ON BINARY CODES FROM CONICS IN PG(2, q)

ADONUS L. MADISON AND JUNHUA WU†,*

Abstract. Let $A$ be the incidence matrix of passant lines and internal points with respect to a conic in PG(2, q), where $q$ is an odd prime power. In this article, we study both geometric and algebraic properties of the column $\mathbb{F}_2$-null space $L$ of $A$. In particular, using methods from both finite geometry and modular presentation theory, we manage to compute the dimension of $L$, which provides a proof for the conjecture on the dimension of the binary code generated by $L$.

1. Introduction

Let PG(2, q) be the classical projective plane of order $q$ with underlying 3-dimensional vector space $V$ over $\mathbb{F}_q$, the finite field of order $q$. Throughout this article, PG(2, q) is represented via homogeneous coordinates. Namely, a point is written as a non-zero vector $(a_0, a_1, a_2)$ and a line is written as $[b_0, b_1, b_2]$ where not all $b_i$ ($i = 1, 2, 3$) are zero. The set of points

$$\mathcal{O} := \{(1, r, r^2) \mid r \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$$

(1.1)

give rise to a geometric object called conic in PG(2, q) [7]. The above set also comprises the projective solutions of the nondegenerate quadratic equation

$$Q(X_0, X_1, X_2) = X_1^2 - X_0 X_2$$

(1.2)

over $\mathbb{F}_q$. With respect to $\mathcal{O}$, the lines of PG(2, q) are partitioned into passant lines (Pa), tangent lines (T), and secant lines (Se) accordingly as the sizes of their intersections with $\mathcal{O}$ are 0, 1, or 2. Similarly, points are partitioned into internal points (I), conic points (O), and external points (E) accordingly as the numbers of tangent lines on which they lie are 0, 1, or 2.

In [4], one low-density parity-check binary code was constructed using the column $\mathbb{F}_2$-null space $L$ of the incidence matrix $A$ of passant lines and internal points with respect to $\mathcal{O}$. With the help of computer software Magma, the authors made a conjecture on the dimension of $L$ as follows:

**Conjecture 1.1.** [4] Conjecture 4.7 Let $L$ be the $\mathbb{F}_2$-null space of $A$, and let $\dim_{\mathbb{F}_2}(L)$ be the dimension of $L$. Then

$$\dim_{\mathbb{F}_2}(L) = \frac{(q-1)^2}{4}.$$
Let $F$ be an algebraic closure of $\mathbb{F}_2$. The idea of proving Conjecture \[ \text{L} \] is to first realize $\mathcal{L}$ as an $FH$-module and then decompose it into a direct sum of its certain submodules whose dimensions can be obtained easily. More concretely speaking, we view $A$ as the matrix of the following homomorphism $\phi$ of free $F$-modules:

$$\phi : F^I \to F^I$$

which first sends an internal point to the formal sum of all internal points on its polar, and then extends linearly to the whole of $F^I$. Additionally, it can be shown that $\phi$ is indeed an $FH$-module. Consequently, computing the dimension of the column $\mathbb{F}_2$-null space amounts to finding the dimension of the $F$-null space of $\phi$. To this end, we investigate the underlying $FH$-module structure of $\mathcal{L}$ by applying Brauer’s theory on the 2-blocks of $H$ and arrive at a convenient decomposition of $\mathcal{L}$.

This article is organized in the following way. In Section 2, we establish that the matrix $A$ satisfying the relation $A^3 \equiv A \pmod{2}$ under certain orderings of its rows and columns; this relation, in turn, reveals a geometric discription of $\ker(\phi)$ as well as yields a set of generating elements of $\ker(\phi)$ in terms of the concept of internal neighbors. In Section 3, the parity of intersection sizes of certain subsets of $H$ with the conjugacy classes of $H$ are computed. We will then in Section 4 review several facts about the 2-blocks of $PSL(2,q)$ and the block idempotents of the 2-blocks of $PSL(2,q)$; the detailed calculations of the 2-block idempotents were performed in \[ \text{[17]} \]. Combining the results in Sections 3 and 4 with Brauer’s theory on blocks, we are able to decompose $\ker(\phi)$ into a direct sum of all non-isomorphic simple $FH$-modules or this sum plus a trivial module depending on $q$. Consequently, the dimension of $\mathcal{L}$ follows as a lemma.

2. Geometry of Conics

First we recall several well-known results related to the geometry of conics in $PG(2,q)$ with $q$ odd. The books \[ \text{[8]} \] and \[ \text{[7]} \] are the references for what follows.

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 line and a line to a point, and preserves incidence. It is well known that each element of $GL(3,q)$, the group of all $3 \times 3$ non-singular matrices over $\mathbb{F}_q$, induces a collineation of $PG(2,q)$. The proof of the following lemma is straightforward.

**Lemma 2.1.** Let $P = (a_0, a_1, a_2)$ and $\ell = [b_0, b_1, b_2]$ be a point and a line of $PG(2,q)$, respectively. Suppose that $\theta$ is a collineation of $PG(2,q)$ that is induced by $D \in GL(3,q)$. If we use $P^\theta$ and $\ell^\theta$ to denote the images of $P$ and $\ell$ under $\theta$, respectively, then $P^\theta = (a_0, a_1, a_2)^\theta = (a_0, a_1, a_2)D$ 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 $D^{-1}(b_0, b_1, b_2)^\top$, respectively.

A correlation of $PG(2,q)$ 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 $PG(2,q)$ 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 \[ \text{[7]} \ p. 181 \] that the non-degenerate quadratic form $Q(X_0, X_1, X_2) = X_1^2 - X_0X_2$ induces a polarity $\sigma$ (or $\perp$) of $PG(2,q)$, which can be represented by the matrix

$$M = \begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}. \quad (2.1)$$
Lemma 2.2. ([8] p. 47) Let \( P = (a_0, a_1, a_2) \) and \( \ell = [b_0, b_1, b_2] \) be a point and a line of \( \text{PG}(2, q) \), respectively. If \( \sigma \) is the polarity represented by the non-singular symmetric matrix \( M \) in (2.1), 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 \( M(a_0, a_1, a_2)^T \), 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, we will denote the set of all non-zero squares of \( \mathbb{F}_q \) by \( \mathbb{F}_q^* \), and the set of non-squares by \( \mathbb{F}_q^\ast \); also, \( \mathbb{F}_q^\ast \) is the set of non-zero elements of \( \mathbb{F}_q \).

Lemma 2.3. ([7] p. 181–182) Assume that \( q \) is odd.

(i) The polarity \( \sigma \) above defines three bijections; that is, \( \sigma : I \rightarrow Pa, \sigma : E \rightarrow Se, \) and \( \sigma : \mathcal{O} \rightarrow T \) 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 \( \mathcal{O} \) if and only if 
\[ b_0^2 - 4b_0b_2 \in \mathbb{F}_q, b_1^2 - 4b_0b_2 = 0, \text{ or } b_1^2 - 4b_0b_2 \in \mathbb{F}_q, \]
respectively.

(iii) A point \((a_0, a_1, a_2)\) of \( \text{PG}(2, q) \) is internal, absolute, or external if and only if
\[ a_0^2 - a_0a_2 \in \mathbb{F}_q, a_1^2 - a_0a_2 = 0, \text{ or } a_1^2 - a_0a_2 \in \mathbb{F}_q, \]
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
\[ |T| = |\mathcal{O}| = q + 1, \quad |Pa| = |I| = \frac{q(q - 1)}{2}, \text{ and } |Se| = |E| = \frac{q(q + 1)}{2}. \tag{2.2} \]

Also, we have the following tables:

**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 | Skew lines |
|--------------|---------------|--------------|------------|
| Absolute points | 1             | \( q \)      | 0          |
| External points   | 2             | \( \frac{q - 1}{2} \) | \( \frac{q - 1}{2} \) |
| Internal points    | 0             | \( \frac{q + 1}{2} \) | \( \frac{q + 1}{2} \) |

2.1. The incidence matrix. Let \( G \) be the automorphism group of \( \mathcal{O} \) in \( \text{PGL}(3, q) \) (i.e. the subgroup of \( \text{PGL}(3, q) \) fixing \( \mathcal{O} \) setwise).

Lemma 2.5. ([7] p. 158] \( G \cong \text{PG}(2, q) \).

We define
\[ H := \left\{ \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix} \middle| a, b, c, d \in \mathbb{F}_q, ad - bc = 1 \right\}. \tag{2.3} \]
Lemma 2.8. Let $a, b, c \in \mathbb{F}_q$, we define
\[ d(a, b, c) := \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}, \quad ad(a, b, c) := \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix}. \]

For the convenience of discussion, we adopt the following special representatives of $G$ from [17]:
\[ H \cup d(1, \xi^{-1}, \xi^{-2}) \cdot H. \]  
(2.4)

Moreover, the following holds.

Lemma 2.6. The group $G$ acts transitively on both $I$ (respectively, $Pa$) and $E$ (respectively, $Se$).

The following result was proved in [17] and will be used frequently.

Lemma 2.7. Let $P$ be a point not on $O$, $\ell$ a non-tangent 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 $q \equiv 1 \pmod 4$, and $P^\perp \cap \ell \in I$ if $q \equiv 3 \pmod 4$.
(ii) If $P \in I$ and $\ell \in Se$, then $P^\perp \cap \ell \in I$ if $q \equiv 1 \pmod 4$, and $P^\perp \cap \ell \in E$ if $q \equiv 3 \pmod 4$.
(iii) If $P \in E$ and $\ell \in Pa$, then $P^\perp \cap \ell \in I$ if $q \equiv 1 \pmod 4$, and $P^\perp \cap \ell \in E$ if $q \equiv 3 \pmod 4$.
(iv) If $P \in E$ and $\ell \in Se$, then $P^\perp \cap \ell \in E$ if $q \equiv 1 \pmod 4$, and $P^\perp \cap \ell \in I$ if $q \equiv 3 \pmod 4$.

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

Lemma 2.8. Using the above notation,
(i) if $q \equiv 1 \pmod 4$, then $|((\Box_q - 1) \cap \Box_q| = \frac{q-5}{4}$ and
\[ |(\Box_q - 1) \cap \Box^q| = |((\Box_q - 1) \cap \Box_q| = |((\Box_q - 1) \cap \Box^q| = \frac{q-1}{4}; \]
(ii) if $q \equiv 3 \pmod 4$, then $|(\Box_q - 1) \cap \Box_q| = \frac{q+1}{4}$ and
\[ |(\Box_q - 1) \cap \Box^q| = |((\Box_q - 1) \cap \Box_q| = |((\Box_q - 1) \cap \Box^q| = \frac{q-3}{4}. \]

Definition 2.9. Let $P$ be a point not on $O$ and $\ell$ a line. We define $E_\ell$ and $I_\ell$ to be the set of external points and the set of internal points on $\ell$, respectively, $Pa_\ell$ and $Se_\ell$ the set of passant lines and the set of secant lines through $P$, respectively, and $T_\ell$ the set of tangent lines through $P$. Also, $N(P)$ is defined to be the set of internal points on the passant lines through $P$ including or excluding $P$ accordingly as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$.

