell_{i} \neq \ell_{j} \in T \rangle_{F} \) to be the spans of the corresponding characteristic vectors over \( F \).

Lemma 5.7 The dimensions of \( M_{1} \) and \( M_{2} \) over \( F \) are \( \text{dim}_{F}(M_{1}) = q \) and \( \text{dim}_{F}(M_{2}) = q - 1 \), respectively. Moreover, the all-one column vector \( 1 \) of length \( \left| E \right| \) is neither in \( M_{1} \) nor in \( M_{2} \).

Proof Since \( \sum_{\ell \in T} \chi_{\ell} = 0, \) where \( 0 \) is the zero column vector of \( \left| E \right| \), it follows that \( \{ \chi_{\ell} \mid \ell \in T \} \) is linearly dependent over \( F \), i.e. \( \text{dim}_{F}(M_{1}) \leq q \). Now let \( T' \subset T \) with \( \left| T' \right| = q \) and suppose that \( \{ \chi_{\ell} \mid \ell \in T' \} \) is linearly dependent over \( F \). Then \( \sum_{\ell \in T'} a_{\ell} \chi_{\ell} = 0, \) where \( a_{\ell} \in F \) and \( a_{\ell_{1}} \neq 0 \) for some \( \ell_{1} \in T' \). Since there are \( q \) external points on \( \ell_{1} \) and there are
only $q - 1$ tangent lines other than $\ell_1$ in $T'$, some external point on $\ell_1$ must be passed only by $\ell_1$, among the tangent lines in $T'$, which forces $a_{\ell_1} = 0$, a contradiction. This shows that $T'$ must be linearly independent over $F$, and so $\dim_F(M_1) = q$. Moreover, if $T' \subset T$ and $|T'| = q$, then $\{\chi_\ell \mid \ell \in T'\}$ must be a basis for $M_1$.

Next if $\ell_1$ is a tangent line, then $M_2 = \langle \chi_\ell_1 + \chi_\ell \mid \ell \in T \setminus \{\ell_1\} \rangle_F$ since $\chi_\ell_1 + \chi_\ell_j = (\chi_\ell_1 + \chi_\ell_j + \chi_\ell_j)$. As $\sum_{\ell \in T \setminus \{\ell_1\}} (\chi_\ell_1 + \chi_\ell) = 0$, $\dim_F(M_2) \leq q - 1$. Let $T' \subset T \setminus \{\ell_1\}$ with $|T'| = q - 1$ and suppose that $\{\chi_\ell_1 + \chi_\ell \mid \ell \in T'\}$ is linearly dependent over $F$. Then $\sum_{\ell \in T'} a_\ell (\chi_\ell_1 + \chi_\ell) = \sum_{\ell \in T'} a_\ell \chi_\ell = 0$ since $|T'|$ is even, where $a_\ell \in F$ and $a_{\ell_2} \neq 0$ for some $\ell_2 \in T'$. By applying the same argument in the first paragraph of this proof, again, we obtain that $a_{\ell_2} = 0$ which is a contradiction. Therefore, $\{\chi_\ell_1 + \chi_\ell \mid \ell \in T'\}$ is linearly independent over $F$, and so $\dim_F(M_2) = q - 1$. Moreover, if $T' \subset T \setminus \{\ell_1\}$ and $|T'| = q - 1$, then $\{\chi_\ell_1 + \chi_\ell \mid \ell \in T'\}$ must be a basis for $M_2$.

Now we assume that $1 \in M_1$ and $\{\chi_\ell \mid \ell \in T'\}$ with $T' \subset T$ and $|T'| = q$ is a basis for $M_1$. Then $\sum_{\ell \in T'} a_\ell \chi_\ell = 1$, where $a_\ell \in F$ for $\ell \in T'$ and $a_{\ell_2} \neq 0$ for some $\ell_2 \in T'$. Since $|T' \setminus \{\ell_2\}| = q - 1$, some external point on $\ell_2$ must be only passed by $\ell_2$ among all the tangent lines in $T'$; this forces $a_{\ell_2} = 1$. For each $\ell \in T' \setminus \{\ell_2\}$, we have $a_\ell + a_\ell = 1$, that is, $a_\ell = 0$ for each $\ell \in T' \setminus \{\ell_2\}$. Thus $\chi_\ell_2 = 1$, which is impossible. Consequently, $1 \notin M_1$. Since $M_2 \subset M_1$, we have $1 \notin M_2$.

