The twisted cubic in $PG(3, q)$ and translation spreads in $H(q)$

G. Bonoli, O. Polverino

Dipartimento di Matematica, Seconda Università degli Studi di Napoli, Via Vivaldi n. 43, Caserta 81100, Italy

Received 14 October 2003; received in revised form 18 February 2005; accepted 1 March 2005
Available online 22 June 2005

Abstract

Using the connection between translation spreads of the classical generalized hexagon $H(q)$ and the twisted cubic of $PG(3, q)$, established in [European J. Combin. 23 (2002) 367–376], we prove that if $q^n \equiv 1 \mod 3$, $q$ odd, $q \geq 4n^2 - 8n + 2$ and $n > 2$, then $H(q^n)$ does not admit an $\mathbb{F}_q$-translation spread.

© 2005 Elsevier B.V. All rights reserved.

Keywords: Generalized hexagon; Spread; Twisted cubic

1. Introduction

In [4] Cardinali et al. prove that each translation spread with respect to a line of the generalized hexagon $H(q^n)$, with kernel containing $\mathbb{F}_q$, defines an $\mathbb{F}_q$-linear subset $\mathcal{S}$ of $PG(3, q^n)$ of rank $2n$ whose points belong to imaginary chords of a twisted cubic $\mathcal{C}$ of $PG(3, q^n)$, and conversely. This connection has motivated the study of $\mathbb{F}_q$-linear sets of $PG(3, q^n)$ of rank $2n$ with the previous property.

In [4] the authors prove that, if $q \equiv 1 \mod 3$, then each imaginary axis of $\mathcal{C}$ is an $\mathbb{F}_q$-linear set of rank 2 of $PG(3, q)$ whose points belong to imaginary chords of a twisted cubic $\mathcal{C}$ of $PG(3, q)$, obtaining new families of examples of $\mathbb{F}_q$-translation spreads of $H(q)$ for $q$ even.
Next, in [9] Lunardon and Polverino show that a line \( l \) of \( \text{PG}(3, q) \) whose points belong to imaginary chords of a twisted cubic \( C \) of \( \text{PG}(3, q) \) either is an imaginary chord of \( C \) or \( q \equiv 1 \pmod{3} \) and \( l \) is an imaginary axis of \( C \). Relying on this result, they extend the classification of semiclassical spreads of \( H(q) \) due to Bloemen et al. [3] to the even characteristic case.

In this paper, we prove that if \( q^n \equiv 1 \pmod{3} \), \( q \) odd, \( q \geq 4n^2 - 8n + 2 \) and \( n > 2 \), then an \( \mathbb{F}_q \)-linear subset of \( \text{PG}(3, q^n) \) of rank \( 2n \) of \( \text{PG}(3, q^n) \) whose points belong to imaginary chords of a twisted cubic \( C \) of \( \text{PG}(3, q^n) \) is an \( \mathbb{F}_{q^n} \)-linear set and hence it is a line. As an application we get that if \( q^n \equiv 1 \pmod{3} \), \( q \) odd, \( q \geq 4n^2 - 8n + 2 \) and \( n > 2 \), then \( H(q^n) \) does not admit an \( \mathbb{F}_q \)-translation spread with respect to a line.

2. Preliminaries and statement of the main results

The twisted cubic \( C \) of \( \text{PG}(3, q) \), \( q = p^r \), \( p \) prime, can be described as

\[
C = \{(f_0(t), f_1(t), f_2(t), f_3(t)) : t \in \mathbb{F}_q \cup \{\infty\}\},
\]

where \( f_0(t), \ldots, f_3(t) \) are linearly independent cubic polynomials over \( \mathbb{F}_q \). Let \( \bar{C} \) be the twisted cubic of \( \text{PG}(3, \bar{F}) \) defined by \( C \), where \( \bar{F} \) is the algebraic closure of \( \mathbb{F}_q \). A line of \( \text{PG}(3, q) \) is a chord of \( C \) if it contains two points of \( \bar{C} \). There are three possibilities: the two points are distinct and belong to \( C \), or they are coincident, or they are conjugate over \( \mathbb{F}_q^2 \); the line is called a real chord, a tangent or an imaginary chord, respectively. Every point not belonging to \( C \) lies on exactly one chord (see e.g. [6, Theorem 21.1.9]). If \( p \neq 3 \), the tangents to \( C \) are self-polar lines of a non-singular symplectic polarity \( \omega \) of \( \text{PG}(3, q) \). An axis of \( C \) is a line \( l \) of \( \text{PG}(3, q) \) whose polar line with respect to \( \omega \) is a chord. We say that \( l \) is a real axis or an imaginary axis when \( l \) is a real chord or an imaginary chord, respectively (for more details, see [6, Section 21]). If \( q \equiv 1 \pmod{3} \) and \( l \) is an imaginary axis, then all points on \( l \) belong to some imaginary chord (see [4]). In [9] the following result has been proved.

**Theorem 2.1** (Lunardon and Polverino [9]). If \( l \) is a line of \( \text{PG}(3, q) \) whose points belong to imaginary chords of \( C \), then either \( l \) is an imaginary chord or \( q \equiv 1 \pmod{3} \) and \( l \) is an imaginary axis.

An \( \mathbb{F}_q \)-linear set of \( \text{PG}(r, q^n) = \text{PG}(V, \mathbb{F}_q^n) \) of rank \( k \) is a set of points of \( \text{PG}(r, q^n) \) defined by the vectors of an \( \mathbb{F}_q \)-vector subspace of \( V \) of dimension \( k \). We say that the pair \((q, n)\), \( q = p^h \), \( p \) an odd prime and \( n \) positive integer, satisfies Property (K) if

(K) there exists no subplane of order \( q \) of \( \text{PG}(2, q^n) \) contained in the set of the internal points of an irreducible conic.

Property (K) can be reformulated in terms of \( \mathbb{F}_q \)-linear sets:

(K) any \( \mathbb{F}_q \)-linear set \( X \) of \( \text{PG}(2, q^n) \), consisting of internal points of an irreducible conic, is contained in a line.
If \( n = 1, 2 \), then Property (K) is always satisfied and the following result shows that for a fixed \( n \), all but a finite number of the pairs \((q, n)\) satisfy Property (K).

**Theorem 2.3.** (Ball et al. [2].) Let \((q, n)\) be a pair of positive integers with \( q = p^h \), \( p \) odd prime. If \( q \geq 4n^2 - 8n + 2 \), then \((q, n)\) satisfies Property (K).

Property (K) is connected to the existence of translation ovoids of \(Q(4, q)\) and semifield flocks of the quadratic cone of \(PG(3, q^n)\) (for more details see [8,14]).

The only known examples of pairs not satisfying Property (K) are the pairs \((3, n)\) with \( n > 2 \) (see, e.g., [3]).

In this paper we generalize the problem studied in Theorem 2.1 to \(\mathbb{F}_q\)-linear sets of \(PG(3, q^n)\) of rank \(2n\), proving the following:

**Theorem 2.3.** Let \(\mathcal{S}\) be an \(\mathbb{F}_q\)-linear set of \(PG(3, q^n)\) of rank \(2n\) whose points belong to imaginary chords of \(\mathcal{C}\). If \(q^n \equiv 1 \pmod{3}\) and the pair \((q, n)\) satisfies Property (K) with \( n > 2 \), then \(\mathcal{S}\) is an \(\mathbb{F}_q\)-linear set and either \(\mathcal{S}\) is an imaginary chord or \(\mathcal{S}\) is an imaginary axis of \(\mathcal{C}\).

From Theorems 2.2 and 2.3 we get the following corollary.

