European Journal of Combinatorics 33 (2012) 33–48

Contents lists available at SciVerse ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

On binary codes from conics in PG$(2, q)$

Adonus L. Madison, Junhua Wu

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

ARTICLE INFO

Article history:
Received 4 April 2011
Received in revised form
1 August 2011
Accepted 1 August 2011
Available online 17 September 2011

ABSTRACT

Let **A** be the $\frac{q(q-1)}{2} \times \frac{q(q-1)}{2}$ 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 $\mathcal{L}$ of **A**. In particular, using methods from both finite geometry and modular presentation theory, we manage to compute the dimension of $\mathcal{L}$, which provides a proof for the conjecture on the dimension of the binary code generated by $\mathcal{L}$.

1. Introduction

Let PG$(2, q)$ be the classical projective plane of order q with underlying three-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

$$\mathcal{O} := \{(1, r, r^2) \mid r \in \mathbb{F}_q\} \cup \{(0, 0, 1)\} \tag{1.1}$$

is a *conic* in PG$(2, q)$ [4]. The above set also comprises the projective solutions of the non-degenerate quadratic equation

$$Q(X_0, X_1, X_2) = X_1^2 - X_0X_2 \tag{1.2}$$

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 ($\mathcal{O}$), and external points (E) accordingly as the numbers of tangent lines on which they lie are 0, 1, or 2.

In [1], one low-density parity-check binary code was constructed using the column $\mathbb{F}_2$-null space $\mathcal{L}$ of the incidence matrix **A** of passant lines and internal points with respect to $\mathcal{O}$. It is apparent that **A**

E-mail addresses: adonus_madison@lanecollege.edu (A.L. Madison), jwu@lanecollege.edu (J. Wu).

0195-6698/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2011.08.001

is a $\frac{q(q-1)}{2} \times \frac{q(q-1)}{2}$ square matrix. With the help of the computer software Magma, the authors made a conjecture on the dimension of $\mathcal{L}$ as follows:

Conjecture 1.1 (*[1, Conjecture 4.7]*). *Let $\mathcal{L}$ be the $\mathbb{F}_2$-null space of* **A**, *and let* $\dim_{\mathbb{F}_2}(\mathcal{L})$ *be the dimension of $\mathcal{L}$. Then*

$$\dim_{\mathbb{F}_2}(\mathcal{L}) = \frac{(q-1)^2}{4}.$$

The purpose of this article is to confirm Conjecture 1.1. Apart from the above conjecture, the dimensions of the column $\mathbb{F}_2$-null spaces of the incidence matrices of external points versus secant lines, external points versus passant lines, and passant lines versus external points were conjectured in the aforementioned paper [1], and have been established in [8,9], respectively. Here we point out that this paper refers to [8] for prerequisites and setting.

To start, we recall that the automorphism group G of $\mathcal{O}$ is isomorphic to $\mathrm{PGL}(2, q)$, and that the normal subgroup H of G isisomorphic to $\mathrm{PSL}(2, q)$. Let F be an algebraic closure of $\mathbb{F}_2$. Our idea of proving Conjecture 1.1 is to first realize $\mathcal{L}$ as an FH-module and then decompose it into a direct sum of its certain submodules whose dimensions are well known. More precisely speaking, we view **A** as the matrix of the following homomorphism ϕ 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. Moreover, it can be shown that ϕ is indeed an FH-module homomorphism. Consequently, computing the dimension of the column $\mathbb{F}_2$-null space of **A** amounts to finding the F-null space of ϕ. 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** satisfies the relation $\mathbf{A}^3 \equiv \mathbf{A} \pmod 2$ under certain orderings of its rows and columns; this relation, in turn, reveals a geometric description of $\mathrm{Ker}(\phi)$ as well as yielding a set of generating elements of $\mathrm{Ker}(\phi)$ 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. Combining the results in Section 3 with Brauer's theory on blocks, we are able to decompose $\mathrm{Ker}(\phi)$ 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

We refer the reader to [5,4] for basic results related to the geometry of conics in $\mathrm{PG}(2, q)$ with q odd. For convenience, we will denote the set of all non-zero squares of $\mathbb{F}_q$ by $\square_q$, and the set of non-squares by $\not\square_q$; also, $\mathbb{F}_q^*$ is the set of non-zero elements of $\mathbb{F}_q$. It is well known [4, p. 181] that the non-degenerate quadratic form $Q(X_0, X_1, X_2) = X_1^2 - X_0X_2$ induces a polarity σ (or $\perp$) of $\mathrm{PG}(2, q)$.

Lemma 2.1 (*[4, p. 181–182]*). *Assume that q is odd.*

(i) *The polarity σ above defines three bijections; that is, $\sigma : I \to Pa$, $\sigma : E \to Se$, and $\sigma : \mathcal{O} \to T$ are all bijections.*
(ii) *A line $[b_0, b_1, b_2]$ of $\mathrm{PG}(2, q)$ is a passant, a tangent, or a secant to $\mathcal{O}$ if and only if $b_1^2 - 4b_0b_2 \in \not\square_q$, $b_1^2 - 4b_0b_2 = 0$, or $b_1^2 - 4b_0b_2 \in \square_q$, respectively.*
(iii) *A point (a_0, a_1, a_2) of $\mathrm{PG}(2, q)$ is internal, absolute, or external if and only if $a_1^2 - a_0a_2 \in \not\square_q$, $a_1^2 - a_0a_2 = 0$, or $a_1^2 - a_0a_2 \in \square_q$, respectively.*

Let G be the automorphism group of $\mathcal{O}$ in $\mathrm{PGL}(3, q)$ (i.e. the subgroup of $\mathrm{PGL}(3, q)$ fixing $\mathcal{O}$ setwise).

Lemma 2.2 (*[4, p. 158]*). $G \cong \mathrm{PGL}(2, q)$.