Lemma 5.8 If $q \equiv 1 \pmod{4}$, then $\col_F(D) = M_1$; if $q \equiv 3 \pmod{4}$, then $\col_F(D) = M_2$.

Proof Assume that $q \equiv 1 \pmod{4}$. Let $\chi_{N_{pa,E}(P)}$ be the column of $D$ indexed by $P$. Then $\chi_{N_{pa,E}(P)}$ is an $F$-linear combination of the generating elements of $M_1$ by Corollary 2.17. Now if $\chi_\ell$ is a generating element of $M_1$, then it is an $F$-linear combination of the columns of $D$ by Corollary 2.21. Therefore, $\col_F(D) = M_1$.

Now we assume that $q \equiv 3 \pmod{4}$. Let $\chi_{N_{pa,E}(P)}$ be the column of $D$ indexed by $P$. Suppose that $\ell(P)$ is a tangent line through an external point on $P_\perp$ and $T(P, \ell(P))$ is the set of tangent lines through the external points on $\ell(P)$ that are also on the passant lines through $P$. Then by Corollary 2.17 and the fact that $|T(P, \ell(P))| = \frac{q + 1}{2}$ is even, we have

$$
\chi_{N_{pa,E}(P)} = \sum_{\ell' \in T(P, \ell(P))} \chi_{\ell'}
= \sum_{\ell' \in T(P, \ell(P))} (\chi_{\ell'} + \chi_{\ell(P)});
$$

that is, $\chi_{N_{pa,E}(P)} \in M_2$. Now let $\chi_{\ell_1} + \chi_{\ell_2}$ be a generating element of $M_2$. Then we have

$$
\chi_{\ell_1} + \chi_{\ell_2} = \sum_{Q \in \cal{M}_2(P)} \chi_{N_{pa,E}(Q)}
$$

by Corollary 2.24, where $P = \ell_1 \cap \ell_2$. Hence, $\col_F(D) = M_2$.

Corollary 5.9 If $q \equiv 1 \pmod{4}$, $\text{rank}_2(D) = q$; if $q \equiv 3 \pmod{4}$, $\text{rank}_2(D) = q - 1$.

Proof It follows from Lemmas 5.7 and 5.8.

Further, we have the following decomposition of $\col_F(D')$.

Lemma 5.10 If $q \equiv 3 \pmod{4}$, then $\col_F(D') = \langle 1 \rangle \oplus \col_F(D)$ as $FH$-modules, where $\langle 1 \rangle$ is the trivial $FH$-module generated by the all-one column vector $1$. 

Springer
Proof Since each row of $D'$ has $\frac{(q-1)^2}{4}$ 1s, then

$$\sum_{P \in I} \chi_{N_{Se,E}}(P) = 1.$$  

For $h \in H$,

$$1 \cdot h = \left( \sum_{P \in I} \chi_{N_{Se,E}}(P) \right) \cdot h = \sum_{P \in I} \chi_{N_{Se,E}}(P^h) = \sum_{P \in I} \chi_{N_{Se,E}}(P) = 1 \in \text{col}_F(D).$$

Consequently, $\langle 1 \rangle$ is indeed a trivial submodule of $\text{col}_F(D')$.

It is clear that $\text{col}_F(D') = \langle 1 \rangle + \text{col}_F(D)$ since $\chi_{N_{Se,E}}(P) = 1 + \chi_{N_{Pa,E}}(P) \in \langle 1 \rangle + \text{col}_F(D)$. Further, $\langle 1 \rangle \cap \text{col}_F(D) = 0$ since $\text{col}_F(D) = M_2$ and $1 \notin M_2$ by Lemmas 5.7 and 5.8. ⊓⊔

6 Statement and proof of main theorem

The main theorem is given as follows.