Remark 2.10. Using the above notation, for $P \in I$, we have $|E_\ell| = |Se_\ell| = \frac{q+1}{2}$; $|I_\ell| = |Pa_\ell| = \frac{q+1}{2}$; and $|N(P)| = \frac{q^2-1}{4}$ or $\frac{q^2+3}{4}$ accordingly as $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$.

Let $P \in I$, $\ell \in Pa$, $g \in G$, and $W \leq G$. Using standard notations from permutation group theory, we have $I^g_\ell = I_\ell^g$, $Pa^g_\ell = Pa_\ell^g$, $E^g_\ell = E_\ell^g$, $Se^g_\ell = Se_\ell^g$, $H^g_\ell = H_\ell^g$, $N(P)^g = N(P)^g$, $(W^g)_\ell = W^g_\ell$. We will use these results later without further reference. Also, the definition of $G$ yields that $(P^\perp)^g = (P^g)^\perp$, where $\perp$ is the above defined polarity of $\mathrm{PG}(2, q)$.
Proposition 2.11. Let $P \in I$ and set $K := G_P$. Then $K$ is transitive on $I_P \cap E_P$, $P a_P$, and $S e_P$, respectively.

Proof: Witt’s theorem [9] implies that $K$ acts transitively on isometry classes of the form $Q$ on the points of $P^\perp$. Note that $K = G_{P^\perp}$ by the definition of $G$. Dually, we must have that $K$ is transitive on both $P a_P$ and $S e_P$.

When $P = (1,0,-\xi)$, using (2.2), (2.3), and (2.4), we obtain that $K := G_P = \{d^2 \quad cd \xi \quad c^2 \xi^2 \\
2cd \quad d^2 + c^2 \xi \quad 2dc \xi \\
c^2 \quad dc \quad -d^2 \}
\bigcup
\{d^2 \quad -cd \xi \quad c^2 \xi^2 \\
2cd \quad d^2 - c^2 \xi \quad 2dc \xi \\
c^2 \quad -dc \quad -d^2 \}
| d, c \in \mathbb{F}_q, d^2 - c^2 \xi = 1 \}
\bigcup
\{d^2 \quad cd \quad c^2 \\
2cd \quad d^2 + c^2 \xi \quad 2dc \\
c^2 \quad dc \xi \quad d^2 \}
| d, c \in \mathbb{F}_q, 2dc - c^2 \xi = 1 \}
\bigcup
\{d^2 \quad -cd \quad c^2 \\
2cd \quad d^2 - c^2 \xi \quad 2dc \\
c^2 \quad -dc \xi \quad d^2 \}
| d, c \in \mathbb{F}_q, -2d^2 \xi + c^2 = 1 \}
| (2.5)\}

Recall that $N(P)$ for $P \in I$ is the set of internal points on the passant lines through $P$, where $P$ is included or not accordingly as $q \equiv 3 \pmod{4}$ or $q \equiv 1 \pmod{4}$.

Theorem 2.12. Let $P \in I$ and $\ell \in Pa$. Then $|N(P) \cap I_\ell| \equiv 0 \pmod{2}$.

Proof: If $P \in \ell$, it is clear that $|N(P) \cap I_\ell| = \begin{cases} \frac{q-1}{2}, & \text{if } q \equiv 1 \pmod{4}, \\ \frac{q+1}{2}, & \text{if } q \equiv 3 \pmod{4}, \end{cases}$
which is even. Therefore, $|N(P) \cap I_\ell| \equiv 0 \pmod{2}$ for this case.

If $\ell = P^\perp$, by Lemma 2.13(i), we have $|N(P) \cap I_\ell| = \begin{cases} 0, & \text{if } q \equiv 1 \pmod{4}, \\ \frac{q+1}{2}, & \text{if } q \equiv 3 \pmod{4}, \end{cases}$
which is even. Hence, $|N(P) \cap I_\ell| \equiv 0 \pmod{2}$ for this case.

Now we assume that neither $\ell = P^\perp$ nor $P \in \ell$. As $G$ is transitive on $Pa$ and preserves incidence, we may take $\ell = P^\perp = [1,0,-\xi^{-1}]$, where $P^\perp = (1,0,-\xi) \in I$. Since $P$ is either on a passant line through $P_1$ or on a secant line through $P_1$, the rest it to show that $|N(P) \cap I_\ell|$ is even for any $P$ on a line through $P_1$ with $P \notin \ell$ and $P \neq P_1$.

Case I: $P$ is a point on a secant line through $P_1$ and $P \notin \ell$.

Since $K = G_{P_1}$ acts transitively on $S e_{P_1}$ by Proposition 2.11, it is enough to establish that $|N(P) \cap I_\ell|$ is even for an arbitrary internal point on a special secant line, $\ell_1$ say, through $P_1$. To this end, we may take $\ell_1 = [0,1,0]$. It is clear that $I_{\ell_1} = \{(1,0,-\xi^j) \mid 0 \leq j \leq q-1, \; j \text{ odd}\}$
and
$I_\ell = \{(1,s,\xi) \mid s \in \mathbb{F}_q, \; s^2 - \xi \in \mathbb{F}_q \}.

Hence, if $P = (1,0,-\xi^j) \in I_{\ell_1}$ then
$D_j = \left\{ \left[ 1, -\frac{\xi^{1-j} + 1}{s} \right] \mid s \in \mathbb{F}_q^*, \; s^2 - \xi \in \mathbb{F}_q \right\} \cup \{[0,1,0]\}$
consists of the lines through both $P$ and the points on $\ell$. Note that the number of passant lines in $D_j$ is determined by the number of $s$ satisfying both

$$\frac{1}{s^2}(\xi^{1-j} + 1)^2 - \frac{4}{\xi^j} \in \mathcal{Q}_q$$  \hspace{1cm} (2.6)$$

and

$$s^2 - \xi \in \mathcal{Q}_q.$$  \hspace{1cm} (2.7)$$

Since, $s \neq 0$ and whenever $s$ satisfies both (2.6) and (2.7), so does $-s$, we see that $|N(P) \cap I_\ell|$ must be even in this case.

**Case II.** $P$ is an internal point on a passant line through $P_1$ and $P \notin \ell$.

By Lemma 2.7, we may assume that $P \in P_3^4$, where $P_3 = (1, x, \xi) \in I_\ell$ with $x \in \mathbb{F}_q^*$ and $x^2 - \xi \in \mathcal{Q}_q$. Here $P_3^4 = [1, -\frac{2x}{\xi}, \frac{1}{x}]$ is a passant line through $P_1$. Let $K = G_{P_1}$. Using (2.5), we can obtain $L := K_{P_3}$ as follows: if $q \equiv 1 \pmod{4}$,

$$L = \left\{ \left( \begin{array}{ccc} \xi & x^2 - \xi & \xi x^2 - \xi \\ -2x & x^2 + x & -2x^2 \\ (x^2 - \xi)x & x^2 - \xi & x^2 - \xi \end{array} \right) \right\} \bigcup \left\{ \left( \begin{array}{ccc} x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \right\};$$  \hspace{1cm} (2.8)$$

if $q \equiv 3 \pmod{4}$,

$$L = \left\{ \left( \begin{array}{ccc} \xi & x^2 - \xi & \xi x^2 - \xi \\ -2x & x^2 + x & -2x^2 \\ (x^2 - \xi)x & x^2 - \xi & x^2 - \xi \end{array} \right) \right\} \bigcup \left\{ \left( \begin{array}{ccc} x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \right\};$$  \hspace{1cm} (2.9)$$

Let $(1, y, \xi)$ be a point on $\ell$. Using (2.5) and (2.9), we have that $L$ fixes $(1, y, \xi)$ if and only if

$$xy^2 - (x^2 + \xi)y + x\xi = 0;$$

that is, $y = x$ or $y = \frac{\xi}{x}$. Consequently, $P_3 = (1, x, \xi)$ and $\ell \cap P_3^4 = (1, \frac{\xi}{x}, \xi)$ are the only points of the form $(1, s, t)$ on $\ell$ fixed by $L$. Since $P \in P_3^4$, $P \notin P_1$ and $P \notin P_3^4 \cap \ell$, $P = (1, \xi + n, n)$ for some $n \neq \xi$. Now if we denote by $V$ the set of passant lines through $P$ that meet $\ell$ in an internal point, then it is clear that $|V| = |N(P) \cap I_\ell|$. Direct computations give us that $L_P \cong Z_2$. Since $P_3$ and $P$ are both fixed by $L_P$, it follows that both $\ell_{P_3,P}$ and $P_3^4$ are fixed by $L_P$. Note that when $q \equiv 3 \pmod{4}$, both $P_3^4$ and $\ell_{P_3,P}$ are in $V$; and when $q \equiv 1 \pmod{4}$, neither $\ell_{P_3,P}$ nor $P_3^4$ is in $V$. If there were another line $\ell'$ through $P$ which is distinct from both $P_3^4$ and $\ell_{P_3,P}$ and which is also fixed by $L_P$, then $L_P$ would fix at least three points on $\ell = P_4^4$, namely, $\ell' \cap \ell$, $P_3^4 \cap \ell$, and $P_3$. Since no further point of the form $(1, s, t)$ except for $P_3$ and $\ell \cap P_3^4$ can be fixed by $L$ due to the above discussion, we must have $\ell' \cap \ell = (0, 1, 0) \in E_\ell$. So $\ell' \notin V$. Using the fact that $L_P$ preserves incidence, we conclude that when $q \equiv 1 \pmod{4}$, $L_P$ has $\frac{\sqrt{q}}{2}$ orbits of length 2 on $V$; and when $q \equiv 3 \pmod{4}$, $L_P$ has two orbits of length 1, namely, $\{P_3^4\}$. 

and \(\{\ell_{P_i, P}\}\), and \(\frac{|V| - 2}{2}\) orbits of length 2 on \(V\). Either forces \(|V|\) to be even. Therefore, 
\(|N(P) \cap I|\) is even. \(\square\)

Recall that \(A\) is the incidence matrix of \(Pa\) and \(I\) whose columns are indexed by the internal points \(P_1, P_2, \ldots, P_N\) and whose rows are indexed by the passant lines \(P_1^\perp, P_2^\perp, \ldots, P_N^\perp\); and \(A\) is symmetric. For the convenience of discussion, for \(P \in I\), we define

\[
\widehat{N}(P) = \begin{cases} 
N(P) \cup \{P\}, & \text{if } q \equiv 1 \pmod{4}, \\
N(P) \setminus \{P\}, & \text{if } q \equiv 3 \pmod{4}.
\end{cases}
\]

That is, \(\widehat{N}(P)\) is the set of the internal points on the passant lines through \(P\) including \(P\). It is clear that for \(P \not\in \ell\), \(|N(P) \cap I| = |\widehat{N}(P) \cap I|\).