We define

$$H := \left\{ \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad+bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix} \middle| a, b, c, d \in \mathbb{F}_q, ad-bc=1 \right\}. \tag{2.1}$$

In the rest of the article, we always use ξ to denote a fixed primitive element of $\mathbb{F}_q$. For $a, b, c \in \mathbb{F}_q$, we define

$$\mathbf{d}(a,b,c) := \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}, \quad \mathbf{ad}(a,b,c) := \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix}.$$

For the convenience of discussion, we adopt the following special representatives of G from [8]:

$$H \cup \mathbf{d}(1, \xi^{-1}, \xi^{-2}) \cdot H. \tag{2.2}$$

Lemma 2.3 ([2]). *The group G acts transitively on both I (respectively, Pa) and E (respectively, Se).*

Definition 2.4. Let P be a point not on $\mathcal{O}$ and ℓ a line. We define E_ℓ and I_ℓ to be the set of external points and the set of internal points on ℓ, respectively, Pa_P and Se_P the set of passant lines and the set of secant lines through P, respectively, and T_P 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 2.5. Using the above notation and Lemma 2.5 in [8], for $P \in I$, we have $|E_{P^\perp}| = |Se_P| = \frac{q+1}{2}$; $|I_{P^\perp}| = |Pa_P| = \frac{q+1}{2}$; 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 $W \le G$. Using standard notation from permutation group theory, we have $I_\ell^g = I_{\ell^g}$, $Pa_P^g = Pa_{P^g}$; $E_\ell^g = E_{\ell^g}$, $Se_P^g = Se_{P^g}$ $H_P^g = H_{P^g}$; $N(P)^g = N(P^g)$, $(W^g)_{P^g} = W_P^g$. 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 PG(2, q).

Proposition 2.6. *Let $P \in I$ and set $K := G_P$. Then K is transitive on $I_{P^\perp}$, $E_{P^\perp}$, Pa_P, and Se_P, respectively.*

Proof. Witt's theorem [6] 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 Pa_P and Se_P. □

When $P = (1, 0, -\xi)$, using (2.1) and (2.2), we obtain that $K := G_P$

$$= \left\{ \begin{pmatrix} d^2 & cd\xi & c^2\xi^2 \\ 2cd & d^2+c^2\xi & 2dc\xi \\ c^2 & dc & d^2 \end{pmatrix} \middle| d, c \in \mathbb{F}_q, d^2 - c^2\xi = 1 \right\}$$
$$\bigcup \left\{ \begin{pmatrix} d^2 & -cd\xi & c^2\xi^2 \\ 2cd & -d^2-c^2\xi & 2dc\xi \\ c^2 & -dc & d^2 \end{pmatrix} \middle| d, c \in \mathbb{F}_q, -d^2 + c^2\xi = 1 \right\}$$
$$\bigcup \left\{ \begin{pmatrix} d^2 & cd & c^2 \\ 2cd\xi^{-1} & d^2+c^2\xi^{-1} & 2dc \\ c^2\xi^{-2} & dc\xi^{-1} & d^2 \end{pmatrix} \middle| d, c \in \mathbb{F}_q, d^2\xi - c^2 = 1 \right\}$$
$$\bigcup \left\{ \begin{pmatrix} d^2 & -cd & c^2 \\ 2cd\xi^{-1} & -d^2-c^2\xi^{-1} & 2dc \\ c^2\xi^{-2} & -dc\xi^{-1} & d^2 \end{pmatrix} \middle| d, c \in \mathbb{F}_q, -d^2\xi + c^2 = 1 \right\}. \tag{2.3}$$

Theorem 2.7. *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

$$|N(P) \cap I_\ell| = \begin{cases} \dfrac{q-1}{2}, & \text{if } q \equiv 1 \pmod 4, \\ \dfrac{q+1}{2}, & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

which is even. Therefore, $|N(P) \cap I_\ell| \equiv 0 \pmod 2$ for this case.

If $\ell = P^\perp$, by Lemma 2.9(i) in [8], we have

$$|N(P) \cap I_\ell| = \begin{cases} 0, & \text{if } q \equiv 1 \pmod 4, \\ \dfrac{q+1}{2}, & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

which is even. Hence, $|N(P) \cap I_\ell| \equiv 0 \pmod 2$ for this case.

Now we assume that we have neither $\ell = P^\perp$ nor $P \in \ell$. As G is transitive on Pa and preserves incidence, we may take $\ell = P_1^\perp = [1, 0, -\xi^{-1}]$, where $P_1 = (1, 0, -\xi) \in I$. Since P is either on a passant line through P_1 or on a secant line through P_1, what remains is 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 Se_{P_1} by Proposition 2.6, it is enough to establish that $|N(P) \cap I_\ell|$ is even for an arbitrary internal point on a *special* secant line, ℓ_1 say, through P_1. To this end, we may take $\ell_1 = [0, 1, 0]$. It is clear that

$$I_{\ell_1} = \{(1, 0, -\xi^j) \mid 0 \le j \le q-1, j \text{ odd}\}$$

and

$$I_\ell = \{(1, s, \xi) \mid s \in \mathbb{F}_q, s^2 - \xi \in \not\square_q\}.$$

Hence, if $P = (1, 0, -\xi^j) \in I_{\ell_1}$ then

$$D_j = \left\{ \left[1, -\frac{\xi^{1-j}+1}{s}, \frac{1}{\xi^j} \right] \middle| s \in \mathbb{F}_q^*, s^2 - \xi \in \not\square_q \right\} \cup \{[0, 1, 0]\}$$

consists of the lines through both P and the points on ℓ. Note that the number of passant lines in D_j is determined by the number of s satisfying both

$$\frac{1}{s^2}(\xi^{1-j}+1)^2 - \frac{4}{\xi^j} \in \not\square_q \tag{2.4}$$

and

$$s^2 - \xi \in \not\square_q. \tag{2.5}$$

Since, $s \neq 0$ and whenever s satisfies both (2.4) and (2.5), 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 2.9 [8], we may assume that $P \in P_3^\perp$, where $P_3 = (1, x, \xi) \in I_\ell$ with $x \in \mathbb{F}_q^*$ and $x^2 - \xi \in \not\square_q$. Here $P_3^\perp = [1, -\frac{2x}{\xi}, \frac{1}{\xi}]$ is a passant line through P_1. Let $K = G_{P_1}$ and let $(1, y, \xi)$ be a point on ℓ. Using (2.3), we have that $L := K_{P_3}$ 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 $\ell \cap P_3^\perp = (1, \frac{\xi}{x}, \xi)$ are the only points of the form $(1, s, t)$ on ℓ fixed by L. Since $P \in P_3^\perp$, $P \neq P_1$ and $P \neq P_3^\perp \cap \ell$, $P = (1, \frac{\xi+n}{2x}, n)$ for some $n \neq \xi$. Now if we denote by $\mathbf{V}$ the set of passant lines through P that meet ℓ in an internal point, then it is clear that $|\mathbf{V}| = |N(P) \cap I_\ell|$. Direct computations give us that $L_P \cong \mathbb{Z}_2$. Since P_3 and P are both fixed by