Theorem 6.1 Let $\text{Im}(\phi_B)$ and $\text{Im}(\phi_D)$ be defined as above. As $FH$-modules,

(i) if $q \equiv 1 \pmod{4}$, then

$$\text{Im}(\phi_B) = \text{Im}(\phi_D) \oplus \left( \bigoplus_{s=1}^{\frac{q-1}{4}} M_s \right),$$

where $M_s$ for $1 \leq s \leq \frac{q-1}{4}$ are pairwise nonisomorphic simple $FH$-modules of dimension $q-1$;

(ii) if $q \equiv 3 \pmod{4}$, then

$$\text{Im}(\phi_B) = \langle 1 \rangle \oplus \text{Im}(\phi_D) \oplus \left( \bigoplus_{r=1}^{\frac{q-3}{4}} M_r \right),$$

where $M_r$ for $1 \leq s \leq \frac{q-3}{4}$ are pairwise nonisomorphic simple $FH$-modules of dimension $q+1$ and $\langle 1 \rangle$ is the trivial $FH$-module generated by the all-one column vector of length $|E|$.

To prove the main theorem, we need the following lemma.

Lemma 6.2 Let $q - 1 = 2^nm$ or $q + 1 = 2^nm$ with $2 \mid m$ depending on whether $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$. Using the above notation,

(i) if $q \equiv 1 \pmod{4}$, then $\text{Im}(\phi_B) \cdot e_{B_0} = \text{Im}(\phi_D)$, $\text{Im}(\phi_B) \cdot e_{B_s} \neq 0$ for $1 \leq s \leq \frac{q-1}{4}$, and $\text{Im}(\phi_B) \cdot e_{B_t'} = 0$ for $m \geq 3$ and $1 \leq t \leq \frac{m-1}{2}$;

(ii) if $q \equiv 3 \pmod{4}$, then $\text{Im}(\phi_B) \cdot e_{B_0} = \text{Im}(\phi_D)$, $\text{Im}(\phi_B) \cdot e_{B_r} \neq 0$ for $1 \leq r \leq \frac{q-3}{4}$, and $\text{Im}(\phi_B) \cdot e_{B_t'} = 0$ for $m \geq 3$ and $1 \leq t \leq \frac{m-1}{2}$.  

Springer
Proof It is clear that Im(φ_B) is generated by \{χ_{P\perp} | P \in I\} over F. Let B ∈ Bl(H). Since

\[\chi_{P\perp} \cdot e_B = \sum_{C ∈ cl(H)} e_B(\tilde{C}) \sum_{h ∈ C} \chi_{P\perp} \cdot h\]

\[= \sum_{C ∈ cl(H)} e_B(\tilde{C}) \sum_{h ∈ C} \chi_{(P\perp)^h}\]

\[= \sum_{C ∈ cl(H)} e_B(\tilde{C}) \sum_{h ∈ C} \sum_{Q ∈ (P\perp)^h \cap E} \chi_Q,\]

we have

\[\chi_{P\perp} \cdot e_B = \sum_{Q ∈ E} S(B, P, Q) \chi_Q,\]

where

\[S(B, P, Q) := \sum_{C ∈ cl(H)} |H_{P, Q} \cap C| e_B(\tilde{C}).\]

Assume first that \(q \equiv 1 \pmod{4}\). If \(ℓ_{P, Q} ∈ S_{P, P}\), then \(S(B, P, Q) = 0\) for each \(B ∈ Bl(H)\) since \(|H_{P, Q} \cap C| = 0\) in \(F\) for each \(C \neq [0]\) by Lemma 3.6(i) and \(e_{B_0}(\tilde{[0]}) = e_{B_1}(\tilde{[0]}) = e_{B_2}(\tilde{[0]}) = 0\) by 1(c), 2(c), 3(c) of Lemma 4.5.