**Corollary 2.4.** Let \(\mathcal{S}\) be an \(\mathbb{F}_q\)-linear set of \(PG(3, q^n)\) of rank \(2n\) whose points belong to imaginary chords of \(\mathcal{C}\). If \(q^n \equiv 1 \pmod{3}\), \(q\) odd, \(q \geq 4n^2 - 8n + 2\) and \(n > 2\), then either \(\mathcal{S}\) is an imaginary chord or \(\mathcal{S}\) is an imaginary axis of \(\mathcal{C}\).

3. Application to translation spreads of \(H(q)\)

Theorem 2.3 can be used to study translation spreads with respect to a line of the generalized hexagon \(H(q)\).

Tits [17] defines the generalized hexagon \(H(q)\) as follows. Let \(Q(6, q)\) be the parabolic quadratic of \(PG(6, q)\) with equation \(X^2_3 = X_0X_4 + X_1X_5 + X_2X_6\). The points of \(H(q)\) are all the points of \(Q(6, q)\). The lines of \(H(q)\) are those lines of \(Q(6, q)\) whose Grassmann coordinates satisfy the equations \(p_{34} = p_{12}, p_{35} = p_{20}, p_{36} = p_{01}, p_{03} = p_{56}, p_{13} = p_{64}\) and \(p_{23} = p_{45}\). Two elements of \(H(q)\) are opposite if they are at distance 6 in the incidence graph of \(H(q)\). A spread \(S\) of \(H(q)\) is a set of \(q^3 + 1\) mutually opposite lines of \(H(q)\). Let \(L\) be a fixed line of \(H(q)\) and denote by \(E^L\) the group of the automorphisms of \(H(q)\) generated by all the collineations fixing \(L\) pointwise and stabilizing all the lines through some point of \(L\). The group \(E^L\) has order \(q^5\) and acts regularly on the set of the lines of \(H(q)\) at distance 6 from \(L\) (see, e.g., [1] or [18]). A spread \(S\) of \(H(q)\) containing \(L\) is a translation spread with respect to \(L\), if for each \(x \in L\) there is a subgroup of \(E^L\) which preserves \(S\) and acts transitively on the lines of \(S\) at distance 4 from \(M\), for all lines \(M\) of \(H(q)\) incident with \(x\) and different from \(L\) (see [3]). By [12] it is possible to associate with any translation spread \(S\) with respect to a line of \(H(q)\) a subfield of \(\mathbb{F}_q\), called the kernel of \(S\).

Using the construction of \(H(q^n)\) as a coset geometry (see [1]) in [4] it is proved that each translation spread \(S\) with respect to a line of \(H(q^n)\) with kernel \(\mathbb{F}_q\) defines an \(\mathbb{F}_q\)-linear
set \( \mathcal{S} \) of \( PG(3, q^n) \) of rank \( 2n \) whose points belong to imaginary chords of the twisted cubic \( \mathcal{C} \) of \( PG(3, q^n) \) having \( \mathbb{F}_q \) as the maximal subfield of linearity, and conversely. If \( S \) is a translation spread of \( H(q^n) \) with kernel \( \mathbb{F}_q \), we say that \( S \) is an \( \mathbb{F}_q \)-translation spread of \( H(q^n) \). The known examples of \( \mathbb{F}_q \)-translation spreads of \( H(q) \) with respect to a line are the hermitian spreads [13], which correspond to \( \mathcal{S} \) being an imaginary chord of \( \mathcal{C} \) [4, Theorem 5], the spreads \( S_{[9]} \) constructed in [3] for \( q \equiv 1 \pmod{3} \), \( q \) odd, and the spreads \( S_l \) constructed, independently, in [4,12] for \( q \equiv 1 \pmod{3} \), \( q \) even. The only known \( \mathbb{F}_q \)-translation spreads of \( H(q^n) \) with respect to a line, with \( \mathbb{F}_q \) a proper subfield of \( \mathbb{F}_{q^n} \), are the spreads \( S_{[9]} \) of \( H(3h) \), \( h > 1 \), constructed in [3]. The hermitian spreads, the spreads \( S_{[9]} \) and \( S_l \), up to isomorphism, are the only \( \mathbb{F}_q \)-translation spreads of \( H(q) \). This classification result is due to Bloemen–Thas–Van Maldeghem [3] for \( q \) odd (they classified the \textit{semiclassical} spreads, which is equivalent by [12]), and to Lunardon–Polverino [9] for \( q \) even. In [11] it is proved that a spread \( S \) of \( H(3h) \) which is a translation spread with respect to a line is either hermitian or an \( S_{[9]} \). If \( q \) is even then by [4, Corollary 1] all translation spreads of \( H(q) \) are \( \mathbb{F}_q \)-translation spreads and, hence, they are classified. In summary, the following results hold:

(a) [4, Corollary 3] \( S \) is an \( \mathbb{F}_q \)-translation spread of \( H(q) \) with respect to a line if and only if \( \mathcal{S} \) is a line of \( PG(3, q) \) whose points belong to imaginary chords of \( \mathcal{C} \).

(b) [4, Theorem 5] \( S \) is a hermitian spread of \( H(q) \) if and only if \( \mathcal{S} \) is an imaginary chord of \( \mathcal{C} \).

(c) [4] If \( q \equiv 1 \pmod{3} \) and \( \mathcal{S} \) is an imaginary axis \( l \) of \( \mathcal{C} \), then \( \mathcal{S} \) defines an \( \mathbb{F}_q \)-translation spread \( S_l \) of \( H(q) \) with respect to a line. If \( q \) is odd, then \( S_l = S_{[9]} \), and if \( q \) is even, then this is the same as the spread \( S_l \) mentioned above.

As an application of Theorem 2.3, Corollary 2.4 and Results (a), (b) and (c) we have the following theorems:

**Theorem 3.1.** If \( q^n \equiv 1 \pmod{3} \), \( n > 2 \) and \((q, n)\) satisfies Property (K), then \( H(q^n) \) does not admit an \( \mathbb{F}_q \)-translation spread.

**Theorem 3.2.** If \( q^n \equiv 1 \pmod{3} \), \( q \) odd, \( n > 2 \) and \( q \geq 4n^2 - 8n + 2 \), then \( H(q^n) \) does not admit an \( \mathbb{F}_q \)-translation spread.

4. \( \mathbb{F}_q \)-linear sets

Let \( PG(r, q^n) = PG(V, \mathbb{F}_{q^n}) \) and let \( X \) be a set of points of \( PG(r, q^n) \). \( X \) is an \( \mathbb{F}_q \)-linear set of \( PG(r, q^n) \) if there is a subset \( W \) of \( V \) which is an \( \mathbb{F}_q \)-vector subspace of \( V \) such that \( X = \{ w \} : w \in W \}. \) If \( \dim_{\mathbb{F}_q} W = t \), we say that \( X \) has rank \( t \) (see [10]). If \( X \) is an \( \mathbb{F}_q \)-linear set of \( PG(r, q^n) \), then it is easy to see that \( |X| = 1 \pmod{q} \). Also, if \( L \) is a projective subspace of \( PG(r, q^n) \) such that \( X \cap L \neq \emptyset \), then \( X \cap L \) is an \( \mathbb{F}_q \)-linear set of \( L \) and hence \( |X \cap L| = 1 \pmod{q} \).