**Lemma 2.13.** Using the above notation, we have \(A^3 \equiv A \pmod{2}\), where the congruence means entry-wise congruence.

**Proof:** Since the \((i, j)\)-entry of \(A^2 = A^\top A\) is the standard dot product of the \(i\)-th row of \(A^\top\) and \(j\)-th column of \(A\), we have

\[
(A^2)_{i,j} = (A^\top A)_{i,j} = \begin{cases} 
\frac{q+1}{2}, & \text{if } i = j, \\
1, & \text{if } \ell_{P_i, P_j} \in Pa, \\
0, & \text{otherwise.}
\end{cases}
\]

Therefore, the \(i\)-th row of \(A^2 \pmod{2}\) indexed by \(P_i\) can be viewed as the characteristic row vector of \(\widehat{N}(P_i)\).

If \(P_i \in P_j^\perp\), then \((A^3)_{i,j} = ((A^2)A^\top)_{i,j} = q\) since \((A^2)_{i,i} = \frac{q+1}{2}\) and there are \(\frac{q+1}{2}\) internal points other than \(P_i\) on \(P_j^\perp\) that are connected with \(P_i\) by the passant line \(P_j^\perp\).

If \(P_i \not\in P_j^\perp\), then \((A^3)_{i,j} = ((A^\top A)A^\top)_{i,j} \equiv |\widehat{N}(P_i) \cap I_{P_j^\perp}| = |N(P_i) \cap I_{P_j^\perp}| \equiv 0 \pmod{2}\) by Theorem 2.12. Consequently,

\[\widehat{N}(P_i) \equiv \begin{cases} 
1 \pmod{2}, & \text{if } P_i \in P_j^\perp, \\
0 \pmod{2}, & \text{if } P_i \not\in P_j^\perp.
\end{cases}\]

The lemma follows immediately. \(\square\)

3. The Conjugacy Classes and Intersection Parity

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

3.1. Conjugacy classes. The conjugacy classes of \(H\) can be read off in terms of the map \(T = \text{tr}(g) + 1\), where \(\text{tr}(g)\) is the trace of \(g\).

**Lemma 3.1.** [17] Lemma 3.2] The conjugacy classes of \(H\) are given as follows.

(i) \(D = \{d(1, 1, 1)\}\);
(ii) \(F^+ \) and \(F^-\), where \(F^+ \cup F^- = \{g \in H \mid T(g) = 4, \ g \notin d(1, 1, 1)\}\);
(iii) \([\theta_i] = \{g \in H \mid T(g) = \theta_i\}, 1 \leq i \leq \frac{q^2}{4} - 1 \pmod{4}\) if \(q \equiv 1 \pmod{4}\), or \(1 \leq i \leq \frac{q^2 - 3}{4} \pmod{4}\) if \(q \equiv 3 \pmod{4}\), where \(\theta_i \in \square_{q}, \theta_i \neq 4, \) and \(\theta_i - 4 \in \square_{q}\);
(iv) \([0] = \{g \in H \mid T(g) = 0\}\);
(v) \([\pi_k] = \{g \in H \mid T(g) = \pi_k\}, 1 \leq k \leq \frac{q^2 - 1}{4} \pmod{4}\) if \(q \equiv 1 \pmod{4}\), or \(1 \leq k \leq \frac{q^2 - 3}{4} \pmod{4}\) if \(q \equiv 3 \pmod{4}\), where \(\pi_i \in \square_{q}, \pi_i \neq 4, \) and \(\pi_i - 4 \in \square_{q}\).
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 $\mathcal{H}$. 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,

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

(3.1)

3.2. Intersection properties.

Definition 3.3. Let $P, Q \in I, W \subseteq I,$ and $\ell \in Pa$. We define $H_{P,Q} = \{h \in H \mid (P^\perp)^h \in Pa_Q\}$, $S_{P,\ell} = \{h \in H \mid (P^\perp)^h = \ell\}$, and $U_{P,W} = \{h \in H \mid P^h \in W\}$. That is, $H_{P,Q}$ consists of all the elements of $H$ that map the passant line $P^\perp$ to a passant line through $Q$. $S_{P,\ell}$ is the set of elements of $H$ that map $P^\perp$ to the passant line $\ell$, and $U_{P,W}$ is the set of elements of $H$ that map $P$ to a point in $W$.

Using the above notation, we have that $H_{P,S_{P,\ell}} = H_{P,Q}$, $S_{P,\ell} = S_{P,\ell}$, and $U_{P,W} = U_{P,W}$, where $H_{P,Q} = \{g^{-1}hg \mid h \in H_{P,Q}\}$, $S_{P,\ell} = \{g^{-1}hg \mid h \in S_{P,\ell}\}$, and $U_{P,W} = \{h^g \mid h \in U_{P,W}\}$. Moreover, it is true that $(C \cap H_{P,Q})^g = (C \cap H_{P,Q})^q$ and $(C \cap U_{P,W})^g = C \cap U_{P,W}$. In the following discussion, we will use these results without further reference.

Next we compute the size of the intersection of each conjugacy class of $H$ with $K$ which is a stabilizer of an internal point in $H$.

Corollary 3.4. Let $P \in I$ and $K = H_P$. Then we have

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

Proof: Let $Q = (1,0,-\xi)$ and $K_1 = H_Q$. As $H$ is transitive on $I$, $Q^g = P$ for some $g \in H$. Moreover,

$$|K \cap C| = |K^q \cap C| = |(K_1 \cap C)^g|.$$ 

Therefore, to prove the corollary, it is sufficient to assume that $P = Q$.

It is obvious that $|D \cap K| = 1$. Let $g \in K \cap C$. Using (2.3), we have that the quadruples $(a,b,c,d)$ determining $g$ satisfy the following equations

$$bd - ac\xi = 0,$$
$$b^2 - a^2\xi = -\xi(d^2 - c^2\xi),$$
$$ad - bc = 1,$$
$$a + d = s,$$  

where $s^2 = 0, 4, \pi_k, \theta_i$. The equations in (3.2) yield (1) $a = d = \frac{s}{2}, c^2 = \frac{s^2 - 4}{4}, b^2 = \frac{(s^2 - 4)\xi}{4}$ and (2) $a = -d, s = 0, c^2\xi - 1 = d^2$. From Case (1), we have $|K \cap [\pi_k]| = 2$ 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 $ad(-\xi, -1, \xi^{-1}) \in K \cap [0]$ in Case (1). Since the number of $t \in \mathcal{D}_q$ satisfying $t - 1 \in \mathcal{D}_q$ is $\frac{q+1}{2}$ or $\frac{q-1}{2}$ accordingly as $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$ by Lemma 2.10, the number of $c \in \mathbb{F}_q^\times$ satisfying $c^2\xi - 1 = 1$ in $\mathcal{D}_q$ is $2(|\mathcal{D}_q - 1| \cap \mathcal{D}_q)$ 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 $c^2\xi - 1 \in \mathcal{D}_q$. Therefore, Case (1) and Case (2) give rise to $\frac{q+1}{2}$ or $\frac{q+1}{2}$ different group elements in $K \cap [0]$ depending on $q$. The corollary now is proved. 

In the following lemmas, we investigate the parity of \(|\mathcal{H}_{P,Q} \cap C|\) for \(C \neq \{0\}\) and \(P, Q \in I\). Recall that \(\ell_{P,Q}\) is the line through \(P\) and \(Q\).

**Lemma 3.5.** Let \(P, Q \in I\). Suppose that \(C = D, [4], [\pi_k] (1 \leq k \leq \frac{q-1}{4})\), or \([\theta_i]\) (\(1 \leq i \leq \frac{q-5}{4}\)).

First assume that \(q \equiv 1 \pmod{4}\).

(i) If \(\ell_{P,Q} \in Pa_P\), then \(|\mathcal{H}_{P,Q} \cap C|\) is always even.

(ii) If \(\ell_{P,Q} \in Sep, Q \notin P^\perp\), and \(|\mathcal{H}_{P,Q} \cap C|\) is odd, then \(C = [\theta_{i_1}]\) or \([\theta_{i_2}]\).

(iii) If \(Q \in \ell_{P,Q} \cap P^\perp\) and \(|\mathcal{H}_{P,Q} \cap C|\) is odd, then \(C = D\).

Now assume that \(q \equiv 3 \pmod{4}\).

(iv) If \(\ell_{P,Q} \in Sep\), then \(|\mathcal{H}_{P,Q} \cap C|\) is always even.

(v) If \(\ell_{P,Q} \in Pa_P, Q \notin P^\perp\), and \(|\mathcal{H}_{P,Q} \cap C|\) is odd, then \(C = [\pi_{i_1}]\) or \([\pi_{i_2}]\).

(vi) If \(Q \in \ell_{P,Q} \cap P^\perp\) and \(|\mathcal{H}_{P,Q} \cap C|\) is odd, then \(C = D\).

**Proof:** We only provide the detailed proof for the case when \(q \equiv 1 \pmod{4}\). Since \(G\) acts transitively on \(I\) and preserves incidence, without loss of generality, we may assume that \(P = (1, 0, -\xi)\) and let \(K = G_P\).

Since \(K\) is transitive on both \(Pa_P\) and \(Sep\) by Proposition 2.11 and \(|\mathcal{H}_{P,Q} \cap C| = |(\mathcal{H}_{P,Q} \cap C)^g| = |\mathcal{H}_{P,Q_0} \cap C|\), we may assume that \(Q\) is on either \(\ell_1\) or \(\ell_2\), where \(\ell_1 = [1, 0, \xi_0] \in Pa_P\) and \(\ell_2 = [0, 1, 0] \in Sep\).