L_P, it follows that both $\ell_{P_3,P}$ and $P_3^\perp$ are fixed by L_P. Note that when $q \equiv 3 \pmod 4$, both $P_3^\perp$ and $\ell_{P_3,P}$ are in $\mathbf{V}$; and when $q \equiv 1 \pmod 4$, neither $\ell_{P_3,P}$ nor $P_3^\perp$ is in $\mathbf{V}$. If there were another line ℓ' through P which is distinct from both $P_3^\perp$ and $\ell_{P_3,P}$ and which is also fixed by L_P, then L_P would fix at least three points on $\ell = P^\perp$, namely, $\ell' \cap \ell$, $P_3^\perp \cap \ell$, and P_3. Since no further point of the form $(1, s, t)$ except for P_3 and $\ell \cap P_3^\perp$ can be fixed by L due to the above discussion, we must have $\ell' \cap \ell = (0, 1, 0) \in E_\ell$. So $\ell' \notin \mathbf{V}$. Using the fact that L_P preserves incidence, we conclude that when $q \equiv 1 \pmod 4$, L_P has $\frac{|\mathbf{V}|}{2}$ orbits of length 2 on $\mathbf{V}$; and when $q \equiv 3 \pmod 4$, L_P has two orbits of length 1, namely, $\{P_3^\perp\}$ and $\{\ell_{P_3,P}\}$, and $\frac{|\mathbf{V}|-2}{2}$ orbits of length 2 on $\mathbf{V}$. Either forces $|\mathbf{V}|$ to be even. Therefore, $|N(P) \cap I_\ell|$ is even. □

Recall that $\mathbf{A}$ 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 $\mathbf{A}$ 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 $P \notin \ell$, $|N(P) \cap I_\ell| = |\widehat{N(P)} \cap I_\ell|$.

Lemma 2.8. *Using the above notation, we have* $\mathbf{A}^3 \equiv \mathbf{A} \pmod 2$, *where the congruence means entrywise congruence.*

Proof. Since the (i, j)-entry of $\mathbf{A}^2 = \mathbf{A}^\top\mathbf{A}$ is the standard dot product of the ith row of $\mathbf{A}^\top$ and jth column of $\mathbf{A}$, we have

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

Therefore, the ith row of $\mathbf{A}^2 \pmod 2$ 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 $(\mathbf{A}^3)_{i,j} = ((\mathbf{A}^2)\mathbf{A}^\top)_{i,j} = q$ since $(\mathbf{A}^2)_{i,i} = \frac{q+1}{2}$ 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 $P_i \notin P_j^\perp$, then $(\mathbf{A}^3)_{i,j} = ((\mathbf{A}^\top\mathbf{A})\mathbf{A}^\top)_{i,j} \equiv |\widehat{N(P_i)} \cap I_{P_j^\perp}| = |N(P_i) \cap I_{P_j^\perp}| \equiv 0 \pmod 2$ by Theorem 2.7. Consequently,

$$(\mathbf{A}^3)_{i,j} \equiv \begin{cases} 1 \pmod 2, & \text{if } P_i \in P_j^\perp, \\ 0 \pmod 2, & \text{if } P_i \notin P_j^\perp. \end{cases}$$

The lemma follows immediately. □

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 $T = \mathrm{tr}(g) + 1$, where $\mathrm{tr}(g)$ is the trace of g.

Lemma 3.1 ([8, Lemma 3.2]). *The conjugacy classes of* H *are given as follows.*

(i) $D = \{\mathbf{d}(1, 1, 1)\}$;
(ii) F^+ *and* F^-, *where* $F^+ \cup F^- = \{g \in H \mid T(g) = 4, g \neq \mathbf{d}(1, 1, 1)\}$;

(iii) $[\theta_i] = \{g \in H \mid T(g) = \theta_i\}$, $1 \le i \le \frac{q-5}{4}$ *if* $q \equiv 1 \pmod 4$, *or* $1 \le i \le \frac{q-3}{4}$ *if* $q \equiv 3 \pmod 4$, *where* $\theta_i \in \Box_q$, $\theta_i \neq 4$, *and* $\theta_i - 4 \in \Box_q$*;*
(iv) $[0] = \{g \in H \mid T(g) = 0\}$*;*
(v) $[\pi_k] = \{g \in H \mid T(g) = \pi_k\}$, $1 \le k \le \frac{q-1}{4}$ *if* $q \equiv 1 \pmod 4$, *or* $1 \le k \le \frac{q-3}{4}$ *if* $q \equiv 3 \pmod 4$, *where* $\pi_i \in \Box_q$, $\pi_k \neq 4$, *and* $\pi_k - 4 \in \not\Box_q$.

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,

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

3.2. Intersection properties

Definition 3.3. Let $P, Q \in I$, $W \subseteq I$, and $\ell \in Pa$. We define $\mathcal{H}_{P,Q} = \{h \in H \mid (P^\perp)^h \in Pa_Q\}$, $\mathcal{S}_{P,\ell} = \{h \in H \mid (P^\perp)^h = \ell\}$, and $\mathcal{U}_{P,W} = \{h \in H \mid P^h \in W\}$. 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, $\mathcal{S}_{P,\ell}$ is the set of elements of H that map $P^\perp$ to the passant line ℓ, and $\mathcal{U}_{P,W}$ is the set of elements of H that map P to a point in W.

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

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) $|K \cap [0]| = \frac{q+1}{2}$ *or* $\frac{q-1}{2}$ *accordingly as* $q \equiv 1 \pmod 4$ *or* $q \equiv 3 \pmod 4$.

Proof. The proof is almost identical to the one of Lemma 3.7 in [8]. We omit the detail. □

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* $C = D, [4], [\pi_k]$ $(1 \le k \le \frac{q-1}{4})$, *or* $[\theta_i]$ $(1 \le i \le \frac{q-5}{4})$.

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* $\ell_{P,Q} \in Se_P$, $Q \notin P^\perp$, *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* $\ell_{P,Q} \in Se_P$, *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 Se_P by Proposition 2.6 and $|\mathcal{H}_{P,Q} \cap C| = |(\mathcal{H}_{P,Q} \cap C)^g| = |\mathcal{H}_{P,Q^g} \cap C|$, we may assume that Q is on either ℓ_1 or ℓ_2, where $\ell_1 = [1, 0, \xi^{-1}] \in Pa_P$ and $\ell_2 = [0, 1, 0] \in Se_P$.

Case I. $Q \in \ell_1$.