**Property 4.1.** Let \( X \) be an \( \mathbb{F}_q \)-linear set of \( PG(r, q^n) \) of rank \( 2n \). If there exists a point \( P \) of \( PG(r, q^n) \) such that \( \text{rank}_{\mathbb{F}_q}(X \cap P) = n \), then \( X \) is the union of \( s \) lines through \( P \) and \( s \equiv 1 \pmod{q} \).
Proof. Let \( Q \) be a point of \( X \) different from \( P \) and let \( l \) be the line through \( P \) and \( Q \). Since \( \text{rank}_{\mathbb{F}_q}(X \cap P) = n \) and \( \text{rank}_{\mathbb{F}_q}(X \cap Q) \geq n + 1 \), we have \( \text{rank}_{\mathbb{F}_q}(X \cap l) \geq n + 1 \). This implies that \( \text{rank}_{\mathbb{F}_q}(X \cap R) \geq n + 1 \) for each point \( R \in l \), i.e. \( l \subseteq X \). So, \( X \) is a union of a certain number of lines through \( P \).

Let \( X \) be an \( \mathbb{F}_q \)-linear set of rank \( 2n \) of \( PG(2, q^n) \) disjoint from an irreducible conic, say \( C \), of \( PG(2, q^n) \). Looking at these objects over the field \( \mathbb{F}_q \), the plane \( PG(3n - 1, q) \) becomes a \((3n - 1)-dimensional\) projective space, the conic \( C \) becomes a pseudo-oval \([15]\) and the \( \mathbb{F}_q \)-linear set \( X \) defines a \((2n - 1)-dimensional\) projective subspace of \( PG(3n - 1, q) \) skew to the elements of \( \mathcal{O} \). Dualizing in \( PG(3n - 1, q) \) with respect to the polarity \( \perp \) defined by \( \mathcal{O} \), from \( X \) we get an \((n - 1)-dimensional\) subspace of \( PG(3n - 1, q) \) skew to all the tangent spaces to \( \mathcal{O} \) and such a subspace defines an \( \mathbb{F}_q \)-linear set, say \( X' \), of \( PG(2, q^n) \) of rank \( n \) contained in the set of internal points of \( C \). If \((q, n)\) satisfies Property \((K)\), then \( X' \) is contained in a line \( l \) of \( PG(2, q^n) \), i.e. \( \text{rank}_{\mathbb{F}_q}(X' \cap l) = n \). This implies that \( \text{rank}_{\mathbb{F}_q}(X \cap l') = n \) and hence, by Property \( 4.1 \), \( X \) is a union of lines through the point \( l' \). Therefore we have proved the following:

**Proposition 4.2.** Let \( X \) be an \( \mathbb{F}_q \)-linear set of \( PG(2, q^n) \) of rank \( 2n \) disjoint from an irreducible conic \( C \) of \( PG(2, q^n) \). If the pair \((q, n)\) satisfies Property \((K)\), then there exists a point \( P \) of \( PG(2, q^n) \) such that \( \text{rank}_{\mathbb{F}_q}(X \cap P) = n \) and \( X \) is a union of lines through the point \( P \).

5. Preliminary results

The following theorem of Carlitz plays a crucial role in proving the main Theorem 2.3:

**Theorem 5.1** (Carlitz [5]). Let \( \chi \) be the multiplicative character of order two on \( \mathbb{F}_q \), where \( q = p^n \), with \( p \) an odd prime. Let \( f \) be a polynomial over \( \mathbb{F}_q \) such that

\[
\chi(f(x) - f(y)) = \lambda \chi(x - y)
\]

for all \( x, y \in \mathbb{F}_q \), where \( \lambda = \pm 1 \) is fixed. Then we have \( f(x) = ax^{j} + b \) for some \( j \) in the range \( 0 \leq j < n \), with \( a, b \in \mathbb{F}_q \) and \( \chi(a) = \lambda \).

Let \( f(x) \) be an \( \mathbb{F}_q \)-linear map from \( \mathbb{F}_q^n \) to itself. Then \( f(x) \) can be represented by a unique polynomial over \( \mathbb{F}_q^n \) of the form

\[
f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}.
\]

Such a polynomial is called a \( q \)-polynomial [7, Chapter 3]. A consequence of Theorem 5.1 on \( q \)-polynomials is the following.
Corollary 5.2. Let \( f(x) \) be a \( q \)-polynomial over \( \mathbb{F}_{q^n} \) and suppose that for a fixed choice of \( \lambda = \pm 1 \)

\[
\chi(f(x)) = \lambda \chi(x)
\]

for all \( x \in \mathbb{F}_{q^n} \). Then \( f(x) = ax^t \) for some \( 0 \leq t < n \) and \( a \in \mathbb{F}_{q^n} \) with \( \chi(a) = \lambda \).

The following lemmas will be used in the next section.

Lemma 5.3. Let \( g(y) \) be a \( q \)-polynomial of \( \mathbb{F}_{q^n}[y] \) which is not linear over \( \mathbb{F}_{q^n} \) and suppose that

\[
g^\sigma(y) + Ag(y) + By^\sigma + Cy = 0 \quad \forall y \in \mathbb{F}_{q^n}, \quad (\ast)
\]

\[
g^{\tau}(y) + A^\tau g(y) + B^\tau y^\tau + C^\tau y = 0 \quad \forall y \in \mathbb{F}_{q^n}, \quad (**)
\]

where \( \sigma = q^h, \tau = q^{h'} \), \( 0 < h, h' < n \), \( A, \tilde{A}, B, \tilde{B}, C, \tilde{C} \in \mathbb{F}_{q^n} \), and \( A, \tilde{A} \neq 0 \). Then, the following holds:

(i) If \( \sigma = \tau \), then either \( A = \tilde{A}, B = \tilde{B}, C = \tilde{C} \) or \( g(y) = [(\tilde{B} - B)/(A - \tilde{A})]y^\sigma + [(\tilde{C} - C)/(A - \tilde{A})]y \) and \( n = 2h \).

(ii) If \( \sigma \neq \tau \), then \( A^\tau \tilde{A} - A\tilde{A}^\sigma = 0, \tilde{B}A^\tau - C^\tau = 0 \) and \( \tilde{C}^\sigma - B\tilde{A}^\sigma = 0 \). Also, if \( \tau \pi \neq 1 \), then \( B^\tau = \tilde{B}^\sigma \) and \( \tilde{C}A^\tau - \tilde{A}^\sigma C = 0 \).

Proof. If \( \sigma = \tau \) then by subtracting \((**)\) from \((\ast)\) we get that either \( A = \tilde{A}, B = \tilde{B}, C = \tilde{C} \) or \( g(y) = [(\tilde{B} - B)/(A - \tilde{A})]y^\sigma + [(\tilde{C} - C)/(A - \tilde{A})]y \). In the latter case, substituting in \((\ast)\), since \( g(y) \) is not linear over \( \mathbb{F}_{q^n} \), we get \( \sigma^2 = 1 \), i.e. \( n = 2h \).