**Case I.** \(Q \in \ell_1\).

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

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

Using (2.5), we obtain that

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

It is obvious that \(d(1, 1, 1)\) fixes each line in \(Pa_Q\). From

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

it follows that a line of the form \([1, s, (1 + sx)\xi^{-1}]\) is fixed by \(K_Q\) if and only if \(s = 0\) or \(s = -2x^{-1}\). Further, since \([1, -2x^{-1}, -\xi^{-1}]\) is a secant line, we obtain that \(K_Q\) on \(Pa_Q\) has one orbit of length 1, i.e. \(\{\ell_1 = [1, 0, \xi^{-1}]\}\), and all other orbits, whose representatives are \(\mathcal{R}_1\), have length 2. From

\[|\mathcal{H}_{P,Q} \cap C| = |\mathcal{S}_{P,\ell_1} \cap C| + 2 \sum_{\ell \in \mathcal{R}_1} |\mathcal{S}_{P,\ell} \cap C| ,\]

it follows that the parity of \(|\mathcal{H}_{P,Q} \cap C|\) is determined by that of \(|\mathcal{S}_{P,\ell_1} \cap C|\). 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 \(Pa_Q\). Meanwhile, it is clear that \(|\mathcal{S}_{P,\ell_1} \cap D| = 0\).

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

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

where \(s^2 = 4, \pi_k, \theta_i\), and that if one of \(b\) and \(c\) is zero, so is the other. If \(b = c = 0\) and \(2 < q\) then the above (3.3) give 4 group elements in [2] and 0 element is any other classes. If neither \(b\) nor \(c\) is zero, then the first two equations in (3.3) yield \(b = \pm \sqrt{-1}\xi c\).
Combining with the last two equations in (3.3), we obtain 0, 4 or 8 quadruples \((a, b, c, d)\) satisfying the above equations, among which both \((a, b, c, d)\) and \((-a, -b, -c, -d)\) appear at the same time. Since \((a, b, c, d)\) and \((-a, -b, -c, -d)\) give rise to the same group element, we conclude that \(|S_{P, t_1} \cap C|\) is 0, 2, or 4.

**Case II.** \(Q \in \ell_2, Q \notin P^\perp,\) and \(Q \notin P.\)

In this case, \(Q = (1, 0, -y)\) for some \(y \in \mathbb{F}_q\) and \(y \neq \pm \xi.\) Using (2.5), we obtain that
\[
K_Q = \{d(1, 1, 1), d(1, 0, 0), d(-1, 1, -1), \xi y = \pm (d^2 - b \xi^{-1})\}. 
\]

Moreover, \(K_Q\) on \(Pa_Q = \{[1, s, y^{-1}] \mid s \in \mathbb{F}_q, s^2 - 4y^{-1} \in \mathbb{F}_q\}\) has one orbit of length 1, that is, \(\{\ell_4 = [1, 0, y^{-1}]\},\) and all other orbits are of length 2. Similar arguments as above show that the parity of \(|H_{P, Q} \cap C|\) is the same as that of \(|S_{P, t_1} \cap C|\). So the rest is to find the parity of \(|S_{P, t_1} \cap C|\). The group elements in \(S_{P, t_1} \cap C\) are determined by the quadruples \((a, b, c, d)\) satisfying the following equations:
\[
\begin{align*}
-2cd + 2ab\xi^{-1} &= 0 \\
c^2 - a^2\xi^{-1} &= (d^2 - b \xi^{-1})y^{-1} \\
a + d &= s \\
ad - bc &= 1.
\end{align*}
\] (3.4)

Note that if one of \(b\) and \(c\) is zero, so is the other. If neither \(b\) nor \(c\) is zero, then the first two equations in (3.4) yield \(b = \pm \sqrt{-\xi y}\) and \(a = \pm \sqrt{-\xi y^{-1}}d.\) Combining with the last two, the above quadruples \((a, b, c, d)\) yield 0, 2, or 4 group elements in \([s^2]\). If \(b = c = 0,\) then \(ad - 1, d^2 = \pm \sqrt{-y\xi^{-1}} \) and \(a^2 = \pm \sqrt{-\xi y^{-1}};\) and so
\[s^2 = \sqrt{-\xi y^{-1}} + \sqrt{-\xi y^{-1}} + 2 \quad \text{or} \quad s^2 = -\sqrt{-\xi y^{-1}} - \sqrt{-\xi y^{-1}} + 2.\]

Since \((\sqrt{-\xi y^{-1}} + \sqrt{-\xi y^{-1}} + 2)(\sqrt{-\xi y^{-1}} - \sqrt{-\xi y^{-1}} + 2) = (\sqrt{-\xi y^{-1}} + \sqrt{-\xi y^{-1}})^2,\) the above quadruples \((a, b, c, d)\) yield 0 or 1 group elements in two classes \([\theta_1]\) and \([\theta_2]\) where \(\theta_1 = \sqrt{-\xi y^{-1}} + \sqrt{-\xi y^{-1}} + 2)\) and \(\theta_2 = -\sqrt{-\xi y^{-1}} - \sqrt{-\xi y^{-1}} + 2.\) The above analysis shows that if \(|H_{P, Q} \cap C|\) is odd then \(C = [\theta_1]\) or \([\theta_2]\) in this case.

**Case III.** \(Q = \ell_2 \cap P^\perp.\)

In this case, \(Q = (1, 0, \xi)\) and the set of passant lines through \(Q\) is
\[Pa_Q = \{[1, u, -\xi^{-1}] \mid u \in \mathbb{F}_q, u^2 + \xi \in \mathbb{F}_q\}.\]

Using (2.5), we obtain that
\[
K_Q = \{d(1, 1, 1), d(1, 0, 0), d(-1, 1, -1), \xi y = \pm (d^2 - b \xi^{-1})\}. 
\]

Therefore, among the orbits of \(K_Q\) on \(Pa_Q, \{[1, 0, -\xi^{-1}]\}\) is the only one of length 1 and all others are of length 2. Hence, the parity of \(|H_{P, Q} \cap C|\) is the same as that of \(|S_{P, \perp} \cap C|\) which is the same as that of \(|K \cap C|;\) by Corollary 3.4 it follows that \(|K \cap C|\) is odd if and only if \(C = D.\)

For \(Q \in I,\) we denote by \(\overline{N(Q)}\) the complement of \(N(Q)\) in \(I,\) that is, \(\overline{N(Q)} = I \setminus N(Q).\)

**Lemma 3.6.** Let \(P\) and \(Q\) be two distinct internal points.

Assume that \(q \equiv 1\) (mod 4).

(i) If \(\ell_{P, Q} \in Pa_P\) and \(|U_{P, N(Q)} \cap C|\) is odd, then \(C = [\pi_k]\) for one \(k\) or \(C = D.\)

(ii) If \(\ell_{P, Q} \in Sep,\) then \(|U_{P, N(Q)} \cap C|\) is even.

Assume that \(q \equiv 3\) (mod 4).

(iii) If \(\ell_{P, Q} \in Pa_P,\) then \(|U_{P, N(Q)} \cap C|\) is even.

(iv) If \(\ell_{P, Q} \in Sep\) and \(|U_{P, N(Q)} \cap C|\) is odd, then \(C = [\theta_i]\) for one \(i\) or \(C = D.\)
The discriminant of (3.7) or (3.8) is

\[ \Delta = (1 - \frac{B_2^2}{s^2\xi})(B_\pm^2 - s^2\xi + 4\xi) = \frac{4\xi u^2}{s^2(u^2 + \xi)} \in \mathbb{Q}. \]

Consequently, the equations in (3.6) have 8 solutions and yield 4 different group elements. If one of \( s^2\xi - (2 + A)\xi \) and \( s^2\xi - (2 - A)\xi \) is a square and the other is nonsquare, similar arguments as above give that the equations in (3.6) have 4 solutions and produce 2 different group element.

**Proof:** Without loss of generality, we can choose \( \mathbf{P} = (1, 0, -\xi) \). Since \( K = G_\mathbf{P} \) acts transitively on both \( Pa_\mathbf{P} \) and \( Se_\mathbf{P} \), we may assume that \( Q \neq \mathbf{P} \) is on either a special passant line \( \ell_1 = [1, 0, \xi^{-1}] \) or a special secant line \( \ell_2 = [0, 1, 0] \) through \( Q \).

**Case I.** \( \ell_1 = \ell_{\mathbf{P},Q} \in Pa_\mathbf{P} \).

In this case, \( Q = (1, x, -\xi) \) for some \( x \in \mathbb{F}_q \) with \( u^2 + \xi \in \mathbb{F}_q \) and its internal neighbor is \( N(Q) = \{(1, u, -\xi) \mid u^2 + \xi \in \mathbb{F}_q \} \setminus \{(1, x, -\xi)\} \) by definition. As \( \mathbf{P} \in N(Q) \), it is obvious that \( |U_{\mathbf{P},N(Q)} \cap D| = 1 \). Since the action of \( K_Q \) on \( Pa_Q \) has one orbit of length 1, i.e., \( \ell_1 \), and all others are of length 2, whose representatives form the set \( R_1 \), we obtain that

\[
|U_{\mathbf{P},N(Q)} \cap C| = \sum_{\ell \in Pa_Q} \sum_{\mathbf{P}_1 \in I_{\mathbf{P}} \setminus \{Q\}} |U_{\mathbf{P},\mathbf{P}_1} \cap C| = \sum_{\mathbf{P}_1 \in I_{\mathbf{P}} \setminus \{Q\}} |U_{\mathbf{P},\mathbf{P}_1} \cap C| + 2 \sum_{\ell \in R} \sum_{\mathbf{P}_1 \in I_{\mathbf{P}} \setminus \{Q\}} |U_{\mathbf{P},\mathbf{P}_1} \cap C|. \tag{3.5}
\]

Now let \( \mathbf{P}_1 = (1, u, -\xi) \in I_{\mathbf{P}} \setminus \{Q\} \). Then the number of group elements that map \( \mathbf{P} \) to \( \mathbf{P}_1 \) is determined by the quadruples \((a, b, c, d)\) which are the solutions to the following system of equations:

\[
\begin{align*}
ab - cd\xi &= u(a^2 - c^2\xi) \\
b^2 - d^2\xi &= -\xi(a^2 - c^2\xi) \\
a + d &= s \\
ad - bc &= 1.
\end{align*} \tag{3.6}
\]

The first two equations in (3.6) yield \( a^2 - c^2\xi = A \) (or \( -A \)) where \( A = \sqrt{\xi(u^2 + \xi^{-1})} \).