In this case, $Q = (1, x, -\xi)$ for some $x \in \mathbb{F}_q^*$ and $x^2 + \xi \in \not\square_q$, and

$$Pa_Q = \{[1, s, (1+sx)\xi^{-1}] \mid s \in \mathbb{F}_q, s^2 - 4(1+sx)\xi^{-1} \in \not\square_q\}.$$

Using (2.3), we obtain that

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

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

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

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:

$$\begin{aligned} &-2cd + 2ab\xi^{-1} = 0 \\ &c^2 - a^2\xi^{-1} = (d^2 - b^2\xi^{-1})\xi^{-1} \\ &a + d = s \\ &ad - bc = 1, \end{aligned} \tag{3.2}$$

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 $2 \in \square_q$ then the above (3.2) gives four group elements in [2] and no elements in any other class. If neither b nor c is zero, then the first two equations in (3.2) yield $b = \pm\sqrt{-1}\xi c$. Combining with the last two equations in (3.2), we obtain zero, four or eight 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 $|\mathcal{S}_{P,\ell_1} \cap C|$ is 0, 2, or 4.

Case II. $Q \in \ell_2$, $Q \notin P^\perp$, and $Q \neq P$.

In this case, $Q = (1, 0, -y)$ for some $y \in \not\square_q$ and $y \neq \pm\xi$. Using (2.3), we obtain that

$$K_Q = \{\mathbf{d}(1, 1, 1), \mathbf{d}(-1, 1, -1)\}.$$

Moreover, K_Q on $Pa_Q = \{[1, s, y^{-1}] \mid s \in \mathbb{F}_q, s^2 - 4y^{-1} \in \not\square_q\}$ has one orbit of length 1, that is, $\{\ell_4 = [1, 0, y^{-1}]\}$, and all other orbits are of length 2. Arguments similar to those above show that the parity of $|\mathcal{H}_{P,Q} \cap C|$ is the same as that of $|\mathcal{S}_{P,\ell_4} \cap C|$. So what remains is to find the parity of $|\mathcal{S}_{P,\ell_4} \cap C|$. The group elements in $\mathcal{S}_{P,\ell_4} \cap C$ are determined by the quadruples (a, b, c, d) satisfying the following equations:

$$\begin{aligned} &-2cd + 2ab\xi^{-1} = 0 \\ &c^2 - a^2\xi^{-1} = (d^2 - b^2\xi^{-1})y^{-1} \\ &a + d = s \\ &ad - bc = 1. \end{aligned} \tag{3.3}$$

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 (3.3) yield $b = \pm\sqrt{-\xi y}c$ and $a = \pm\sqrt{-\xi y^{-1}}d$. Combining with the last two, the above quadruples (a, b, c, d) yield zero, two, or four 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

$$s^2 = \sqrt{-\xi y^{-1}} + \sqrt{-y\xi^{-1}} + 2 \quad \text{or} \quad s^2 = -\sqrt{-\xi y^{-1}} - \sqrt{-y\xi^{-1}} + 2.$$

Since $(\sqrt{-\xi y^{-1}} + \sqrt{-y\xi^{-1}} + 2)(-\sqrt{-\xi y^{-1}} - \sqrt{-y\xi^{-1}} + 2) = (\sqrt{\xi y^{-1}} + \sqrt{y\xi^{-1}})^2$, the above quadruples (a, b, c, d) yield no or one group element in two classes $[\theta_{i_1}]$ and $[\theta_{i_2}]$ where $\theta_{i_1} = \sqrt{-\xi y^{-1}} + \sqrt{-y\xi^{-1}} + 2$ and $\theta_{i_2} = -\sqrt{-\xi y^{-1}} - \sqrt{-y\xi^{-1}} + 2$. The above analysis shows that if $|\mathcal{H}_{P,Q} \cap C|$ is odd then $C = [\theta_{i_1}]$ or $[\theta_{i_2}]$ 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

$$Pa_Q = \{[1, u, -\xi^{-1}] \mid u \in \mathbb{F}_q, u^2 + \xi \in \not\square_q\}.$$

Using (2.3), we obtain that

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

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 $|\mathcal{H}_{P,Q} \cap C|$ is the same as that of $|\mathcal{S}_{P,P} \cap C|$ 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 $q \equiv 1 \pmod 4$.

(i) *If $\ell_{P,Q} \in Pa_P$ and $|\mathcal{U}_{P,N(Q)} \cap C|$ is odd, then $C = [\pi_k]$ for one k or $C = D$.*
(ii) *If $\ell_{P,Q} \in Se_P$, then $|\mathcal{U}_{P,N(Q)} \cap C|$ is even.*

Assume that $q \equiv 3 \pmod 4$.

(iii) *If $\ell_{P,Q} \in Pa_P$, then $|\mathcal{U}_{P,\overline{N(Q)}} \cap C|$ is even.*
(iv) *If $\ell_{P,Q} \in Se_P$ and $|\mathcal{U}_{P,\overline{N(Q)}} \cap C|$ is odd, then $C = [\theta_i]$ for one i or $C = D$.*

Proof. Without loss of generality, we can choose $P = (1, 0, -\xi)$. Since $K = G_P$ acts transitively on both Pa_P and Se_P, we may assume that $Q \neq P$ 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. $\ell_1 = \ell_{P,Q} \in Pa_P$.

In this case, $Q = (1, x, -\xi)$ for some $x \in \mathbb{F}_q$ with $u^2 + \xi \in \not\square_q$ and its internal neighbor is $N(Q) = \{(1, u, -\xi) \mid u^2 + \xi \in \not\square_q\} \setminus \{(1, x, -\xi)\}$ by definition. As $P \in N(Q)$, it is obvious that $|\mathcal{U}_{P,N(Q)} \cap D| = 1$. Since the action of K_Q on Pa_Q has one orbit of length 1, i.e. ℓ_1, and all others are of length 2, whose representatives form the set $\mathcal{R}_1$, we obtain that

$$\begin{aligned} |\mathcal{U}_{P,N(Q)} \cap C| &= \sum_{\ell \in Pa_Q} \sum_{P_1 \in I_\ell \setminus \{Q\}} |\mathcal{U}_{P,P_1} \cap C| \\ &= \sum_{P_1 \in I_{\ell_1} \setminus \{Q\}} |\mathcal{U}_{P,P_1} \cap C| + 2 \sum_{\ell \in \mathcal{R}} \sum_{P_1 \in I_\ell \setminus \{Q\}} |\mathcal{U}_{P,P_1} \cap C|. \end{aligned} \tag{3.4}$$

Now let $P_1 = (1, u, -\xi) \in I_{\ell_1} \setminus \{Q\}$. Then the number of group elements that map P to P_1 is determined by the quadruples (a, b, c, d) which are the solutions to the following system of equations:

$$\begin{aligned} &ab - cd\xi = u(a^2 - c^2\xi) \\ &b^2 - d^2\xi = -\xi(a^2 - c^2\xi) \\ &a + d = s \\ &ad - bc = 1. \end{aligned} \tag{3.5}$$

The first two equations in (3.5) 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