Now, suppose \( \sigma \neq \tau \). From equalities \((\ast)\) and \((**)\), we get

\[
A^\tau(\ast) - [(\ast) - (**\ast)] - \tilde{A}\tilde{A}(\ast) = 0,
\]

i.e.

\[
(A^\tau \tilde{A} - A\tilde{A}^\sigma)g(y) + (\tilde{B}A^\tau - C^\tau)y^\tau - (B^\tau - \tilde{B}^\sigma)y^{\sigma\tau} + (\tilde{C}^\sigma - B\tilde{A}^\sigma)y^\sigma + (\tilde{C}A^\tau - \tilde{A}^\sigma C)y = 0
\]

(1)

for each \( y \in \mathbb{F}_{q^n} \). If \( A^\tau \tilde{A} - A\tilde{A}^\sigma \neq 0 \), from (1) we obtain

\[
g(y) = ay + by^\sigma + cy^\tau + dy^{\sigma\tau},
\]

(2)

where \( a = (C\tilde{A}^\sigma - \tilde{C}A^\tau)/(A^\tau \tilde{A} - A\tilde{A}^\sigma), b = (B\tilde{A}^\tau - C^\tau)/(A^\tau \tilde{A} - A\tilde{A}^\sigma), c = (C^\tau - \tilde{B}A^\tau)/(A^\tau \tilde{A} - A\tilde{A}^\sigma) \) and \( d = (B^\tau - \tilde{B}^\sigma)/(A^\tau \tilde{A} - A\tilde{A}^\sigma) \). Substituting in \((\ast)\) and \((**)\), we get, respectively,

\[
d^\sigma y^{\sigma\tau} + (c^\sigma + Ad)y^{\sigma\tau} + b^\sigma y^\sigma + (a^\sigma + Ab + B)y^\sigma + Acy^\tau + (Aa + C)y = 0
\]

(3)

\[
d^\tau y^{\sigma\tau} + (b^\tau + \tilde{A}d)y^{\sigma\tau} + c^\tau y^\tau + (a^\tau + \tilde{A}c + \tilde{B})y^\tau + \tilde{A}by^\sigma + (\tilde{A}a + \tilde{C})y = 0.
\]

(4)

If \( \sigma\tau = 1 \), since \( \sigma \neq \tau \) and \( g(y) \) is not linear over \( \mathbb{F}_{q^n} \), from (3) we get \( \sigma^2 = \sigma^{-1} \). In this case, from (3) and (4) we obtain, respectively, \( Ac + b^\sigma = 0 \) and \( \tilde{A}b + c^\sigma = 0 \), which imply
If $l$ is an external line to $C$, we get $b = c = 0$, i.e. $g(y)$ is linear over $\mathbb{F}_q^\sigma$: a contradiction. Now, suppose $\sigma \tau \neq 1$. If $d = 0$, from (3) and (4) we get $b = c = 0$, i.e. $g(y)$ is linear over $\mathbb{F}_q^\sigma$: a contradiction. Hence $d \neq 0$. In this case, from (3) we have either $\sigma^2 = 1$ or $\sigma^2 \tau = 1$ and from (4) we have either $\tau^2 = 1$ or $\sigma^2 = 1$. From these conditions, since $\sigma \neq \tau$, we obtain either $\sigma^4 = 1$ and $\tau = \sigma^2$ or $\tau^4 = 1$ and $\sigma = \tau^2$. In the first case, equating the coefficients of (3) and (4) to 0, in particular we get $c^\sigma + Ad = 0, b^\sigma + Ad = 0$ and $b^\sigma + Ac = 0$ from which we have $\bar{A} = -A^\sigma + 1$, which implies $A^\sigma \bar{A} = A^{\sigma^2} = 0$: a contradiction. In the second case, in a similar way, we again get a contradiction. Hence, we always have $A^\sigma \bar{A} = A^{\sigma^2} = 0$ and, in this case, from (1) we easily get (ii). \qed

As an application of Corollary 5.2 we get the following:

**Lemma 5.4.** Let $q^n \equiv 1 \pmod{3}$, where $q$ is a power of a prime $p \neq 2$, and let $X$ be an $\mathbb{F}_q^\sigma$-linear set of $PG(2, q^n)$ of rank $n$ contained in the set of internal points of the irreducible conic $C$ with equation $-3Y_2^2 + 4Y_2Y_0 = 0$. Also, suppose that $X$ is contained in a line $l$ of $PG(2, q^n)$. Then the following holds:

1. If $l$ is an external line to $C$, then $X$ is a point.
2. If $X = \{(x, f(x), g(x)) : x \in \mathbb{F}_q^n \}$ and $(0, 0, 1) \in l$, then
   \[
   X = \left\{ \left( x, \gamma x, \frac{m}{4}x^\gamma + \frac{3}{4}x^2 \right) : x \in \mathbb{F}_q^n \right\},
   \]
   where $\gamma \in \mathbb{F}_q^n$, $\tau = q^{h'}$, $0 \leq h' < n$ and $m$ is a non-square in $\mathbb{F}_q^n$.
3. If $X = \{(f(x), \tilde{g}(x), x) : x \in \mathbb{F}_q^n \}$ and $(1, 0, 0) \in l$, then
   \[
   X = \left\{ \left( \frac{3}{4} \rho^2 x + \frac{m'}{4}x^\sigma, \rho x, x \right) : x \in \mathbb{F}_q^n \right\},
   \]
   where $\sigma = q^h$, $0 \leq h < n$, $\rho \in \mathbb{F}_q^n$ and $m'$ is a non-square in $\mathbb{F}_q^n$.
4. If $X = \{(f(x), \tilde{g}(x), x) : x \in \mathbb{F}_q^n \}$ and $(1, 0, 0) \notin l$, then
   \[
   X = \{(\alpha \tilde{g}(x) + \beta x, \tilde{g}(x), x) : x \in \mathbb{F}_q^n \},
   \]
   where $\alpha, \beta \in \mathbb{F}_q^n$, $\Delta = \alpha^2 + 3\beta$ is a non-zero square of $\mathbb{F}_q^n$ and $\tilde{g}(x)$ satisfies equality (*) of Lemma 5.3 with $A = (\alpha + \sqrt{\Delta})^{2\sigma+2}/3m'\sqrt{\Delta}^{\sigma+1}$, $B = -2(\alpha + \sqrt{\Delta})^\sigma/3$, $C = 2\beta(\alpha + \sqrt{\Delta})^{2\sigma+2}/3m'\sqrt{\Delta}^{\sigma+1}$, $\sigma = q^h$, $0 \leq h < n$ and $m'$ a non-square in $\mathbb{F}_q^n$.

**Proof.** If $l$ is an external line to $C$, then $X$ defines a dual semifield flock $\mathcal{F}$ of the quadratic cone $\mathcal{K}$ of $PG(3, q^n)$ whose planes all contain a common interior point of $\mathcal{K}$ (see, e.g., [8,16]). Then by [14, Section 1.5.6] $\mathcal{F}$ is a linear flock and hence $X$ is a point of $PG(2, q^n)$.

So, from now on, suppose that $l$ is a secant line of $C$. Since $X$ is an $\mathbb{F}_q$-linear set of rank $n$, we can write
\[
X = \{(H_0(x), H_1(x), H_2(x)) : x \in \mathbb{F}_q^n \},
\]
where $H_0(x)$, $H_1(x)$ and $H_2(x)$ are $\mathbb{F}_q$-linear operators on $\mathbb{F}_{q^n}$. Also, since $X$ is a set of internal points of $C$ and $-3$ is a square in $\mathbb{F}_{q^n}$, we have that $-3H_1(x)^2 + 4H_0(x)H_2(x)$ is a non-square for all $x \neq 0$. This implies that $H_0(x)$ and $H_2(x)$ are bijective maps and, hence, we can write either $X = \{(x, f(x), g(x)) : x \in \mathbb{F}_{q^n}\}$ or $X = \{(\bar{f}(x), \bar{g}(x), x) : x \in \mathbb{F}_{q^n}\}$ for suitable $\mathbb{F}_q$-linear operators $f, g, \bar{f}$ and $\bar{g}$ on $\mathbb{F}_{q^n}$. If $X = \{(x, f(x), g(x)) : x \in \mathbb{F}_{q^n}\}$ and $(0, 0, 1) \in l$, then $l$ has equation $Y_0 = \gamma Y_1$, where $\gamma \in \mathbb{F}_{q^n}$, and hence $f(x) = \gamma x$ and $-\gamma^2 x^2 + 4xg(x)$ is a non-square for all $x \in \mathbb{F}_{q^n}$, i.e.