If \(ℓ_{P, Q} ∈ P_{ap}\), and \(Q ∈ P_{\perp}\), by Lemma 3.6(ii), 1(a) and 1(c) of Lemma 4.5,

\[S(B_0, P, Q) = |H_{P, Q} \cap [0]| e_{B_0}(\tilde{[0]}) + |H_{P, Q} \cap D| e_{B_0}(\tilde{D}) = 0 + 1 = 1,\]

by Lemma 3.6(ii), 2(a) and 2(c) of Lemma 4.5,

\[S(B_s, P, Q) = |H_{P, Q} \cap [0]| e_{B_s}(\tilde{[0]}) + |H_{P, Q} \cap D| e_{B_s}(\tilde{D}) = 0 + 0 = 0,\]

by Lemma 3.6(ii), 3(a) and 3(c) of Lemma 4.5,

\[S(B_t, P, Q) = |H_{P, Q} \cap [0]| e_{B_t}(\tilde{[0]}) + |H_{P, Q} \cap D| e_{B_t}(\tilde{D}) = 0 + 0 = 0.\]

If \(Q\) is on a passant line \(ℓ\) through \(P\) and \(Q \notin P_{\perp}\), by Lemma 3.6(iii), 1(a) and 1(c) of Lemma 4.5,

\[S(B_0, P, Q) = |H_{P, Q} \cap [0]| e_{B_0}(\tilde{[0]}) + |H_{P, Q} \cap [π_k]| e_{B_0}(\tilde{[π_k]}) = 1,\]

by Lemma 3.6(iii), 3(a) and 3(c) of Lemma 4.5,

\[S(B_t, P, Q) = |H_{P, Q} \cap [0]| e_{B_t}(\tilde{[0]}) + |H_{P, Q} \cap [π_k]| e_{B_t}(\tilde{[π_k]}) = 0.\]

Since each class \([π_k]\) is associated with two different external points \(Q_{k_1}\) and \(Q_{k_2}\) on \(ℓ_{P, Q}\) satisfying \([|π_k| \cap H_{P, Q}],\) for \(i = 1, 2\) by Lemma 3.6(iii) and there are \(q^2 - 1/4\) classes of the form \([π_k]\) and there are \(q^2 - 1/4\) points in \(E_ℓ\) that are not on \(P_{\perp}\), we conclude that for each \(Q ∈ ℓ\) with \(Q \notin P_{\perp}\) there is a class \([π_k]\) such that \(|H_{P, Q} \cap [π_k]|\) is odd. Moreover, Lemma 4.6(i) guarantees the existence of nonzero \(e_{B_t}(\tilde{[π_k]})\) for each \(B_s\). Consequently, we have there is a \(Q\) on \(ℓ\) and a class \([π_k]\) such that

\[S(B_s, P, Q) = |H_{P, Q} \cap [0]| e_{B_s}(\tilde{[0]}) + |H_{P, Q} \cap [π_k]| e_{B_s}(\tilde{[π_k]}) = e_{B_s}(\tilde{[π_k]}) \neq 0.\]

Therefore, we have shown that \(\text{Im}(φ_B) \cdot e_{B_0} = \text{Im}(φ_D)\) and \(\text{Im}(φ_B) \cdot e_{B_s} \neq 0\) for each \(s\) and \(\text{Im}(φ_B) \cdot e_{B_t} = 0\). The proof of (i) is completed.
Now assume that $q \equiv 3 \pmod{4}$. If $\ell_{PQ} \in Pa_P$, then $S(B, PQ) = 0$ for each $B \in BI(H)$ since $|\tau_{PQ} \cap C| = 0$ by (4d), (5c), (6d) of Lemma 4.5.