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

and

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

combining with the last two equations of (3.5), we have

$$\left(\xi - \frac{B_\pm^2}{s^2}\right)c^2 + \left(\frac{B_\pm^3}{s^2\xi} - B_\pm\right)c + \left(\frac{s^2}{4} - \frac{B_\pm^4}{4s^2\xi^2} - 1\right) = 0 \tag{3.6}$$

or

$$\left(\xi - \frac{B_\pm^2}{s^2}\right)c^2 - \left(\frac{B_\pm^3}{s^2\xi} - B_\pm\right)c + \left(\frac{s^2}{4} - \frac{B_\pm^4}{4s^2\xi^2} - 1\right) = 0. \tag{3.7}$$

The discriminant of (3.6) or (3.7) is

$$\Delta = \left(1 - \frac{B_\pm^2}{s^2\xi}\right)\left(B_\pm^2 - s^2\xi + 4\xi\right) = \frac{4\xi u^2}{s^2(u^2 + \xi)} \in \square_q.$$

Consequently, the equations in (3.5) have eight solutions and yield four 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 non-square, arguments similar to those above give that the equations in (3.5) have four solutions and produce two different group elements.

If one of $s^2\xi - (2 + A)\xi$ and $s^2\xi - (2 - A)\xi$ is zero, then s^2 is one of $2 + A$ and $2 - A$; and moreover it is one of π_k for $1 \le k \le \frac{q-1}{4}$ since $(2 + A)(2 - A) = \frac{4u^2}{u^2+\xi} \in \not\square_q$ and $-1 \in \square_q$. Consequently, the equations in (3.5) yield either one or three group elements in $[s^2]$.

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

Case II. $\ell_2 = \ell_{P,Q} \in Se_P$ and $Q \notin P^\perp$.

Then $Q = (1, 0, -y)$ for $y \notin \not\square_q$ and $y \neq \pm\xi$. From the proof of Case II in Lemma 3.5, we have that $K_Q = \{\mathbf{d}(1, 1, 1), \mathbf{ad}(-1, 1, -1)\}$, 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 $|\mathcal{U}_{P,I_{\ell_i}} \cap C| = |\mathcal{U}_{P,I_{\ell_j}} \cap C|$ where $\ell_i, \ell_j \in Pa_P$ and $\ell_j = \ell_i^g$ for $g \in K_Q$, we obtain that

$$\begin{aligned} |\mathcal{U}_{P,N(Q)} \cap C| &= \sum_{\ell \in Pa_Q} \sum_{P_1 \in I_\ell \setminus \{Q\}} |\mathcal{U}_{P,P_1} \cap C| \\ &= \sum_{P_1 \in I_{\ell_4} \setminus \{Q\}} |\mathcal{U}_{P,P_1} \cap C| + 2\sum_{\ell \in \mathcal{R}} \sum_{P_1 \in I_\ell \setminus \{Q\}} |\mathcal{U}_{P,P_1} \cap C|. \end{aligned} \tag{3.8}$$

Moreover, since the orbits of K_Q on $I_{\ell_4} \setminus \{Q\}$, whose representatives form the set $\mathcal{R}_1$, are of length 2 and $|\mathcal{U}_{P,P_1} \cap C| = |\mathcal{U}_{P,P_2} \cap C|$ for $P_2 = P_1^g$, the first term of the last expression in (3.8) can be rewritten as

$$2\sum_{P_1 \in \mathcal{R}_1} |\mathcal{U}_{P,P_1} \cap C|.$$

So $|\mathcal{U}_{P,N(Q)} \cap C|$ is even in this case.

Case III. $P = \ell_2 \cap P^{\perp}$.

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. $P^{\perp}$. Moreover, all the orbits of K_Q on $I_{P^{\perp}} \setminus \{Q\}$ are of length 2. Hence $|\mathcal{U}_{P,N(Q)} \cap C|$ is even.

The case when $q \equiv 3 \pmod 4$ can be established in the same way and we omit the details. □

4. Linear maps

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 if and only if $q \equiv 3 \pmod 4$. We define $\mathbf{D}$ to be the incidence matrix of $N(P)$ $(P \in I)$ and I. That is, the rows of $\mathbf{D}$ can be viewed as the characteristic vectors of $N(P)$ with respect to I. In the following, we always regard both $\mathbf{D}$ and $\mathbf{A}$ as matrices over F. Moreover, it is apparent that $\mathbf{D} = \mathbf{A}^2 + \mathbf{I}$, where $\mathbf{I}$ is the identity matrix of proper size.

Definition 4.1. For $W \subseteq I$, we define $\mathcal{C}_W$ to be the row characteristic vector of W with respect to I, namely $\mathcal{C}_W$ is a 0–1 row vector of length $|I|$ with entries indexed by internal points and the entry of $\mathcal{C}_W$ is 1 if and only if the point indexing the entry is in W. If $W = \{P\}$, as a convention, we write $\mathcal{C}_W$ as $\mathcal{C}_P$.

Let k be the complex field $\mathbb{C}$, the algebraic closure F of $\mathbb{F}_2$, or the ring $\mathbf{S}$ in (4.1) of [8]. Let k^I be the free k-module with the base $\{\mathcal{C}_P \mid P \in I\}$. If we extend the action of H on the basis elements of k^I, which is defined by $\mathcal{C}_Q \cdot h = \mathcal{C}_{Q^h}$ for $P \in I$ and $h \in H$, linearly to k^I, then k^I is a kH-permutation module. Since H is transitive on I, we have

$$k^I = \mathrm{Ind}_K^H(1_k),$$

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

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

Lemma 4.2. *Let K be the stabilizer of an internal point in H.*

Assume that $q \equiv 1 \pmod 4$. Let χ_s, $1 \le s \le \frac{q-1}{4}$, be the irreducible characters of degree $q-1$, ϕ_r, $1 \le r \le \frac{q-5}{4}$, the irreducible characters of degree $q+1$, γ the irreducible character of degree q, and β_j, $1 \le j \le 2$, the irreducible characters of degree $\frac{q+1}{2}$.

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

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

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

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

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

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

Next assume that $q \equiv 3 \pmod 4$. Let χ_s, $1 \le s \le \frac{q-3}{4}$, be the irreducible characters of degree $q-1$, ϕ_r, $1 \le r \le \frac{q-3}{4}$, the irreducible characters of degree $q+1$, γ the irreducible character of degree q, and η_j, $1 \le j \le 2$, the irreducible characters of degree $\frac{q-1}{2}$.