$$\chi(x) \chi(-3\gamma^2 x + 4g(x)) = \frac{\chi(-3\gamma^2 x + 4g(x))}{\chi(x)} = -1$$

for each $x \in \mathbb{F}_{q^n}$. Applying Corollary 5.2, we get $g(x) = (m/4)x^2 + (3/4)\gamma^2 x$ where $\tau = q^{h'}$, $0 \leq h' < n$, and $m$ is a non-square in $\mathbb{F}_{q^n}$. If $X = \{(\bar{f}(x), \bar{g}(x), x) : x \in \mathbb{F}_{q^n}\}$ and $(1, 0, 0) \in l$, using the same arguments as in the previous case we get (3). Finally, suppose that $X = \{(\bar{f}(x), \bar{g}(x), x) : x \in \mathbb{F}_{q^n}\}$ and $(1, 0, 0) \notin l$. In this case, $l$ has equation $Y_0 = \alpha Y_1 + \beta Y_2$ where $\alpha, \beta \in \mathbb{F}_{q^n}$ and $\bar{f}(x) = \alpha \bar{g}(x) + \beta x$. Since $l$ is a secant line of $C$, $A = \alpha^2 + 3\beta$ is a non-zero square in $\mathbb{F}_{q^n}$ and $l \cap C = \{P_1, P_2\}$, where $P_1 = ((\alpha + \sqrt{A}), 2(\alpha + \sqrt{A}), 3)$ and $P_2 = ((\alpha - \sqrt{A}), 2(\alpha - \sqrt{A}), 3)$. The linear transformation $\omega_{\bar{c}}$ of $PG(2, q^n)$, mapping the point $(\gamma_0, \gamma_1, \gamma_2)$ into the point $(\gamma_0, 2\gamma_0 + \gamma_1, 3\gamma_0 + 3\gamma_1 + \gamma_2)$, fixes the conic $C$ for each $c \in \mathbb{F}_{q^n}$ and, if $\bar{c} = \bar{c} = -1/(\alpha + \sqrt{A})$, then $P_{\bar{c}}^{\omega_{\bar{c}}} = (1, 0, 0)$. So, $X_{\bar{c}}$ is an $\mathbb{F}_q$-linear set of rank $n$ of internal points of $C$ contained in the line $l_{\bar{c}}^{\omega_{\bar{c}}}$ and $(1, 0, 0) \in l_{\bar{c}}^{\omega_{\bar{c}}}$. Hence, if $X_{\bar{c}} = \{(F(x'), G(x'), x') : x' \in \mathbb{F}_{q^n}\}$, by Case (3) we get $F(x') = (3/4)\rho^2 x' + (m'/4)x'^{\sigma}$ and $G(x') = \rho x'$, where $\sigma = q^{h}, 0 \leq h < n, \rho \in \mathbb{F}_{q^n}$ and $m'$ is a non-square in $\mathbb{F}_{q^n}$. Applying $\omega_{\bar{c}}$ to $l$ and $X$, respectively, we obtain $\rho = -\beta/\sqrt{A}$ and

$$F(x') = \frac{3}{4}\rho^2 x' + \frac{m'}{4}x'^{\sigma} = \alpha \bar{g}(x) + \beta x,$$

$$G(x') = \rho x' = (2\epsilon \alpha + 1)\bar{g}(x) + 2\epsilon \beta x,$$

$$x' = (3\epsilon^2 - \epsilon + 3\epsilon \beta + 1)x.$$

From the first and the third equations of the above system we get

$$\bar{g}^{\sigma}(x) + A \bar{g}(x) + B x^{\sigma} + C x = 0,$$

(5)

for each $x \in \mathbb{F}_{q^n}$, where $A = (\alpha + \sqrt{A})^{\sigma} + 2/3m'\sqrt{A}^{\sigma+1}$, $B = -2(\alpha + \sqrt{A})^{\sigma}/3, C = 2\beta(\alpha + \sqrt{A})^{\sigma+1}/3m'\sqrt{A}^{\sigma+1}$.

If $A = 0$, then $\alpha + \sqrt{A} = 0$ and this implies $\alpha = \beta = 0$: a contradiction. So, $A \neq 0$ and hence $\bar{g}(x)$ satisfies equality (*) of Lemma 5.3.

**Remark 5.5.** Note that, in Cases (2), (3) and (4) of Lemma 5.4 if either $\sigma = 1$ or $\tau = 1$ or $\bar{g}(y)$ is linear over $\mathbb{F}_{q^n}$, then $X$ is a point of $PG(2, q^n)$.

**Lemma 5.6.** Let $h(y)$ and $k(y)$ be $q$-polynomials over $\mathbb{F}_{q^n}$ and suppose that $h(y)$ is a permutation polynomial. Let

$$C = \{(x, ax + h(y), bx^k + cx + k(y)) : x, y \in \mathbb{F}_{q^n}\}$$
be an $\mathbb{F}_q$-linear set of $\text{PG}(2, q^n)$ of rank $2n$ with $a, b, c \in \mathbb{F}_{q^n}$, $b \neq 0$, and $\tau = q^{h'}, 0 < h' < n$. Suppose that there exists a point $R$ of $\text{PG}(2, q^n)$ such that $\text{rank}_{\mathbb{F}_q}(R \cap \mathcal{C}) = n$. Then there exists $(x_0, y_0) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n})^*$ such that $h(y)$ and $k(y)$ satisfy the following identity:

$$k(y) = -\frac{bx_0^5}{h(y_0)}h(y)^5 + \frac{bx_0^5 + k(y_0)}{h(y_0)}h(y).$$

(6)

**Proof.** Since $\text{rank}_{\mathbb{F}_q}(R \cap \mathcal{C}) = n$, there exists $(x_0, y_0) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n})^*$ such that $R = (x_0, ax_0 + h(y_0), bx_0^5 + cx_0 + k(y_0))$ and

$$\lambda x_0 = x,$n

$$\lambda(ax_0 + h(y_0)) = ax + h(y),$$n

$$\lambda(bx_0^5 + cx_0 + k(y_0)) = bx^5 + cx + k(y),$$n

$
\ast$

$$\lambda x_0 = x,$n

$$\lambda h(y_0) = h(y),$$n

$$\lambda(bx_0^5 + k(y_0)) = bx^5 + k(y),$$

(7)

for each $\lambda \in \mathbb{F}_{q^n}$. If $h(y_0) = 0$, then $y_0 = 0, y = 0$ and from (7) we get $\lambda = \lambda^5$ for each $\lambda \in \mathbb{F}_{q^n}$; a contradiction since $\tau \neq 1$. Hence $h(y_0) \neq 0$ and from the first and second equations of (7) we get $x = (x_0/h(y_0))h(y)$. Now, substituting in the third equation we obtain identity (6). \[\Box\]

6. **Proof of Theorem 2.3**

Fix the twisted cubic of $\text{PG}(3, q^n)$, $q = p^r, p$ prime, in the canonical form $\mathcal{C} = \{P_t = (r^3, r^2, r, 1) : t \in \mathbb{F}_{q^n}\} \cup \{P_{\infty} = (1, 0, 0, 0)\}$. Let $\pi_t$ and $l_t$ be, respectively, the osculating plane and the tangent line to $\mathcal{C}$ at the point $P_t$ with $t \in \mathbb{F}_{q^n} \cup \{\infty\}$. The points on the tangents to $\mathcal{C}$ form a quartic surface $\Omega$ with equation

$$F(X_0, X_1, X_2, X_3) = X_2^3X_0^2 - 3X_2^2X_1^2 - 6X_0X_1X_2X_3 + 4X_3^2X_1^2 + 4X_2^2X_0 = 0$$

(see, e.g., [6, p. 240]). For each osculating plane $\pi_t$, the curve $\Omega \cap \pi_t$ of degree four contains $l_t$ with multiplicity two and a conic $C_t$ through the point $P_t$.