Let $\ell_{PQ} \in Sep$ and $Q \in P^\perp$, by Lemma 3.7(ii), 4(a) and 4(d) of Lemma 4.5,

$$S(B_0, P, Q) = |\tau_{PQ} \cap [0]|e_{B_0}(\hat{0})| + |\tau_{PQ} \cap D|e_{B_0}(\hat{D}) = 0 + 1 = 1,$$

by Lemma 3.7(ii), 5(a) and 5(c) of Lemma 4.5,

$$S(B_1, P, Q) = |\tau_{PQ} \cap [0]|e_{B_1}(\hat{0})| + |\tau_{PQ} \cap D|e_{B_1}(\hat{D}) = 0 + 0 = 0,$$

and by Lemma 3.7(ii), 6(a) and 6(d) of Lemma 4.5,

$$S(B'_1, P, Q) = |\tau_{PQ} \cap [0]|e_{B'_1}(\hat{0})| + |\tau_{PQ} \cap D|e_{B'_1}(\hat{D}) = 0 + 0 = 0.$$

If $\ell_{PQ} \in Sep$ and $Q \notin P^\perp$, by Lemma 3.7(i), 4(c) and 4(d) of Lemma 4.5,

$$S(B_0, P, Q) = |\tau_{PQ} \cap [0]|e_{B_0}(\hat{0})| + |\tau_{PQ} \cap [\theta_i]|e_{B_0}(\hat{\theta_i}) = 1,$$

and by Lemma 3.7(i), 6(c) and 6(d) of Lemma 4.5,

$$S(B'_1, P, Q) = |\tau_{PQ} \cap [0]|e_{B'_1}(\hat{0})| + |\tau_{PQ} \cap [\theta_i]|e_{B'_1}(\hat{\theta_i}) = 0.$$

Since each class $[\theta_i]$ is associated with two different external points $Q_{i_1}$ and $Q_{i_2}$ on $\ell_{PQ}$ satisfying $|[\theta_i] \cap \tau_{PQ}|$ for $j = 1, 2$ by Lemma 3.7(i) and there are $q^3 - 1$ classes of the form $[\pi_k]$ and there are $q^2 - 2$ points in $E_\ell$ that are not on $P^\perp$, we conclude that for each $Q \in \ell$ with $Q \notin P^\perp$ there is a class $[\theta_i]$ such that $|\tau_{PQ} \cap [\theta_i]|$ is odd. Moreover, Lemma 4.6(ii) guarantees the existence of nonzero $e_{B_1}(\hat{\theta_i})$ for each $B_1$. Consequently, we have there is a $Q$ on $\ell$ and a class $[\theta_i]$ such that

$$S(B_1, P, Q) = |\tau_{PQ} \cap [0]|e_{B_1}(\hat{0})| + |\tau_{PQ} \cap [\theta_i]|e_{B_1}(\hat{\theta_i}) = e_{B_1}(\hat{\theta_i}) \neq 0.$$

Therefore, we have shown that $\text{Im}(\phi_B) \cdot e_{B_0} = \text{Im}(\phi_B \cdot e_{B_1})$ and $\text{Im}(\phi_B) \cdot e_{B_1} \neq 0$ for each $s$ and $\text{Im}(\phi_B) \cdot e_{B'_1} = 0$. The proof of (ii) is completed.

\begin{proof}[Proof of Theorem 6.1]
Let $B$ be a 2-block of defect 0 of $H$. Then by Lemma 4.7, we have

$$F^I \cdot e_B = \overline{S^I} \cdot f_B.$$

Therefore, by Corollary 5.3, $F^I \cdot e_B = N$, where $N$ is the simple $FH$-module of dimension $q - 1$ or $q + 1$ lying in $B$ accordingly as $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$. It is clear that $\phi_B(F^I) = \text{Im}(\phi_B)$.

Assume that $q \equiv 1 \pmod{4}$ and $q - 1 = m2^n$ with $2 \nmid m$. Since

$$1 = e_{B_0} + \sum_{s=1}^{(q-1)/4} e_{B_s} + \sum_{t=1}^{(m-1)/2} e_{B'_t},$$

\end{proof}
we have

\[
\text{Im}(\phi_B) = \text{Im}(\phi_B) \cdot e_{B_0} \oplus \left( \bigoplus_{s=1}^{(q-1)/4} \text{Im}(\phi_B) \cdot e_{B_s} \right) \oplus \left( \bigoplus_{t=1}^{(m-1)/2} \text{Im}(\phi_B) \cdot e_{B_t'} \right)
\]

\[
= \text{Im}(\phi_D) \oplus \left( \bigoplus_{s=1}^{(q-1)/4} \phi_B(F^I) \cdot e_{B_s} \right)
\]

\[
= \text{Im}(\phi_D) \oplus \left( \bigoplus_{s=1}^{(q-1)/4} \phi_B(N_s) \right)
\]

\[
= \text{Im}(\phi_D) \oplus \left( \bigoplus_{s=1}^{(q-1)/4} M_s \right)
\]