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

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

where χ_{s_j}, $1 \le j \le \frac{q-3}{4}$, 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 χ_{s_j}, $1 \le j \le \frac{q+1}{4}$, *may not be distinct.*

Proof. We provide the proof for the case when $q \equiv 1 \pmod 4$ and we use the character tables of PSL(2, q) in the appendix of [8].

Let 1_H be the trivial character of H. By the Frobenius reciprocity [3],

$$\left\langle 1_K\uparrow_K^H, 1_H\right\rangle_H = \left\langle 1_K, 1_H\downarrow_K^H\right\rangle_K = 1.$$

Let χ_s be an irreducible character of degree $q-1$ of H, where $1 \le s \le \frac{q-1}{4}$. We denote the number of elements of K lying in the class $[\pi_k]$ by d_k. Then $d_k = 2$ by Lemma 3.4(iii), and so

$$\begin{aligned}\left\langle 1_K\uparrow_K^H, \chi_s\right\rangle_H = \left\langle 1_K, \chi_s\downarrow_K^H\right\rangle_K &= \frac{1}{|K|}\sum_{g\in K}\chi_s \downarrow_K^H (g)\\ &= \frac{1}{q+1}\left[(1)(q-1) + 2\sum_{k=1}^{(q-1)/4}(-\delta^{(2k)s} - \delta^{-(2k)s})\right]\\ &= 1,\end{aligned}$$

where

$$\begin{aligned}\sum_{k=1}^{(q-1)/4}(-\delta^{(2k)s} - \delta^{-(2k)s}) &= -(1 + \delta^{2s} + (\delta^{2s})^2 + \cdots + (\delta^{2s})^{(q-1)/2} - 1)\\ &= -\frac{1-\delta^{(q+1)s}}{1-\delta^{2s}} + 1\\ &= 1\end{aligned}$$

since $\delta^{q+1} = 1$.

Let γ be the irreducible character of degree q of H. Then

$$\begin{aligned}\left\langle 1_K\uparrow_K^H, \gamma\right\rangle_H = \left\langle 1_K, \gamma\downarrow_K^H\right\rangle_K &= \frac{1}{|K|}\sum_{g\in K}\gamma \downarrow_K^H (g)\\ &= \frac{1}{q+1}\left[(1)(q) + (2)(-1)\left(\frac{q-1}{4}\right) + (1)\left(\frac{q+1}{2}\right)\right]\\ &= 1.\end{aligned}$$

Let β_j be any irreducible character of degree $\frac{q+1}{2}$ of H. Then

$$\begin{aligned}\left\langle 1_K\uparrow_K^H, \beta_j\right\rangle_H &= \frac{1}{|K|}\sum_{g\in K}\beta_j \downarrow_K^H (g)\\ &= \frac{1}{q+1}\left[(1)\left(\frac{q+1}{2}\right) + (2)\left(\frac{q-1}{4}\right)(0) + \left(\frac{q+1}{2}\right)(-1)^{(q-1)/4}\right].\end{aligned} \tag{4.1}$$

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

Since the sum of the degrees of 1, χ_s, γ, and β_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

$$1_K\uparrow_K^H - 1_H - \sum_{s=1}^{(q-1)/4} \chi_s - \gamma - \beta_1 - \beta_2 \quad \text{or} \quad 1_K\uparrow_K^H - 1_H - \sum_{s=1}^{(q-1)/4} \chi_s - \gamma$$

must have degree $q+1$. □

Since H preserves incidence, it is obvious that, for $P \in I$ and $h \in H$,

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

In the rest of the article, we always view $\mathcal{C}_P$ as a vector over F. Consider the maps ϕ and μ 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 ϕ and μ, are $\mathbf{A}$ and $\mathbf{D}$, respectively, and for $\mathbf{x} \in F^I$, $\phi(\mathbf{x}) = \mathbf{xA}$ and $\mu(\mathbf{x}) = \mathbf{xD}$. Moreover, we have the following result since H is transitive on I and preserves incidence:

Lemma 4.3. *The maps ϕ and μ are both FH-module homomorphisms from F^I to F^I.*

We will always use $\mathbf{0}$ and $\hat{\mathbf{0}}$ 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 $\hat{\mathbf{J}}$ and $\mathbf{J}$ the all-one row vector of length $|I|$ and the all-one matrix of size $|I| \times |I|$. The following proposition can be easily verified using the fact that $\mathbf{A}^3 \equiv \mathbf{A} \pmod 2$.

Proposition 4.4. *As FH-modules, $F^I = \operatorname{Im}(\phi) \oplus \operatorname{Ker}(\phi)$, where $\operatorname{Im}(\phi)$ and $\operatorname{Ker}(\phi)$ are the image and kernel of ϕ, respectively.*

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

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

Therefore, $\operatorname{Ker}(\phi^2) = \operatorname{Ker}(\phi)$. Furthermore, since $\operatorname{Ker}(\phi) \subseteq \operatorname{Ker}(\phi^2) \subseteq \operatorname{Ker}(\phi^3) \subseteq \cdots$, we have $\operatorname{Ker}(\phi^i) = \operatorname{Ker}(\phi)$ for $i \geq 2$. Applying the Fitting decomposition theorem [7, p. 285] to the operator ϕ, we can find an i such that $F^I = \operatorname{Ker}(\phi^i) \oplus \operatorname{Im}(\phi^i)$. From the above discussions, we must have $F^I = \operatorname{Ker}(\phi) \oplus \operatorname{Im}(\phi)$. □

Corollary 4.5. *As FH-modules, $\operatorname{Ind}_K^H(1_F) \cong \operatorname{Ker}(\phi) \oplus \operatorname{Im}(\phi)$.*

Proof. The conclusion follows immediately from Proposition 4.4 and the fact that $\operatorname{Ind}_K^H(1_F) \cong F^E$. □

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

Let μ_2 be the FH-homomorphism from F^I to F^I whose matrix with respect to the natural basis is $\mathbf{C}$. The following proposition is clear.

Proposition 4.6. *Using the above notation, we have* $\operatorname{Ker}(\phi) = \operatorname{Im}(\mu)$.

Furthermore, we have the following decomposition of $\operatorname{Ker}(\phi)$.