Now using \( b^2 - d^2\xi = \mp\xi A \), we obtain

\[
(b + c\xi)^2 = s^2\xi - (2 + A)\xi \quad \text{(or) } s^2\xi - (2 - A)\xi.
\]

If both \( s^2\xi - (2 + A)\xi \) and \( s^2\xi - (2 - A)\xi \) are squares, we set \( B_+ = \sqrt{s^2\xi - (2 + A)\xi} \) and \( B_- = \sqrt{s^2\xi - (2 - A)\xi} \), then

\[
a = \frac{1}{2s\xi}[s^2\xi - (B_+ - 2B_\pm\xi c)] \quad \text{(or) } \frac{1}{2s\xi}[s^2\xi - (B_+ + 2B_\pm\xi c)]
\]

and

\[
d = \frac{1}{2s\xi}[s^2\xi + (B_+ - 2B_\pm\xi c)] \quad \text{(or) } \frac{1}{2s\xi}[s^2\xi + (B_+ + 2B_\pm\xi c)]
\]

combining with the last two equations of (3.6), we have

\[
(\xi - \frac{B_2^2}{s^2\xi})c^2 + (\frac{B_3^2}{s^2\xi} - B_\pm)c + (\frac{s^2}{4} - \frac{B_4^2}{4s^2\xi^2} - 1) = 0 \tag{3.7}
\]

or

\[
(\xi - \frac{B_2^2}{s^2\xi})c^2 - (\frac{B_3^2}{s^2\xi} - B_\pm)c + (\frac{s^2}{4} - \frac{B_4^2}{4s^2\xi^2} - 1) = 0. \tag{3.8}
\]

The discriminant of (3.7) or (3.8) is

\[
\Delta = (1 - \frac{B_2^2}{s^2\xi})(B_\pm^2 - s^2\xi + 4\xi) = \frac{4\xi u^2}{s^2(u^2 + \xi)} \in \mathbb{Q}.
\]

If one of \( s^2\xi - (2 + A)\xi \) and \( s^2\xi - (2 - A)\xi \) is a square and the other is nonsquare, similar arguments as above give that the equations in (3.6) have 4 solutions and produce 2 different group element.
If one of \( s^2 - (2 + A) \xi \) and \( s^2 - (2 - A) \xi \) is zero, then \( s^2 \) is one of \( 2 + A \) and \( 2 - A \); and moreover it is one of \( \pi_k \) for \( 1 \leq k \leq \frac{q-1}{2} \) since \((2 + A)(2 - A) = \frac{4 - 2s^2}{s^2 - \xi} \in \mathcal{C}_q \) and \( -1 \in \square_q \). Consequently, the equations in (3.6) yield either 1 or 3 group elements in \([s^2]\).

Therefore, if \( [U_{P,N,Q}) \cap C| \) is odd, then \( C = D \) or \([\pi_k] \) for one \( k \).

**Case II.** \( \ell_2 = \ell_{P,Q} \in S_{P} \) and \( Q \notin P \).

Then \( Q = (1, 0, -y) \) for \( y \notin \mathcal{C}_q \) and \( y \neq \pm \xi \). From the proof of Case II in Lemma 3.3 we have that \( K_Q = \{d(1, 1, 1), \text{ad}(-1, 1, -1)\} \), and among the orbits of \( K_Q \) on \( Pa_P \), \( K_Q \) has only one orbit of length 1, that is, \( \ell_4 = [1, 0, y^{-1}] \); and all other orbits are of length 2 whose representatives form the set \( \mathcal{R} \). Since \( |U_{P,J_i} \cap C| = |U_{P,J_j} \cap C| \) where \( \ell_i \), \( \ell_j \in Pa_P \) and \( \ell_j = \ell_i^g \) for \( g \in K_Q \), we obtain that

\[
|U_{P,N(Q)} \cap C| = \sum_{\ell \in Pa_P} \sum_{P_1 \in I_4 \\{Q\}} |U_{P,P_1} \cap C|
= \sum_{P_1 \in I_4 \\{Q\}} |U_{P,P_1} \cap C| + 2 \sum_{\ell \in \mathcal{R}} \sum_{P_1 \in I_4 \\{Q\}} |U_{P,P_1} \cap C|. 
\] (3.9)

Moreover, since the orbits of \( K_Q \) on \( I_4 \setminus \{Q\} \), whose representatives form the set \( \mathcal{R}_1 \), are of length 2 and \( |U_{P,P_1} \cap C| = |U_{P,P_2} \cap C| \) for \( P_2 = P_1^g \), the first term of the last expression in (3.9) can be rewritten as

\[ 2 \sum_{P_1 \in \mathcal{R}_1} |U_{P,P_1} \cap C|.
\]

So \( |U_{P,N(Q)} \cap C| \) is even in this case.

**Case III.** \( P = \ell_2 \cap P \).

In this case, we have \( Q = (1, 0, \xi) \). Among the orbits of \( K_Q \) on \( Pa_P \), only one has length 1, i.e. \( P \). Moreover, all the orbits of \( K_Q \) on \( I_{P} \setminus \{Q\} \) are of length 2. Hence \( |U_{P,N(Q)} \cap C| \) is even.

The case when \( q \equiv 3 \) (mod 4) can be established in the same way and we eliminate the detail. \( \square \)

### 4. Group Algebra \( FH \)

#### 4.1. 2-Blocks of \( H \)

In this section we recall several results on the 2-blocks of \( H \cong \text{PSL}(2, q) \). We refer the reader to [14] 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

\[
S = \{ \frac{r}{s} \mid r \in R, s \in R \setminus M \}.
\] (4.1)

Then it is clear that the map \( * : S \to F \) defined by \( (\frac{r}{s})^* = r^*(s^*)^{-1} \) is a ring homomorphism with kernel \( P = \{ \frac{r}{s} \mid r \in M, s \in R \setminus M \} \). 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 \( \mathbb{F}_2 \).

As a convention, we use \( \text{Irr}(H) \) and \( \text{IBr}(H) \) to denote the set of irreducible ordinary characters and the set of irreducible Brauer characters of \( H \), respectively.

In the following, the irreducible characters of \( H \) are classified according to the character tables of \( \text{PSL}(2, q) \) displayed in Appendix.

**Lemma 4.1.** ([10], [11], [15]) The irreducible ordinary characters of \( H \) are:
\( 1 = \chi_0, \gamma, \chi_1, \ldots, \chi_{q-1}^2, \beta_1, \beta_2, \phi_1, \ldots, \phi_{q-1}^2 \) 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) \( 1 = \chi_0, \chi_1, \ldots, \chi_{q-3}^2, \beta_1, \eta_2, \eta_1, \ldots, \phi_{q-1}^2 \) 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 illustrates how the irreducible ordinary characters of \( H \) are partitioned into 2-blocks.

**Lemma 4.2.** [17] 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 \( \chi_0 = 1, \gamma, \beta_1, \beta_2, \phi_{11}, \ldots, \phi_{(2^{n-2}+1)} \), 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 irreducible characters of degree \( \frac{q+1}{2} \), and \( \phi_{ik} \) 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 \( q - 1 \).

(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 \( \phi_{it} \) for \( 1 \leq i \leq 2^{n-1} \).

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 \( \chi_0 = 1, \gamma, \eta_1, \eta_2, \chi_{11}, \ldots, \chi_{(2^{n-2}+1)} \), 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 irreducible characters of degree \( \frac{q+1}{2} \), and \( \chi_{ik} \) for \( 1 \leq k \leq 2^{n-2} - 1 \) are distinct irreducible characters of degree \( q + 1 \) of \( H \).

(v) \( H \) has \( \frac{q-3}{4} \) blocks \( B_r \) of defect 0 for \( 1 \leq r \leq \frac{q-3}{4} \), 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 \( \chi_{it} \) for \( 1 \leq i \leq 2^{n-1} \).

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

**Remark 4.3.** Parts (i) and (iv) are from Theorem 1.3 in [13] and their proofs can be found in Chapter 7 of III in [2]. Parts (ii) and (v) are special cases of Theorem 3.18 in [13]. Parts (iii) and (vi) are proved in Sections 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 \( Z(\text{CH}) \) 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 \( Z(\text{CH}) \), we may write

\[
 f_B = \sum_{\widehat{C} \in \text{ed}(H)} f_B(\widehat{C})\widehat{C},
\]
where $\text{cl}(H)$ is the set of conjugacy classes of $H$, $\hat{C}$ is the sum of elements in the class $C$, and
\[
 f_B(\hat{C}) = \frac{1}{|H|} \sum_{\chi \in \text{Irr}(B)} \chi(1) \chi(x_C^{-1})
\]
with a fixed element $x_C \in C$.

**Theorem 4.4.** Let $B \in \text{Bl}(H)$. 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 [14].

We extend the ring homomorphism $*: S \to F$ to a ring homomorphism $*: SH \to FH$ by setting $(\sum_{g \in H} s_g g)^* = \sum_{g \in H} s_g^* g$. Note that $*$ maps $\mathbb{Z}(SH)$ onto $\mathbb{Z}(FH)$ via $(\sum_{C \in \text{cl}(H)} s_C \hat{C})^* = \sum_{C \in \text{cl}(H)} s_C^* \hat{C}$. 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 $B, B' \in \text{Bl}(H)$, where $\delta_{BB'}$ equals 1 if $B = B'$, 0 otherwise. Also $1 = \sum_{B \in \text{Bl}(H)} e_B$.

All the block idempotents of the 2-blocks of $H$ are given in the following lemma; see [17] for the detailed calculations.

**Lemma 4.5.** [17] 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) $e_{B_0}(\hat{D}) = 1$; (b) $e_{B_0}(\hat{F}^+) = e_{B_0}(\hat{F}^-) \in F$; (c) $e_{B_0}(\hat{t}_1) \notin F$, $e_{B_0}(\hat{0}) = 0$; (d) $e_{B_0}(\hat{\pi}_k) = 1$.

2. Let $B_\delta$ be any block of defect 0 of $H$. Then (a) $e_{B_\delta}(\hat{D}) = 0$; (b) $e_{B_\delta}(\hat{F}^+) = e_{B_\delta}(\hat{F}^-) = 1$; (c) $e_{B_\delta}(\hat{0}) = e_{B_\delta}(\hat{\theta}_1) = 0$; (d) $e_{B_\delta}(\hat{\pi}_k) \in F$.

3. Suppose $m \geq 3$ and let $B'_t$ be any block of defect $n - 1$ of $H$. Then (a) $e_{B'_t}(\hat{D}) = 0$; (b) $e_{B'_t}(\hat{F}^+) = e_{B'_t}(\hat{F}^-) = 1$; (c) $e_{B'_t}(\hat{\theta}_1) \in F$, $e_{B'_t}(\hat{0}) = 0$; (d) $e_{B'_t}(\hat{\pi}_k) = 0$.