(6.1)

where \( N_s \) is the simple module of dimension \( q - 1 \) lying in \( B_s \) for each \( s \) by the discussion in the first paragraph and \( M_s := \phi_B(N_s) \) for each \( s \). In (6.1), the terms \( e_{B_t'} \) for \( 1 \leq t \leq \frac{m-1}{2} \) and \( \text{Im}(\phi_B) \cdot e_{B_t'} \) for \( 1 \leq t \leq \frac{m-1}{2} \) appear only when \( m \geq 3 \); the second equality holds since \( \text{Im}(\phi_B) \cdot e_{B_s'} = 0 \) for each \( t \) and \( \text{Im}(\phi_B) \cdot e_{B_0} = \text{Im}(\phi_B) \) by Lemma 6.2(i); and the third equality holds since \( \phi_B \) is an \( FH \)-homomorphism by Lemma 5.5 and \( e_{B_s} \in FH \). Consider the map

\[
\lambda_s : N_s \rightarrow \phi_B(N_s)
\]

defined by \( \lambda_s(n) = \phi_B(n) \) for \( n \in N_s \), where \( 1 \leq s \leq \frac{q-1}{4} \). It is clear that \( \lambda_s \) is the same as the restriction of \( \phi_B \) to \( N_s \). Consequently, \( \lambda_s \) is a surjective \( FH \)-homomorphism. Moreover, \( \text{Ker}(\lambda_s) \) is either \( 0 \) or \( N_s \) since, otherwise, \( \text{Ker}(\lambda_s) \) would be a nontrivial submodule of \( N_s \), which is impossible. If \( \text{Ker}(\lambda_s) = N_s \), then \( \phi_B(N_s) = \phi_B(F^I) \cdot e_{B_s} = 0 \), which is not the case by Lemma 6.2(i). Thus, we must have \( \text{Ker}(\lambda_s) = 0 \); that is, \( \lambda_s \) is an \( FH \)-isomorphism. So we have shown that \( M_s := \text{Im}(N_s) \cong N_s \) and thus \( M_s \) for \( 1 \leq s \leq \frac{q-1}{4} \) are pairwise nonisomorphic simple modules of dimension \( q - 1 \). The proof of (i) is finished.

Now assume that \( q \equiv 3 \pmod{4} \). Applying the same argument as above, we have

\[
\text{Im}(\phi_B) = \text{Im}(\phi_D') \oplus \left( \bigoplus_{r=1}^{(q-3)/4} M_r \right)
\]

where \( M_r \) for \( 1 \leq r \leq \frac{q-3}{4} \) are pairwise nonisomorphic simple \( FH \)-modules of dimension \( q + 1 \). Since \( \text{Im}(\phi_D') = \langle 1 \rangle \oplus \text{Im}(\phi_D) \) by Lemma 5.10, it follows that

\[
\text{Im}(\phi_B) = \langle 1 \rangle \oplus \text{Im}(\phi_D) \oplus \left( \bigoplus_{r=1}^{(q-3)/4} M_r \right)
\]

□

Now Conjecture 1.1 follows as a corollary.
Corollary 6.3 Let \( L \) and \( L_0 \) be the \( \mathbb{F}_2 \)-null spaces of \( B \) and \( B_0 \), respectively. Then

\[
\dim_{\mathbb{F}_2}(L) = \begin{cases} 
q^2 - q & \text{if } q \equiv 1 \pmod{4}, \\
q^2 - q + 1 & \text{if } q \equiv 3 \pmod{4}
\end{cases}
\]

and

\[
\dim_{\mathbb{F}_2}(L_0) = \begin{cases} 
q^2 - 1 & \text{if } q \equiv 1 \pmod{4}, \\
q^2 + 1 & \text{if } q \equiv 3 \pmod{4}.
\end{cases}
\]