Lemma 4.7. *Assume that $q \equiv 3 \pmod 4$. Then we have, as FH-modules,* $\operatorname{Ker}(\phi) = \langle\hat{\mathbf{J}}\rangle \oplus \operatorname{Im}(\mu_2)$, *where $\langle\hat{\mathbf{J}}\rangle$ is the trivial FH-module generated by $\hat{\mathbf{J}}$.*

Proof. Let $\mathbf{y} \in \langle \hat{\mathbf{J}} \rangle \cap \mathrm{Im}(\mu_2)$. Then $\mathbf{y} = \mu_2(\mathbf{x}) = \lambda \hat{\mathbf{J}}$ for some $\lambda \in F$ and $\mathbf{x} \in F^I$. Or equivalently, we have $\mu_2(\mathbf{x}) = \mathbf{xC} = \mathbf{x}(\mathbf{A}^2 + \mathbf{I} + \mathbf{J}) = \lambda \hat{\mathbf{J}}$. Note that $\mathbf{J}^2 = \mathbf{J}$ and $\hat{\mathbf{J}}\mathbf{J} = \hat{\mathbf{J}}$ since $2 \nmid |I|$ when $q \equiv 3 \pmod 4$. Moreover, $\mathbf{A}^2\mathbf{J} = \hat{\mathbf{0}}$ as each row of $\mathbf{A}^2$, viewed as the characteristic vector of $\widehat{N(P)}$, has an even number of 1s. Consequently,

$$\lambda \hat{\mathbf{J}} = \lambda \hat{\mathbf{J}}\mathbf{J} = \mathbf{x}(\mathbf{A}^2 + \mathbf{I} + \mathbf{J})\mathbf{J} = \mathbf{x}(\mathbf{A}^2\mathbf{J} + \mathbf{IJ} + \mathbf{J}^2) = \mathbf{x}(\hat{\mathbf{0}} + \mathbf{J} + \mathbf{J}) = \mathbf{0}.$$

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

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

5. Statement and proof of the main theorem

The main theorem is stated as follows.

Theorem 5.1. *Let* $\mathrm{Ker}(\phi)$ *be defined as above. As FH-modules,*

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

$$\mathrm{Ker}(\phi) = \bigoplus_{s=1}^{(q-1)/4} M_s,$$

where M_s *for* $1 \le s \le \frac{q-1}{4}$ *are pairwise non-isomorphic simple FH-modules of dimension* $q - 1$;

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

$$\mathrm{Ker}(\phi) = \langle \hat{\mathbf{J}} \rangle \oplus \left(\bigoplus_{r=1}^{(q-3)/4} M_r \right),$$

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

In what follows, we refer the reader to Section 4 and Lemma 7.1 in [8] for the discussions of the block idempotents of H and their corresponding standard notation.

Lemma 5.2. *The following two statements are true.*

(i) *If* $q \equiv 1 \pmod 4$, *then the character of* $f_{B_s} \cdot \mathrm{Ind}_K^H(1_{\mathbb{C}})$ *is* χ_s *for each block* B_s *of defect* 0.
(ii) *If* $q \equiv 3 \pmod 4$, *then the character of* $f_{B_r} \cdot \mathrm{Ind}_K^H(1_{\mathbb{C}})$ *is* ϕ_r *for each block* B_r *of defect* 0.

Proof. The corollary follows from Lemma 4.1 in [8] and Lemma 4.2. □

Lemma 5.3. *Let* $q-1 = 2^n m$ *or* $q+1 = 2^n m$ *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* $e_{B_0} \cdot \mathrm{Ker}(\phi) = \mathbf{0}$, $e_{B_s} \cdot \mathrm{Im}(\phi) = \mathbf{0}$ *for* $1 \le s \le \frac{q-1}{4}$, *and* $e_{B'_t} \cdot \mathrm{Ker}(\phi) = \mathbf{0}$ *for* $m \ge 3$ *and* $1 \le t \le \frac{m-1}{2}$;
(ii) *if* $q \equiv 3 \pmod 4$, *then* $e_{B_0} \cdot \mathrm{Im}(\mu_2) = \mathbf{0}$, $e_{B_r} \cdot \mathrm{Im}(\phi) = \mathbf{0}$ *for* $1 \le r \le \frac{q-3}{4}$, *and* $e_{B'_t} \cdot \mathrm{Im}(\mu_2) = \mathbf{0}$ *for* $m \ge 3$ *and* $1 \le t \le \frac{m-1}{2}$.

Proof. It is clear that $\mathrm{Im}(\phi)$, $\mathrm{Ker}(\phi)$, and $\mathrm{Im}(\mu_2)$ are generated by

$$\{\mathcal{C}_{P^\perp} \mid P \in I\}, \quad \{\mathcal{C}_{N(P)} \mid P \in I\}, \quad \text{and} \quad \{\mathcal{C}_{\overline{N(P)}} \mid P \in I\}$$

over F, respectively. Now let $B \in Bl(H)$. Since

$$e_B \cdot \mathcal{C}_{P^\perp} = \sum_{C \in Cl(H)} e_B(\widehat{C}) \sum_{h \in C} h \cdot \mathcal{C}_{P^\perp} = \sum_{C \in Cl(H)} e_B(\widehat{C}) \sum_{h \in C} \mathcal{C}_{(P^\perp)^h}, = \sum_{C \in Cl(H)} e_B(\widehat{C}) \sum_{h \in C} \sum_{Q \in (P^\perp)^h \cap I} \mathcal{C}_Q,$$

we have

$$e_B \cdot \mathcal{C}_{P^\perp} = \sum_{Q \in I} \mathcal{S}_1(B, P, Q)\mathcal{C}_Q,$$

where

$$\mathcal{S}_1(B, P, Q) := \sum_{C \in Cl(H)} |\mathcal{H}_{P,Q} \cap C| e_B(\widehat{C}).$$

Similarly $e_B \cdot \mathcal{C}_{N(P)} = \sum_{Q \in I} \mathcal{S}_2(B, P, Q)\mathcal{C}_Q$ and $e_B \cdot \mathcal{C}_{\overline{N(P)}} = \sum_{Q \in I} \mathcal{S}_3(B, P, Q)\mathcal{C}_Q$, where

$$\mathcal{S}_2(B, P, Q) = \sum_{C \in Cl(H)} |\mathcal{U}_{P,N(Q)} \cap C| e_B(\widehat{C})$$

and

$$\mathcal{S}_3(B, P, Q) = \sum_{C \in Cl(H)} |\mathcal{U}_{P,\overline{N(Q)}} \cap C| e_B(\widehat{C}).$$

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 $|\mathcal{H}_{P,Q} \cap C| = 0$ in F for each $C \neq [0]$ by Lemma 3.6(i), and $e_{B_s}(\widehat{[0]}) = 0$ by Lemma 4.5 2(c) in [8]; and by Lemma 3.6(i), and Lemma 4.5 1(a), (c), (d), (a), (c), (d) in [8], we obtain

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

and

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

If $\ell_{P,Q} \in Se_P$ and $Q \notin P^\perp$, then by Lemma 3.5(ii), and Lemma 4.5 2(c) in [8] we obtain

$$S_1(B_s, P, Q) = e_{B_s}(\widehat{[0]}) + e_{B_s}(\widehat{[\theta_{i_1}]}) + e_{B_s}(\widehat{[\theta_{i_1}]}) = 0 + 0 + 0 = 0;$$

and by Lemma 4.5 1(c), 3(c) in [8], and Lemma 3.6(ii), $S_2(B_0, P, Q) = e_{B_0}(\widehat{[0]}) = 0$ and $S_2(B'_t, P, Q) = e_{B'_t}(\widehat{[0]}) = 0$.