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) $e_{B_0}(\hat{D}) = 1$; (b) $e_{B_0}(\hat{F}^+) = e_{B_0}(\hat{F}^-) \in F$; (c) $e_{B_0}(\hat{\theta}_1) = 1$; (d) $e_{B_0}(\hat{0}) = 0$, $e_{B_0}(\hat{\pi}_k) \in F$.

5. Let $B_r$ be any block of defect 0 of $H$. Then (a) $e_{B_r}(\hat{D}) = 0$; (b) $e_{B_r}(\hat{F}^+) = e_{B_r}(\hat{F}^-) = 1$; (c) $e_{B_r}(\hat{0}) = e_{B_r}(\hat{\pi}_k) = 0$; (d) $e_{B_r}(\hat{\theta}_1) \in F$.

6. Suppose that $m \geq 3$ and let $B'_t$ be any block of defect $n - 1$ of $H$. Then (a) $e_{B'_t}(\hat{D}) = 0$; (b) $e_{B'_t}(\hat{F}^+) = e_{B'_t}(\hat{F}^-) = 1$; (c) $e_{B'_t}(\hat{\theta}_1) = 0$; (d) $e_{B'_t}(\hat{0}) = 0$, $e_{B'_t}(\hat{\pi}_k) \in F$.

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

**Lemma 4.6.** Let $M$ be an $SH$-module and $B \in \text{Bl}(H)$. Using the above notation, we have
\[
\overline{M} \cdot f_B = \overline{M} \cdot e_B,
\]
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 Section 4. Recall that for $P \in I$, $N(P)$ is the set of external points on the passant lines through $P$ with $P$ included or excluded accordingly as $q \equiv 3 \pmod{4}$ or $q \equiv 1 \pmod{4}$. We define $D$ to be the incidence matrix of $N(P)$ ($P \in I$) and $I$. Correspondingly, the rows of $D$ can be viewed as the characteristic vectors of $N(P)$. In the following, we always regard both $D$ and $A$ as matrices over $F$. Moreover, it is clear that $D = A^2 + I$, where $I$ is the identity matrix of proper size.

Definition 5.1. For $W \subseteq I$, we define $C_W$ to be the row characteristic vector of $W$ with respect to $I$, i.e. $C_W$ is a 0-1 row vector of length $|I|$ with entries indexed by the internal points and the entry of $C_W$ is 1 if and only if the point indexing the entry is in $W$. If $W = \{P\}$, as a convention, we write $C_W$ as $C_P$.

Let $k$ be the complex field $\mathbb{C}$, the algebraic closure $F$ of $\mathbb{F}_2$, or the ring $S$ in (4.1). Let $k^I$ be the free $k$-module with the base $\{C_P | P \in I\}$, respectively. If we extend the action of $H$ on the basis elements of $k^I$, which is defined by $C_Q \cdot h = C_{Qh}$ for $P \in I$ and $h \in H$, linearly to $k^I$, then $k^I$ is a $kH$-permutation modules. Since $H$ is transitive on $I$, we have

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

where $K$ is the stabilizer of an internal point in $H$ and $\text{Ind}^H_K(1_k)$ is the $kH$-module induced from $1_k$.

The decomposition of $1 \uparrow^H_K$, the character of $\text{Ind}^H_K(1_k)$, into a sum of the irreducible ordinary characters of $H$ is given as follows.

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 characters of degree $q-1$, $\phi_r$, $1 \leq r \leq \frac{q-5}{4}$, irreducible characters of degree $q+1$, $\gamma$ the irreducible character of degree $q$, and $\beta_j$, $1 \leq j \leq 2$, irreducible characters of degree $\frac{q+1}{2}$.

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

$$1_K \uparrow^H_K = 1_H + \sum_{s=1}^{(q-1)/4} \chi_s + \gamma + \beta_1 + \beta_2 + \sum_{j=1}^{(q-9)/4} \phi_{r_j},$$

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

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

$$1_K \uparrow^H_K = 1_H + \sum_{s=1}^{(q-1)/4} \chi_s + \gamma + \sum_{j=1}^{(q-5)/4} \phi_{r_j},$$

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 characters of degree $q-1$, $\phi_r$, $1 \leq r \leq \frac{q-3}{4}$, the irreducible characters of degree $q+1$, $\gamma$ the irreducible character of degree $q$, and $\eta_j$, $1 \leq j \leq 2$, the irreducible characters of degree $\frac{q+1}{2}$.

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

$$1_K \uparrow^H_K = 1_H + \sum_{r=1}^{(q-3)/4} \phi_r + \eta_1 + \eta_2 + \sum_{j=1}^{(q-3)/4} \chi_{s_j},$$

where $\chi_{s_j}$, $1 \leq j \leq \frac{q-3}{4}$, may not be distinct.
(iv) If \( q \equiv 7 \pmod{8} \), then
\[
1_K \uparrow_K^H = 1_H + \sum_{r=1}^{(q-3)/4} \phi_r + \sum_{j=1}^{(q+1)/4} \chi_{s_j},
\]
where \( \chi_{s_j}, 1 \leq j \leq \frac{q+1}{4} \), may not be distinct.

**Proof:** We provide the proof for the case when \( q \equiv 1 \pmod{4} \).
Let \( 1_H \) be the trivial character of \( H \). By the Frobenius reciprocity [5],
\[
\langle 1_K \uparrow_K^H, 1_H \rangle_H = \langle 1_K, 1_H \downarrow_K^H \rangle_K = 1.
\]

Let \( \chi_s \) be an irreducible character of degree \( q-1 \) of \( H \), where \( 1 \leq s \leq \frac{q-1}{2} \). We denote the number of elements of \( K \) lying in the class \([\pi_k] \) by \( d_k \). Then \( d_k = 2 \) by Lemma 3.3(iii), and so
\[
\langle 1_K \uparrow_K^H, \chi_s \rangle_H = \langle 1_K, \chi_s \downarrow_K^H \rangle_K = \frac{1}{|K|} \sum_{g \in K} \chi_s \downarrow_K^H (g)
\]
\[
= \frac{1}{q+1} [(1)(q-1) + 2 \sum_{k=1}^{(q-1)/4} (-\delta^{(2k)s} - \delta^{-(2k)s})] = 1,
\]
where
\[
\sum_{k=1}^{(q-1)/4} (-\delta^{(2k)s} - \delta^{-(2k)s}) = -(1 + \delta^{2s} + (\delta^{2s})^2 + \cdots + (\delta^{2s})^{(q-1)/2 - 1})
\]
\[
= \frac{1-\delta^{(q+1)s}}{1-\delta^{2s}} + 1
\]
since \( \delta^{q+1} = 1 \).

Let \( \gamma \) be the irreducible character of degree \( q \) of \( H \). Then
\[
\langle 1_K \uparrow_K^H, \gamma \rangle_H = \langle 1_K, \gamma \downarrow_K^H \rangle_K = \frac{1}{|K|} \sum_{g \in K} \gamma \downarrow_K^H (g)
\]
\[
= \frac{1}{q+1} [(1)(q) + (2)(-1)(\frac{q-1}{2}) + (1)(\frac{q+1}{2})] = 1.
\]

Let \( \beta_j \) be any irreducible character of degree \( \frac{q+1}{2} \) of \( H \). Then
\[
\langle 1_K \uparrow_K^H, \beta_j \rangle_H = \frac{1}{|K|} \sum_{g \in K} \beta_j \downarrow_K^H (g)
\]
\[
= \frac{1}{q+1} [(1)(\frac{q+1}{2}) + (2)(\frac{q-1}{2})(0) + (1)(\frac{q+1}{2})(-1)(q-1)/4] = 0.
\]

Consequently, if \( q \equiv 1 \pmod{8} \), then \( (-1)^{\frac{q+1}{4}} = 1 \), and so \( \langle 1_K \uparrow_K^H, \beta_j \rangle_H = 1 \); otherwise, \( (-1)^{\frac{q+1}{4}} = -1 \), and so \( \langle 1_K \uparrow_K^H, \beta_j \rangle_H = 0 \).

Since the sum of the degrees of \( 1, \chi_s, \gamma, \) and \( \beta_j \) is less than the degree of \( 1 \uparrow_K^H \) and only the irreducible characters of degree \( q+1 \) of \( H \) have not been taken into account yet, we see that all the irreducible constituents of
\[
1_K \uparrow_K^H - 1_H - \sum_{s=1}^{(q-1)/4} \chi_s - \gamma - \beta_1 - \beta_2 \text{ or } 1_K \uparrow_K^H - 1_H - \sum_{s=1}^{(q-1)/4} \chi_s - \gamma
\]
must have degree \( q+1 \).
\[
\Box
\]
Corollary 5.3. Using the above notation,

(i) if $q \equiv 1 \pmod{4}$, then the character of $\text{Ind}^H_K(1_C) \cdot f_{B_s}$ is $\chi_s$ for each block $B_s$ of defect 0;
(ii) if $q \equiv 3 \pmod{4}$, then the character of $\text{Ind}^H_K(1_C) \cdot f_{B_r}$ 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, it is obvious that, for $P \in I$ and $h \in H$, 

$\mathcal{C}_{N(P)} \cdot h = \mathcal{C}_{N(P^h)}$.

In the rest of the article, we always view $\mathcal{C}_P$ as a vector over $F$. Consider the maps $\phi$ and $\mu$ from $F^I$ to $F^I$ defined by extending

$\mathcal{C}_P \mapsto \mathcal{C}_P \perp, \mathcal{C}_P \mapsto \mathcal{C}_{N(P)}$

linearly to $F^I$, respectively. Then it is clear that as $F$-linear maps, the matrices of $\phi$ and $\mu$, are $A$ and $D$, respectively, and for $x \in F^I$, $\phi(x) = xA$ and $\mu(x) = xD$. Moreover, we have the following result since $H$ is transitive on $I$ and preserves incidence:

Lemma 5.4. The maps $\phi$ and $\mu$ are both $FH$-module homomorphisms from $F^I$ to $F^I$.

We will always use $0$ and $\hat{0}$ to denote the all-zero row vector of length $|I|$ and the all-zero matrix of size $|I| \times |I|$, respectively; and we denote by $\hat{J}$ and $J$ the all-one row vector of length $|I|$ and the all-one matrix of size $|I| \times |I|$.

Proposition 5.5. As $FH$-modules, $F^I = \text{Im}(\phi) \oplus \text{Ker}(\phi)$, where $\text{Im}(\phi)$ and $\text{Ker}(\phi)$ are the image and kernel of $\phi$, respectively.

Proof: It is clear that $\text{Ker}(\phi) \subseteq \text{Ker}(\phi^2)$. If $x \in \text{Ker}(\phi^2)$, then $x \in \text{Ker}(\phi)$ since

$\phi(x) = \phi^3(x) = \phi(\phi^2(x)) = 0$.