A point $P$ of $\text{PG}(3, q^n)$, $p \neq 2$, belongs to an imaginary chord of $\mathcal{C}$ if and only if $P$ lies on a line with coordinate vector $(x_1^2, x_1x_2, x_1^2 - x_2, x_2, -x_1, 1)$ where $x_1, x_2 \in \mathbb{F}_{q^n}$ and $x_1^2 - 4x_2$ is a non-square in $\mathbb{F}_{q^n}$ (see [6, Section 21, p. 231]). Now, by Lemma 15.2.3 of [6], we easily get that $P = (a_0, a_1, a_2, a_3)$ belongs to an imaginary chord of $\mathcal{C}$ if and only if $F(a_0, a_1, a_2, a_3)$ is a non-square in $\mathbb{F}_{q^n}$.

Let $\mathcal{S}$ be an $\mathbb{F}_q$-linear set of $\text{PG}(3, q^n)$ of rank $2n$ whose points belong to imaginary chords of $\mathcal{C}$ and suppose that $\mathbb{F}_q$ is the maximal subfield of $\mathbb{F}_{q^n}$ with respect to which $\mathcal{S}$ is a linear subset. If $(a_0, a_1, a_2, a_3)$ and $(a_0, a_1', a_2', a_3)$ are distinct points of $\mathcal{S}$, then $(0, a_1 - a_1', a_2 - a_2', 0) \in \mathcal{S}$ and hence $F(0, a_1 - a_1', a_2 - a_2', 0) = -3(a_2 - a_2')^2(a_1 - a_1')^2$ is a non-square in $\mathbb{F}_{q^n}$. Therefore, if $-3$ is a square in $\mathbb{F}_{q^n}$, i.e. if $q^n \equiv 1 \pmod{3}$, there are no distinct points of $\mathcal{S}$ of type $(a_0, a_1, a_2, a_3)$ and $(a_0, a_1', a_2', a_3)$. This implies that,
if \( q^n \equiv 1 \pmod{3} \), there exist two \( \mathbb{F}_q \)-linear functions \( f(x, y), g(x, y) : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \) such that

\[
\mathcal{S} = \{(x, f(x, y), g(x, y), y) : (x, y) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n})^*\}.
\]

Note that \( \mathbb{F}_q \) is the maximal subfield of \( \mathbb{F}_{q^n} \) with respect to which \( f \) and \( g \) are both linear. Also, if \( p \neq 2 \), since the points of \( \mathcal{S} \) belong to imaginary chords of \( \mathcal{C} \), we have that

\[
F(x, f(x, y), g(x, y), y) \text{ is a non-square for all } (x, y) \neq (0, 0).
\]

Let \( \mathcal{S}_\infty = \mathcal{S} \cap \pi_\infty \) and let \( f_1(x) = f(x, 0) \) and \( g_1(x) = g(x, 0) \). Since \( \pi_\infty \) has equation \( X_3 = 0 \), we can write

\[
\mathcal{S}_\infty = \{(x, f_1(x), g_1(x), 0) : x \in \mathbb{F}_{q^n}^*\}.
\]

**Proposition 6.1.** If \( q^n \equiv 1 \pmod{3} \) and \((q, n)\) satisfies Property (K), then either \( S_\infty \) is a point or, without loss of generality, we can suppose

\[
\mathcal{S}_\infty = \left\{ \left( x, \gamma x, \frac{m}{4} x^2 + \frac{3}{4} \gamma^2 x, 0 \right) : x \in \mathbb{F}_{q^n}^* \right\},
\]

where \( \gamma \in \mathbb{F}_{q^n}, \tau = q^{h'}, 0 \leq h' < n \) and \( m \) is a non-square in \( \mathbb{F}_{q^n} \).

**Proof.** The conic \( C_\infty \) has equations \(-3X_1^2 + 4X_0X_2 = X_3 = 0\), and hence, since \( p \neq 2, 3 \), \( C_\infty \) is an irreducible conic of \( \pi_\infty \). From (8) we get that \(-3f_1^2(x) + 4xg_1(x)\) is a non-square for all \( x \in \mathbb{F}_{q^n}^* \) and, since \( q^n \equiv 1 \pmod{3} \), the above condition implies that \( \mathcal{S}_\infty \) is an \( \mathbb{F}_q \)-linear set of rank \( n \) of internal points of \( C_\infty \). By Property (K), \( \mathcal{S}_\infty \) is contained in a line \( r \) of \( \pi_\infty \) and, applying Lemma 5.4, we have that either \( \mathcal{S}_\infty \) is a point or \( r \) is a secant line to \( C_\infty \). In this case, since the stabilizer \( G_{P_\infty} \) of the full automorphism group \( G \) of \( \mathcal{C} \) acts transitively on \( C_\infty \setminus \{P_\infty\} \), we can suppose, without loss of generality, that the point \((0, 0, 1, 0)\) of \( C_\infty \) belongs to the line \( r \). Hence, by (2) of Lemma 5.4, we can write

\[
\mathcal{S}_\infty = \left\{ \left( x, \gamma x, \frac{m}{4} x^2 + \frac{3}{4} \gamma^2 x, 0 \right) : x \in \mathbb{F}_{q^n}^* \right\},
\]

where \( \gamma \in \mathbb{F}_{q^n}, \tau = q^{h'}, 0 \leq h' < n \) and \( m \) is a non-square in \( \mathbb{F}_{q^n} \). \( \square \)

Let \( \mathcal{S}_0 = \mathcal{S} \cap \pi_0 \) and let \( f_2(y) = f(0, y) \) and \( g_2(y) = g(0, y) \). Since \( \pi_0 \) has equation \( X_0 = 0 \), we can write

\[
\mathcal{S}_0 = \{(0, f_2(y), g_2(y), y) : y \in \mathbb{F}_{q^n}^*\}.
\]

**Proposition 6.2.** If \( q^n \equiv 1 \pmod{3} \) and \((q, n)\) satisfies Property (K), then one of the following occurs:

1. \( \mathcal{S}_0 \) is a point, i.e. \( f_2(y) \) and \( g_2(y) \) are linear over \( \mathbb{F}_{q^n} \).
2. \( \mathcal{S}_0 = \{(0, (3/4)\rho^2 y + (m'/4)y^\sigma, \rho y, y) : y \in \mathbb{F}_{q^n}^*\} \) where \( \sigma = q^{h}, 0 \leq h < n, \rho \in \mathbb{F}_{q^n}^* \) and \( m' \) is a non-square in \( \mathbb{F}_{q^n} \).
(3) \( \mathcal{S}_0 = \{(0, \alpha g_2(y) + \beta y, g_2(y), y) : y \in \mathbb{F}_{q^n}\} \), where \( \Delta = x^2 + 3\beta \) is a non-zero square of \( \mathbb{F}_{q^n} \) and \( g_2(y) \) satisfies equality (*) of Lemma 5.3 with \( A = (x + \sqrt{\Delta})^{2\sigma+2}/3m'=\sqrt{\Delta}^{\sigma+1} \), \( B = -2(x + \sqrt{\Delta})^\sigma/3 \), \( C = 2\beta(x + \sqrt{\Delta})^{2\sigma+1}/3m'=\sqrt{\Delta}^{\sigma+1} \), \( \sigma = q^h, 0 \leq h < n \) and \( m' \) a non-square in \( \mathbb{F}_{q^n} \). 