If $\ell_{P,Q} \in Se_P$ and $Q \in P^\perp$, then by Lemma 3.5(iii), and Lemma 4.5 2(a) and (c) in [8] we obtain $S_1(B_s, P, Q) = e_{B_s}(\widehat{[0]}) + e_{B_s}(\widehat{D}) = 0 + 0 = 0$; and from Lemma 3.6(ii), and Lemmas 4.5 1(c) and 3(c) in [8], it follows that $S_2(B_0, P, Q) = e_{B_0}(\widehat{[0]}) = 0$ and $S_2(B'_t, P, Q) = e_{B'_t}(\widehat{[0]}) = 0$.

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) in [8], we have

$$S_1(B_r, P, Q) = e_{B_r}(\widehat{[0]}) + e_{B_r}(\widehat{[\pi_{k_1}]}) + e_{B_r}(\widehat{[\pi_{k_2}]}) = 0 + 0 + 0 = 0;$$

and by Lemma 3.6(iii), and Lemma 4.5 4(d) and 6(d) in [8], we obtain $S_3(B_0, P, Q) = e_{B_0}(\widehat{[0]}) = 0$ and $S_3(B'_t, P, Q) = e_{B'_t}(\widehat{[0]}) = 0$.

If $Q = \ell_{P,Q} \cap P^\perp$, then by Lemma 3.6(iii) and 3.5(iii), and 4(d), 5(a), (c), 6(d) of Lemma 4.5 in [8], $S_3(B_0, P, Q) = e_{B_0}(\widehat{[0]}) = 0$, $S_1(B_r, P, Q) = e_{B_r}(\widehat{[0]}) + e_{B_r}(\widehat{D}) = 0 + 0 = 0$, and $S_3(B'_t, P, Q) = e_{B'_t}(\widehat{[0]}) = 0$.

If $\ell_{P,Q} \in Se_P$, then by Lemma 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 in [8],

$$S_3(B_0, P, Q) = e_{B_0}(\widehat{[0]}) + e_{B_0}(\widehat{D}) + e_{B_0}(\widehat{[\theta_i]}) = 0 + 1 + 1 = 0,$$

$S_1(B_r, P, Q) = e_{B_r}(\widehat{[0]}) = 0$, and

$$S_3(B'_t, P, Q) = e_{B'_t}(\widehat{[0]}) + e_{B'_t}(\widehat{D}) + e_{B'_t}(\widehat{[\theta_i]}) = 0 + 0 + 0 = 0. \quad \square$$

Proof of Theorem 5.1. Let B be a 2-block of defect 0 of H. Then by Lemma 4.6 in [8], we have

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

Therefore, by Lemma 5.2, $F^I \cdot e_B = N$, 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 $q \equiv 3 \pmod 4$.

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

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

$e_{B_0} \cdot \mathrm{Ker}(\phi) = \mathbf{0}$ and $e_{B'_t} \cdot \mathrm{Ker}(\phi) = \mathbf{0}$, then

$$\mathrm{Ker}(\phi) = \bigoplus_{B \in Bl(H)} e_B \cdot \mathrm{Ker}(\phi) = \bigoplus_{s=1}^{(q-1)/4} e_{B_s} \cdot \mathrm{Ker}(\phi) = \bigoplus_{s=1}^{(q-1)/4} N_s,$$

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 $q \equiv 3 \pmod 4$. Lemma 4.7 yields $\mathrm{Ker}(\phi) = \langle \hat{\mathbf{J}} \rangle \oplus \mathrm{Im}(\mu_2)$. Since $e_{B_0} \cdot \mathrm{Im}(\mu_2) = \mathbf{0}$ and $e_{B'_t} \cdot \mathrm{Im}(\mu_2) = \mathbf{0}$, applying the same argument as above, we have

$$\mathrm{Im}(\mu_2) = \bigoplus_{r=1}^{(q-3)/4} M_r,$$

where each M_r is a simple FH-module of dimension $q+1$. Consequently,

$$\mathrm{Ker}(\phi) = \langle \hat{\mathbf{J}} \rangle \oplus \left(\bigoplus_{r=1}^{(q-3)/4} M_r \right). \quad \square$$

Now Conjecture 1.1 follows as a corollary.

Corollary 5.4. *Let $\mathcal{L}$ be the $\mathbb{F}_2$-null space of* $\mathbf{A}$. *Then*

$$\dim_{\mathbb{F}_2}(\mathcal{L}) = \frac{(q-1)^2}{4}.$$

Proof. By Theorem 5.1 and the fact that $\dim_{\mathbb{F}_2}(\mathcal{L}) = \dim_{\mathbb{F}_2}(\mathrm{Ker}(\phi))$, when $q \equiv 1 \pmod 4$, we have

$$\dim_{\mathbb{F}_2}(\mathcal{L}) = \sum_{i=1}^{(q-1)/4} (q-1),$$

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

$$\dim_{\mathbb{F}_2}(\mathcal{L}) = 1 + \sum_{i=1}^{(q-3)/4} (q+1),$$

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

Acknowledgment

The second author's research was supported in part by NSF HBCU-UP Grant Award #0929257 at Lane College.

References

[1] S. Droms, K.E. Mellinger, C. Meyer, LDPC codes generated by conics in the classical projective plane, Des. Codes Cryptogr. 40 (2006) 343–356.
[2] R.H. Dye, Hexagons, conics, A_5 and $\mathrm{PSL}_2\,(K)$, J. Lond. Math. Soc. 44 (2) (1991) 270–286.
[3] 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.
[4] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, second ed., Oxford University Press, Oxford, 1998.
[5] D.R. Hughes, F.C. Piper, Projective Planes, Graduate Texts in Mathematics, vol. 6, Springer-Verlag, New York Inc., 1983.
[6] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1976.
[7] T.-Y. Lam, A First Course in Noncommutative Rings, in: Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York Inc., 1991.
[8] P. Sin, J. Wu, Q. Xiang, Dimensions of some binary codes arising from a conic in $PG(2, q)$, J. Combin. Theory A 118 (2011) 853–878.
[9] J. Wu, Proofs of two conjectures on the dimensions of binary codes (under review).