Therefore, $\text{Ker}(\phi^2) = \text{Ker}(\phi)$. Furthermore, since $\text{Ker}(\phi) \subseteq \text{Ker}(\phi^2) \subseteq \text{Ker}(\phi^3) \subseteq \cdots$, we have $\text{Ker}(\phi^i) = \text{Ker}(\phi)$ for $i \geq 2$. Applying the Fitting decomposition theorem [12, p. 285] to the operator $\phi$, we can find an $i$ such that $F^E = \text{Ker}(\phi^i) \oplus \text{Im}(\phi^i)$. From the above discussions, we must have $F^E = \text{Ker}(\phi) \oplus \text{Im}(\phi)$. □

Corollary 5.6. As $FH$-modules, $\text{Ind}^H_K(1_F) \cong \text{Ker}(\phi) \oplus \text{Im}(\phi)$.

Proof: The conclusion follows immediately from Proposition 5.5 and the fact that $\text{Ind}^H_K(1_F) \cong F^E$. □

Using the above notation, we set $C = D + J$, where $J$ is the all-one matrix of proper size. Then the matrix $C$ can be viewed as the incidence matrix of $N(P)$ ($P \in I$) and $I$, and so $C_P \subseteq C_{N(P)}$.

Let $\mu_2$ be the $FH$-homomorphism from $F^I$ to $F^I$ whose matrix with respect to the natural basis is $C$. The following proposition is clear.

Proposition 5.7. Using the above notation, we have $\text{Ker}(\phi) = \langle J \rangle \oplus \text{Im}(\mu_2)$, where $\langle J \rangle$ is the trivial $FH$-module generated by $J$.

Lemma 5.8. Assume that $q \equiv 3 \pmod{4}$. Then as $FH$-modules, we have $\text{Ker}(\phi) = \langle \hat{J} \rangle \oplus \text{Im}(\mu_2)$, where $\langle \hat{J} \rangle$ is the trivial $FH$-module generated by $\hat{J}$. 
Proof: Let \( y \in \langle \hat{J} \rangle \cap \text{Im}(\mu_2) \). Then \( y = \mu_2(x) = \lambda \hat{J} \) for some \( \lambda \in F \) and \( x \in F^I \). Or equivalently, we have \( \mu_2(x) = xC = x(A^2 + I + J) = \lambda \hat{J} \). Note that \( J^2 = J \) and \( J \hat{J} = \hat{J} \) since \( 2 \nmid |I| \) when \( q \equiv 3 \pmod{4} \). Moreover, \( A^2J = 0 \) as each row of \( A^2 \), viewed as the characteristic vector of \( N(P) \), has an even number of 1s. Consequently,

\[
\lambda \hat{J} = \lambda JJ = x(A^2 + I + J)J = x(A^2J + IJ + J^2) = x(\hat{0} + J + J) = 0.
\]

It follows that \( \lambda = 0 \). Therefore, we must have \( \langle \hat{J} \rangle \cap \text{Im}(\mu_2) = 0 \).

It is obvious that \( \langle \hat{J} \rangle + \text{Im}(\mu_2) \subseteq \text{Ker}(\phi) \). Let \( x \in \text{Ker}(\phi) \). Then \( x = y(A^2 + I) \) for some \( y \in F^I \). Since \( yJ = \langle y, \hat{J} \rangle \hat{J} \), we obtain that \( x = y(A^2 + I + J) + \langle y, \hat{J} \rangle \hat{J} \), where \( \langle y, \hat{J} \rangle \) is the standard inner product of the vectors \( y \) and \( \hat{J} \). Hence \( x \in \langle \hat{J} \rangle + \text{Im}(\mu_2) \) and so \( \text{Ker}(\phi) = \langle \hat{J} \rangle \oplus \text{Im}(\mu_2) \).

\[
\square
\]

6. Statement and Proof of Main Theorem

The main theorem is stated as follows.

Theorem 6.1. Let \( \text{Ker}(\phi) \) be defined as above. As \( FH \)-modules,

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

\[
\text{Ker}(\phi) = \bigoplus_{s=1}^{(q-1)/4} M_s,
\]

where \( M_s \) for \( 1 \leq s \leq \frac{q-1}{4} \) are pairwise non-isomorphic simple \( FH \)-modules of dimension \( q - 1 \);

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

\[
\text{Ker}(\phi) = \langle \hat{J} \rangle \oplus \bigoplus_{r=1}^{(q-3)/4} M_r,
\]

where \( M_r \) for \( 1 \leq s \leq \frac{q-3}{4} \) are pairwise non-isomorphic simple \( FH \)-modules of dimension \( q + 1 \) and \( \langle \hat{J} \rangle \) is the trivial \( FH \)-module generated by the all-one column vector of length \(|I|\).

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

Lemma 6.2. Let \( q - 1 = 2^nm \) or \( q + 1 = 2^nm \) with \( 2 \nmid m \) accordingly as \( q \equiv 1 \pmod{4} \) or \( q \equiv 3 \pmod{4} \). Using the above notation,

(i) if \( q \equiv 1 \pmod{4} \), then \( \text{Ker}(\phi) \cdot e_{B_s} = 0 \), \( \text{Im}(\phi) \cdot e_{B_s} = 0 \) for \( 1 \leq s \leq \frac{q-1}{4} \), and \( \text{Ker}(\phi) \cdot e_{B'_1} = 0 \) for \( m \geq 3 \) and \( 1 \leq t \leq \frac{m-1}{2} \);

(ii) if \( q \equiv 3 \pmod{4} \), then \( \text{Im}(\mu_2) \cdot e_{B_0} = 0 \), \( \text{Im}(\phi) \cdot e_{B_r} = 0 \) for \( 1 \leq r \leq \frac{q-3}{4} \), and \( \text{Im}(\mu_2) \cdot e_{B'_1} = 0 \) for \( m \geq 3 \) and \( 1 \leq t \leq \frac{m-1}{2} \).

Proof: It is clear that \( \text{Im}(\phi), \text{Ker}(\phi), \) and \( \text{Im}(\mu_2) \) are generated by

\[
\{ C_P \mid P \in I \}, \quad \{ C_{N(P)} \mid P \in I \}, \quad \text{and} \quad \{ C_{N(P)} \mid P \in I \}
\]
over $F$, respectively. Now let $B \in Bl(H)$. Since 

$$C_{p^\perp} \cdot e_B = \sum_{C \in d(H)} e_B(\hat{C}) \sum_{h \in C} C_{p^\perp} \cdot h$$

$$= \sum_{C \in d(H)} e_B(\hat{C}) \sum_{h \in C} C_{(p^\perp)h},$$

$$= \sum_{C \in d(H)} e_B(\hat{C}) \sum_{h \in C} Q \in (p^\perp)h \cap I \sum C_q,$$

we have

$$C_{p^\perp} \cdot e_B = \sum_{Q \in I} S_1(B, P, Q)C_q,$$

where

$$S_1(B, P, Q) := \sum_{C \in d(H)} |H_{p,q} \cap C| e_B(\hat{C}).$$

Similarly $C_{N(p)} \cdot e_B = \sum_{Q \in I} S_2(B, P, Q)C_q$ and $C_{N(p)} \cdot e_B = \sum_{Q \in I} S_3(B, P, Q)C_q$, where

$$S_2(B, P, Q) = \sum_{C \in Cl(H)} |U_{P,N(q)} \cap C| e_B(\hat{C})$$

and

$$S_3(B, P, Q) = \sum_{C \in Cl(H)} |U_{P,N(q)} \cap C| e_B(\hat{C}).$$

Assume first that $q \equiv 1 \pmod{4}$. If $\ell_{p,q} \in Pa_p$, then $S_1(B_s, P, Q) = 0$ for each $s$ since $|H_{p,q} \cap C| = 0$ in $F$ for each $C \neq [0]$ by Lemma 3.6(i) and $e_B([0]) = 0$ by Lemmas 4.5 2(c); and by Lemma 3.6(i) and Lemma 4.5 1(a), 1(c), 1(d), 3(a), 3(c), 3(d), we obtain

$$S_2(B_0, P, Q) = e_{B_0}([0]) + e_{B_0}([\overline{\pi_k}]) + e_{B_0}([\hat{D}]) = 0 + 1 + 1 = 0$$

and

$$S_2(B'_s, P, Q) = e_{B'_s}([0]) + e_{B'_s}([\overline{\pi_k}]) + e_{B'_s}([\hat{D}]) = 0 + 0 + 0 = 0.$$

If $\ell_{p,q} \in Se_p$ and $Q \notin P^\perp$, then by Lemma 3.5(ii) and Lemma 4.5 2(c) we obtain

$$S_1(B_s, P, Q) = e_{B_s}([0]) + e_{B_s}([\overline{\theta_i}]) + e_{B_s}([\hat{\theta}_i]) = 0 + 0 + 0 = 0;$$

and by Lemma 4.5 1(c), 3(c), and Lemma 3.6(ii), $S_2(B_0, P, Q) = e_{B_0}([0]) = 0$ and $S_2(B'_s, P, Q) = e_{B'_s}([0]) = 0$.

If $\ell_{p,q} \in Se_p$ and $Q \notin P^\perp$, then by Lemma 3.5(iii) and Lemma 4.5 2(a) and 2(c) we obtain $S_1(B_s, P, Q) = e_{B_s}([0]) + e_{B_s}([\hat{D}]) = 0 + 0 = 0$; and from Lemma 3.6(ii) and Lemma 4.5 1(c) and 3(c), it follows that $S_2(B_0, P, Q) = e_{B_0}([0]) = 0$ and $S_2(B'_s, P, Q) = e_{B'_s}([0]) = 0$.

Next we assume that $q \equiv 3 \pmod{4}$. If $\ell_{p,q} \in Pa_p$ and $Q \notin P^\perp$, then by Lemma 3.5(v) and Lemma 4.5 5(c), we have

$$S_1(B_s, P, Q) = e_{B_s}([0]) + e_{B_s}([\overline{\pi_k}]) + e_{B_s}([\hat{\pi_k}]) = 0 + 0 + 0 = 0;$$

and by Lemma 3.6(iii) and Lemma 4.5 4(d) and 6(d), we obtain $S_3(B_0, P, Q) = e_{B_0}([0]) = 0$ and $S_3(B'_s, P, Q) = e_{B'_s}([0]) = 0$. 