Proof From Theorem 6.1 and Corollary 5.9, it follows that the 2-rank of \( B \) is

\[
\operatorname{rank}_2(B) = q + \frac{(q - 1)^2}{4}
\]

or

\[
\operatorname{rank}_2(B) = 1 + (q - 1) + \frac{(q + 1)(q - 3)}{4}
\]

accordingly as \( q \equiv 1 \pmod{4} \) or \( q \equiv 3 \pmod{4} \). Therefore, the dimension of the \( \mathbb{F}_2 \)-null space of \( B \) is

\[
\dim_{\mathbb{F}_2}(L) = \frac{q(q - 1)}{2} - (q + \frac{(q - 1)^2}{4}) = \frac{q^2 - 1}{4} - q
\]

or

\[
\dim_{\mathbb{F}_2}(L) = \frac{q(q - 1)}{2} - (1 + (q - 1) + \frac{(q + 1)(q - 3)}{4}) = \frac{q^2 - 1}{4} - q + 1
\]

accordingly as \( q \equiv 1 \pmod{4} \) or \( q \equiv 3 \pmod{4} \).

Since \( \operatorname{rank}_2(B) = \operatorname{rank}_2(B_0) \), the dimension of \( L_0 \) can be calculated in the same way. We omit the details. \( \square \)

Acknowledgments Research supported in part by NSF HBCU-UP Grant Award #0929257 at Lane College.

References

1. Assmus E.F.Jr., Key D.: Designs and Their Codes. Cambridge University Press, New York (1992).
2. Brauer R.: Some applications of the theory of blocks of characters of finite groups. I, II, III, and IV. J. Algebr. 1, 152–167, 304–334 (1964); 3, 225–255 (1966); 17, 489–521 (1971).
3. Burkhardt R.: Die zerkleugsmatrizen der gruppen PSL\(_2(2, p^f)\). J. Algebr. 40, 75–96 (1976).
4. Droms S., Mellinger K.E., Meyer C.: LDPC codes generated by conics in the classical projective plane. Des. Codes Cryptogr. 40, 343–356 (2006).
5. Frobenius G.: Über relationen zwischen den charakteren einer gruppe and denen ihrer untergruppen, S’ber. Akad. Wiss. Berlin. 501–515 (1898); Ges. Abh. III, 104–118.
6. Dye R.H.: Hexagons, conics, \( A_5 \) and PSL\(_2(K)\). J. Lond. Math. Soc. (2) 44, 270–286 (1991).
7. Hirschfeld J.W.P.: Projective Geometries Over Finite Fields, 2nd edn. Oxford University Press, Oxford (1998).
8. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
9. Hughes D.R., Piper F.C.: Projective Planes, Graduate Texts in Mathematics, vol. 6. Springer, New York (1973).
10. Jordan H.E.: Group-characters of various types of linear groups. Am. J. Math. 29, 387–405 (1907).
11. Karpilovsky G.: Group Representations, vol. 3, North-Holland, Amsterdam (1993).
12. Landrock P.: The principal block of finite groups with dihedral Sylow 2-subgroups. J. Algebr. 39, 410–428 (1976).
13. Navarro G.: Characters and Blocks of Finite Groups. London Mathematical Society Lecture Note Series, vol. 250. Cambridge University Press, Cambridge (1998).
14. Schur I.: Untersuchungen über die darstellung der endlichen gruppen durch gebrochene lineare substitutionen. J. Reine Angew. Math. 132, 85–137 (1907).
15. Segre B.: Ovals in a finite projective plane. Can. J. Math. 7, 414–416 (1955).
16. Sin P., Wu J., Xiang Q.: Dimensions of some binary codes arising from a conic in PG(2, q), J. Combin. Theory (A) 118, 853–878 (2011).
17. Store T.: Cyclotomy and Difference Sets. Markham, Chicago (1967).
18. Madison A.L., Wu J.: On binary codes from conics in PG(2, q). Eur. J. Combin. 33, 33–48 (2012).