Proof. The conic \( C_0 \) has equations \( -3X_2^2 + 4X_3X_1 = X_0 = 0 \), and hence, since \( p \neq 2, 3 \), \( C_0 \) is an irreducible conic of \( \pi_0 \). By (8) we get that

\[
-3g_2^2(y) + 4yf_2(y) \text{ is a non-square for all } y \in \mathbb{F}_{q^n}.
\]

As in the previous case, since \( q^n \equiv 1 \) (mod 3), from the above condition we get that \( \mathcal{S}_0 \) is an \( \mathbb{F}_q \)-linear set of rank \( n \) of internal points of \( C_0 \). Hence, by Property (K), \( \mathcal{S}_0 \) is contained in a line \( \ell \) of \( \pi_0 \). Now, applying Lemma 5.4 to the \( \mathbb{F}_q \)-linear set \( \mathcal{S}_0 \), we obtain (1), (2) and (3). \( \Box \)

If \( \mathcal{S}_\infty \) (resp. \( \mathcal{S}_0 \)) is a point, then, by Property 4.1, \( \mathcal{S} \) is union of \( s \) lines through \( \mathcal{S}_\infty \) (resp. \( \mathcal{S}_0 \)) and \( s \equiv 1 \) (mod \( q \)). By Theorem 2.1, each of these lines is either an imaginary chord or an imaginary axis. But, since every point not belonging to \( \mathcal{C} \) lies on exactly one chord and exactly one axis, we have \( s = 1 \). Hence, if \( q^n \equiv 1 \) (mod 3), \( (q, n) \) satisfies Property (K) and \( \mathcal{S} \) is not a line, then from Propositions 6.1 and 6.2 we have that \( \mathcal{S} \) is one of the following:

(a) \( \mathcal{S} = \{(x, yx + (3/4)y^2 + (m'/4)y^2, (m'/4)x^2 + (3/4)y^2x + \rho y, y) : x, y \in \mathbb{F}_{q^n}\} \),

(b) \( \mathcal{S} = \{(x, yx + \alpha g_2(y) + \beta y, (m'/4)x^2 + (3/4)y^2x + g_2(y), y) : x, y \in \mathbb{F}_{q^n}\} \),

where \( g_2(y) \) is a polynomial satisfying equality (*) of Lemma 5.3. Also, since \( \mathcal{S} \) is not a line, \( \mathcal{S}_0 \) and \( \mathcal{S}_\infty \) are not points and hence \( g_2(y) \) is not linear on \( \mathbb{F}_{q^n} \) and \( \sigma, \tau \neq 1 \) (see Remark 5.5).

Projecting \( \mathcal{S} \) and \( \mathcal{C} \) from the point \( P_t = (t^2, t, 1) \) onto the plane \( \pi_\infty \) we get, respectively, the \( \mathbb{F}_q \)-linear set of rank 2n

\[
\mathcal{C}_t = \{(x - t^3y, f(x, y) - t^2y, g(x, y) - ty, 0) : x, y \in \mathbb{F}_{q^n}\}
\]

and the irreducible conic \( \Gamma_t \) with equations \( t^2X_2^2 + X_1^2 - tX_1X_2 - X_0X_2 = X_3 = 0 \). Since the points of \( \mathcal{S} \) belong to imaginary chords of \( \mathcal{C} \), the \( \mathbb{F}_q \)-linear set \( \mathcal{C}_t \) and the irreducible conic \( \Gamma_t \) are disjoint for each \( t \in \mathbb{F}_{q^n} \).

If the pair \((q, n)\) satisfies Property (K), then by Proposition 4.2 for each \( t \in \mathbb{F}_{q^n} \) there exists a point \( R_t \in \pi_\infty \) such that \( \mathbb{F}_q(\Gamma_t \cap \mathcal{C}_t) = n \). By using this condition for suitable values of \( t \), we can exclude Cases (a) and (b).

Proposition 6.3. If \( q^n \equiv 1 \) (mod 3) and \((q, n)\) satisfies Property (K) with \( n > 2 \), then Case (a) does not occur.

Proof. Suppose Case (a) occurs and let \( t = 0 \). In this case, we can write

\[
\mathcal{C}_0 = \left\{(x, yx + \frac{3}{4}y^2x + \frac{m'}{4}y^2, \frac{m}{4}x^2 + \frac{3}{4}y^2x + \rho y, 0) : x, y \in \mathbb{F}_{q^n}\right\}.
\]
Since \( \mathbb{F}_q \) is the maximal subfield with respect to which \( f(x, y) \) and \( g(x, y) \) are both linear, we have \( g.c.d.(n, h, h') = 1 \). Also, as previously noted, by Proposition 4.2 there exists a point \( R_0 \in \pi_{\infty} \) such that \( \text{rank}_{\mathbb{F}_q}(R_0 \cap \mathcal{O}_0) = n \). Therefore, since \( f_2(y) = (3/4)x^2y + (m'/4)y^2 \) is a permutation polynomial, we can apply Lemma 5.6 to the \( \mathbb{F}_q \)-linear set \( \mathcal{O}_0 \), i.e. there exists \( (x_0, y_0) \in (\mathbb{F}_q^n \times \mathbb{F}_q^n)^* \) such that

\[
\rho y = -\frac{m}{4} \frac{x_0^2}{f_2(y_0)} \left( \frac{3}{4} \rho^{x_2} y^2 + \frac{m'}{4} y^{x_2} \right) + \frac{m}{4} x_0^2 + \rho y_0 f_2(y_0) \left( \frac{3}{4} \rho^{y_2} y + \frac{m'}{4} y^2 \right) \tag{10}
\]

for each \( y \in \mathbb{F}_q^n \). If \( x_0 \neq 0 \), from (10) we get \( \sigma \tau = 1 \) and \( \sigma = \tau \), i.e. \( n = 2 \) since \( g.c.d.(n, h, h') = 1 \). Hence, if \( n > 2 \), then \( x_0 = 0 \) and from (10) it follows \( \rho = 0 \). In this case, as \( \mathcal{O}_0 \cap \mathcal{O}_0 = \emptyset \), we have

\[
m^2 = \frac{16}{16} y^2 + \frac{m'}{2} xy - \left( \frac{m}{4} x^{\tau + 1} - \frac{y^2}{4} x^2 \right) \neq 0
\]

for each \( x, y \in \mathbb{F}_q^n \) with \( (x, y) \neq (0, 0) \). This implies that \( (m^2/16)x^{\tau + 1} + (3/2)2x^2/16) \) is a non-square for all \( x \in \mathbb{F}_q^n \) and, from Corollary 5.2, we have \( \gamma = 0 \). Therefore, \( \rho = \gamma = 0 \). Now, let \( \bar{t} \) be an element of \( \mathbb{F}_q^n \) such that \( \bar{t}^{\tau + 1} \neq m'/m \) and \( \bar{t}^{\tau - 1} \neq 16/mm' \) and let \( z = x - \bar{t}^2y \); we can write

\[
\mathcal{O}_{\bar{t}} = \left\{ \left( z, x, y, \frac{m'}{4} x^{\tau + 1} - \frac{y^2}{4} x^2 \bar{t}y, 0 \right) : z, y \in \mathbb{F}_q^n \right\}
\]

and, applying Lemma 5.6 to \( \mathcal{O}_{\bar{t}} \), there exists \( (z_0, y_0) \in (\mathbb{F}_q^n \times \mathbb{F}_q^n)^* \) such that