If \( Q = \ell_{P,Q} \cap P^\perp \), then by Lemmas 3.6(iii) and 3.5(iii), and 4(d), 5(a), 5(c), 6(d) of Lemma 4.5, \( S_3(B_0, P, Q) = e_{B_0}([0]) = 0 \), \( S_1(B_r, P, Q) = e_{B_r}([\theta_i]) = 0 + 0 = 0 \), and \( S_3(B'_t, P, Q) = e_{B'_t}([0]) = 0 \).

If \( \ell_{P,Q} \in \mathcal{S}_{BP} \), then by Lemmas 3.6(iv) and 3.5(iv), and 4(a), 4(c), 4(d), 5(c), 6(a), 6(c), 6(d) of Lemma 4.5, \( S_3(B_0, P, Q) = e_{B_0}([\theta_i]) = 0 + 1 + 1 = 0 \), \( S_1(B_r, P, Q) = e_{B_r}([\theta_i]) = 0 \), and \( S_3(B'_t, P, Q) = e_{B'_t}([\theta_i]) = 0 + 0 + 0 = 0 \).

□

**Proof of Theorem 6.1:** Let \( B \) be a 2-block of defect 0 of \( H \). Then by Lemma 4.6, we have
\[
F^I \cdot e_B = \mathcal{S}^I \cdot f_B.
\]
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 \( q \equiv 1 \) (mod 4) or \( q \equiv 3 \) (mod 4).

Assume that \( q \equiv 1 \) (mod 4) and \( q - 1 = m2^n \) with \( 2 \nmid m \). Since
\[
1 = e_{B_0} + \sum_{s=1}^{(q-1)/4} e_{B_s} + \sum_{t=1}^{(m-1)/2} e_{B'_t},
\]
\( \text{Ker}(\phi) \cdot e_{B_0} = 0 \) and \( \text{Ker}(\phi) \cdot e_{B'_t} = 0 \), then
\[
\text{Ker}(\phi) = \bigoplus_{B \in \mathcal{B}(H)} \text{Ker}(\phi) \cdot e_B = \bigoplus_{s=1}^{(q-1)/4} \text{Ker}(\phi) \cdot e_{B_s} = \bigoplus_{s=1}^{(q-1)/4} N_s,
\]
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.

Now assume that \( q \equiv 3 \) (mod 4). Lemma 5.8 yields \( \text{Ker}(\phi) = \langle J \rangle \oplus \text{Im}(\mu_2) \). Since \( \text{Im}(\mu_2) \cdot e_{B_0} = 0 \) and \( \text{Im}(\mu_2) \cdot e_{B'_t} = 0 \), applying the same argument as above, we have
\[
\text{Im}(\mu_2) = \bigoplus_{r=1}^{(q-3)/4} M_r,
\]
where each \( M_r \) is a simple \( FH \)-module of dimension \( q + 1 \). Consequently,
\[
\text{Ker}(\phi) = \langle J \rangle \oplus ( \bigoplus_{r=1}^{(q-3)/4} M_r ) .
\]

□

Now Conjecture 1.1 follows as a corollary.

**Corollary 6.3.** Let \( \mathcal{L} \) be the \( \mathbb{F}_2 \)-null space of \( A \). Then
\[
\dim_{\mathbb{F}_2}(\mathcal{L}) = \frac{(q - 1)^2}{4}.
\]
Proof: By Theorem 6.1 and the fact that $\dim F_2(\mathcal{L}) = \dim F_2(\ker(\phi))$, when $q \equiv 1 \pmod{4}$, we have

$$\dim F_2(\mathcal{L}) = \sum_{i=1}^{(q-1)/4} (q - 1),$$

and when $q \equiv 3 \pmod{4}$, we have

$$\dim F_2(\mathcal{L}) = 1 + \sum_{i=1}^{(q-3)/4} (q + 1),$$

both of which are equal to $\frac{(q-1)^2}{4}$.

□
APPENDIX

The character tables of PSL(2, q) were obtained by Jordan [10] and Schur [15] independently, from which we can deduce the character tables of \( H \) as follows. Let \( \epsilon \in \mathbb{C} \) be a primitive \((q - 1)\)-th root of unity and \( \delta \in \mathbb{C} \) a primitive \((q + 1)\)-th root of unity.

Table 3. Character table of \( H \) when \( q \equiv 1 \) (mod 4)

| Number | 1 | \( \frac{q-1}{2} \) | \( q(q+1) \) | \( \frac{q+1}{2} \) | \( q(q-1) \) |
|--------|---|----------------|--------------|----------------|--------------|
| Size   | 1 | \( \frac{q-1}{2} \) | \( q(q+1) \) | \( \frac{q+1}{2} \) | \( q(q-1) \) |
| \( D \) | \( \theta_i \) | \( [0] \) | \( [\pi_k] \) | \( [\pi_k] \) | \( [\theta_i] \) |
| \( \phi_r \) | \( q+1 \) | 1 | \( \epsilon^{(2i)r} + \epsilon^{-(2i)r} \) | 0 | 0 |
| \( \gamma \) | \( q \) | 0 | 1 | 1 | -1 |
| \( 1 \) | 1 | 1 | 1 | 1 | 1 |
| \( \chi_s \) | \( q-1 \) | -1 | 0 | 0 | -\( \delta^{(2k)s} - \delta^{-(2k)s} \) |
| \( \beta_1 \) | \( \frac{q+1}{2} \) | \( \frac{1}{2}(1 + \sqrt{q}) \) | \( \zeta(\theta_i) \) | (\( -1 \))^{(q-1)/4} | 0 |
| \( \beta_2 \) | \( \frac{q+1}{2} \) | \( \frac{1}{2}(1 - \sqrt{q}) \) | \( \zeta(\theta_i) \) | (\( -1 \))^{(q-1)/4} | 0 |

Here \( s = 1, 2, \ldots, \frac{q-1}{4}, \; r = 1, 2, \ldots, \frac{q-5}{4}, \; k = 1, 2, \ldots, \frac{q-1}{4}, \; i = 1, 2, \ldots, \frac{q-5}{4}, \) and \( \zeta(\theta_i) = 1 \) or -1.

Table 4. Character table of \( H \) when \( q \equiv 3 \) (mod 4)

| Number | 1 | \( \frac{q-3}{4} \) | \( q(q+1) \) | \( \frac{q-1}{2} \) | \( q(q-1) \) |
|--------|---|----------------|--------------|----------------|--------------|
| Size   | 1 | \( \frac{q-3}{4} \) | \( q(q+1) \) | \( \frac{q+1}{2} \) | \( q(q-1) \) |
| \( D \) | \( \theta_i \) | \( [0] \) | \( [\pi_k] \) | \( [\pi_k] \) | \( [\theta_i] \) |
| \( \phi_r \) | \( q+1 \) | 1 | \( \epsilon^{(2i)r} + \epsilon^{-(2i)r} \) | 0 | 0 |
| \( \gamma \) | \( q \) | 0 | 1 | -1 | -1 |
| \( 1 \) | 1 | 1 | 1 | 1 | 1 |
| \( \chi_s \) | \( q-1 \) | -1 | 0 | -2(\( -1 \))^s | -\( \delta^{(2k)s} - \delta^{-(2k)s} \) |
| \( \eta_1 \) | \( \frac{q-3}{2} \) | \( \frac{1}{2}(-1 + \sqrt{-q}) \) | 0 | (\( -1 \))^{(q+5)/4} | -\( \zeta(\pi_k) \) |
| \( \eta_2 \) | \( \frac{q-3}{2} \) | \( \frac{1}{2}(-1 - \sqrt{-q}) \) | 0 | (\( -1 \))^{(q+5)/4} | -\( \zeta(\pi_k) \) |

Here \( s = 1, 2, \ldots, \frac{q-3}{4}, \; r = 1, 2, \ldots, \frac{q-3}{4}, \; k = 1, 2, \ldots, \frac{q-3}{4}, \; i = 1, 2, \ldots, \frac{q-3}{4}, \) and \( \zeta(\pi_k) = 1 \) or -1.

REFERENCES

[1] E. F. Assmus Jr. and D. Key, Designs and Their Codes, Cambridge University Press, New York, 1992.
[2] R. Brauer, Some applications of the theory of blocks of characters of finite groups. I, II, III, and IV, J. Algebra 1 (1964), 152–167, 304–334; 3 (1966), 225–255; 17 (1971), 489–521.
[3] R. Burkhardt, Die zerlegungsmatrizen der gruppen PSL(2, p^\ell), J. Algebra 40 (1976), 75–96.
[4] S. Droms, K. E. Mellinger, and C. Meyer, LDPC codes generated by conics in the classical projective plane, Des. Codes Cryptogr. 40 (2006), 343–356.
[5] G. Frobenius, Über relationen zwischen den charakteren einer gruppe und denen ihrer untergruppen, S‘ber. Akad. Wiss. Berlin (1898), 501–515; Ges. Abh. III, 104–118.
[6] R. H. Dye, Hexagons, Conics, A3 and PSL3(K), J. Lond. Math. Soc. (2) 44 (1991), 270–286.
[7] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, Second Edition, Oxford University Press, Oxford, 1998.
[8] D. R. Hughes and F. C. Piper, *Projective Planes*, Graduate Texts in Mathematics 6, Springer-Verlag, New York Inc.

[9] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1976.

[10] H. E. Jordan, Group-characters of various types of linear groups, *Amer. J. Math.* 29 (1907), 387–405.

[11] G. Karpilovsky, *Group Representations, Volume 3*, North-Holland, Amsterdam, 1993.

[12] T.-Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics 131, Springer-Verlag, New York Inc.

[13] P. Landrock, The principal block of finite groups with dihedral Sylow 2-subgroups *J. Algebra* 39 (1976), 410–428.

[14] G. Navarro, *Characters and Blocks of Finite Groups*, London Mathematical Society Lecture Note Series 250, Cambridge University Press, Cambridge, 1998.

[15] I. Schur, Untersuchungen über die darstellung der endlichen gruppen durch gebrochene lineare substitutionen, *J. Reine Angew. Math.* 132 (1907), 85–137.

[16] B. Segre, Ovals in a finite projective plane, *Canad. J. Math.* 7 (1955), 414–416.

[17] P. Sin, J. Wu, and Q. Xiang, Dimensions of some binary codes arising from a conic in $PG(2, q)$, *J. Combin. Theory (A)* 118 (2011), 853–878.

[18] T. Store, *Cyclotomy and Difference Sets*, Markham, Chicago, 1967.

[19] J. Wu, Proofs of two conjectures on the dimensions of binary codes, submitted.

**Department of Mathematics, Lane College, Jackson, TN, USA**

*E-mail address: jwu@lanecollege.edu*

**Lane College, Jackson, TN, USA**

*E-mail address: adonus_madison@lanecollege.edu*