\[
\frac{m}{4} \frac{x^{\tau + 1}}{f_2(y_0)} - \frac{y^2}{4} x^2 + g(y) - \bar{t}y = \frac{m}{4} \frac{z_0^2}{h(y_0)} \left( \frac{m'}{4} y^{\tau + 1} - \frac{y^2}{4} x^2 \bar{t}y, 0 \right) + \frac{4h(y_0)}{m} \left( \frac{m'}{4} y^{\tau + 1} - \frac{y^2}{4} x^2 \bar{t}y \right) \tag{11}
\]

for each \( y \in \mathbb{F}_q^n \), where \( h(y) = (m'/4)y_{\sigma} - \bar{t}^2 y \) and \( k(y) = (m/4)\bar{t}^3 y_{\sigma} - \bar{t}y \). If \( z_0 = 0 \), we get \( \sigma = \tau \) and \( \bar{t}^{\tau + 1} = m'/m \), which contradicts our assumption. If \( z_0 \neq 0 \), we obtain \( \sigma \tau = 1 \). If \( \sigma = \tau \), then \( n = 2 \). If \( \sigma \neq \tau \), then from (11) we get \( \bar{t}^{\tau - 1} = 16/m^2 \); a contradiction. Hence, Case (a) does not occur. \( \square \)

**Proposition 6.4.** If \( q^n \equiv 1 \) (mod 3) and \( (q, n) \) satisfies Property (K) with \( n > 2 \), then Case (b) does not occur.

**Proof.** Suppose Case (b) occurs. Then

\[
\mathcal{O}_{\bar{t}} = \left\{ \left( (x - \bar{t}^3 y, \gamma x + xg_2(y) + \beta y - \bar{t}^2 y, \frac{m}{4} x^{\tau + 1} + \frac{3}{4} \bar{t}^2 x + g_2(y) - \bar{t}y, 0 \right) \ : x, y \in \mathbb{F}_q^n \right\}
\]

From (9) we easily get that \( f_2(y) = xg_2(y) + \beta y \) is a permutation polynomial. So we can apply Lemma 5.6 to the \( \mathbb{F}_q \)-linear set \( \mathcal{O}_0 \), i.e. there exists \( (x_0, y_0) \in (\mathbb{F}_q^n \times \mathbb{F}_q^n)^* \) such that

\[
g_2(y) = -\frac{m}{4} \frac{x_0^2}{f_2(y_0)} \left( xg_2(y) + \beta y \right)^2 + \left( \frac{m}{4} x_0^2 + \frac{4g_2(y_0)}{f_2(y_0)} \right) \left( xg_2(y) + \beta y \right)
\]
Applying Lemma 5.6 to contradicting our assumption. Hence we get which we get for each $\bar{q}$, where

$$g_2(y) + \bar{A} g_2(y) + \bar{B} y^2 + \bar{C} y = 0,$$

(12)

where $\bar{A} = [(4\beta y_0 - m\bar{x}y_0)/(m\bar{x}^2)]f_2(y_0)^{\gamma - 1}$, $\bar{B} = (\beta/x)^{\gamma}$, $\bar{C} = -(m\bar{x}^2 + 4g_2(y_0)) /m\bar{x}^2].f_2(y_0)^{\gamma - 1}$. If $\tilde{A} = 0$, then $g_2(y) = -\bar{B}^{\gamma - 1} y - \bar{C}^{\gamma - 1} y^{\gamma - 1}$. As $g_2(y)$ satisfies (*) of Lemma 5.3, we get that either $g_2(y)$ is linear on $\mathbb{F}_q^n$ or $n = 2$. So $\tilde{A} \neq 0$ and we can apply Lemma 5.3 to the polynomial $g_2(y)$. Since $\bar{B}^\gamma \neq \bar{B}^2$, if Case (i) of Lemma 5.3 occurs, then $g_2(y) = [(\bar{B} - B)/(A - \bar{A})]y^\gamma + [(\bar{C} - C)/(A - \bar{A})]y$ and $n = 2h = 2h'$. Therefore, we have $g.c.d.(h, h', n) = 1$ and hence $n = 2$: a contradiction. If Case (ii) of Lemma 5.3 occurs, then $\bar{B}A^\gamma - C^\gamma = 0$ from which we get $\beta = 0$. In this case, since $\mathcal{O}_0$ and $\mathcal{I}_0$ are disjoint, we can write

$$x^2 g_2(y)^2 + (2\gamma - 1)x g_2(y) + \frac{x^2}{4} x^2 - \frac{m}{4} x^{\gamma + 1} \neq 0$$

for each $x, y \in \mathbb{F}_q^n$. Since $g_2(y)$ is a permutation polynomial, this equality implies that $x^2(3\gamma^2 x^2 - 4\gamma x + 1) + x^2 mx^{\gamma + 1}$ is a non-square for all $x \in \mathbb{F}_q^n$. By Corollary 5.2 we have $3\gamma^2 x^2 - 4\gamma x + 1 = 0$ and hence $x^\gamma \in \{1, 1/3\}$. In particular, $\gamma \neq 0$. Now, let $t = \gamma^{-1}$ and $z = x - \gamma^{-3} y$; then

$$\mathcal{O}_{\gamma^{-1}} = \left\{ (z, \gamma z + \gamma z g_2(y), \frac{m z}{4} z^t + \frac{3}{4} \gamma z^t + \frac{m}{4} \gamma z^t y^t - \frac{1}{4} \gamma y + g_2(y), 0) : y, z \in \mathbb{F}_q^n \right\}. $$

Applying Lemma 5.6 to $\mathcal{O}_{\gamma^{-1}}$, we get that there exists $(z_0, y_0) \in (\mathbb{F}_q^n \times \mathbb{F}_q^n)^*$ such that

$$\frac{m}{4\gamma^2} y^t - \frac{1}{4\gamma} y + g_2(y) = -\frac{m}{4} \frac{z_0}{h(y_0)^{\gamma}} x^t g_2(y) + \left( \frac{m z_0^t + 4k(y_0)}{4h(y_0)^{\gamma}} \right) z g_2(y)$$

for each $y \in \mathbb{F}_q^n$, where $h(y) = \gamma z_2(y) + (m/4\gamma^3) y^t - (1/4\gamma) y + \gamma g_2(y)$. If $z_0 = 0$, then $g_2(y)(1 - (k(y_0)/h(y_0)) z) = (1/4\gamma) y - (1/4m\gamma^3) y^t$ and substituting in (*) we get $n = 2$: a contradiction. If $z_0 \neq 0$, we can write

$$g_2(y)^t + \bar{A} g_2(y) + \bar{B} y^t + \bar{C} y = 0$$

(13)

for each $y \in \mathbb{F}_q^n$, where $\bar{A} = (4h(y_0)^{\gamma - 1}/m\bar{z}_0^t) [h(y_0) - \gamma((m/4)z_0^t + k(y_0))]$, $\bar{B} = (h(y_0)^{\gamma - 1}/m\gamma z_0^t) z_0^t$, $\bar{C} = (h(y_0)^{\gamma - 1}/m\gamma z_0^t) z_0^t$. If $\bar{A} = 0$ (similar to the case $\bar{A} = 0$), we get $n = 2$, contradicting our assumption. Hence $\bar{A} \neq 0$ and we can apply Lemma 5.3 to the polynomial $g_2(y)$. Since $C = 0$ and $\bar{C} \neq 0$, in our hypotheses, Case (ii) of Lemma 5.3 occurs, from which we get $\bar{B} = 0$, i.e. $h(y_0) = 0$: a contradiction. This proves that Case (b) does not occur. \(\square\)

From the previous results Theorem 2.3 follows.
References