Available online at www.sciencedirect.com

Discrete Mathematics 296 (2005) 129–142

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

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

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 $\mathscr{S}$ of $PG(3, q^n)$ of rank $2n$ whose points belong to imaginary chords of a twisted cubic $\mathscr{C}$ 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 $q \equiv 1 \pmod 3$, then each imaginary axis of $\mathscr{C}$ is an $\mathbb{F}_q$-linear set of rank 2 of $PG(3, q)$ whose points belong to imaginary chords of a twisted cubic $\mathscr{C}$ of $PG(3, q)$, obtaining new families of examples of $\mathbb{F}_q$-translation spreads of $H(q)$ for q even.

☆ Work supported by National Research Project *Strutture geometriche, Combinatoria e loro applicazioni* of the Italian *Ministero dell'Università e della Ricerca Scientifica*.

E-mail addresses: giovanna.bonoli@unina2.it (G. Bonoli), opolveri@unina.it, olga.polverino@unina2.it (O. Polverino).

0012-365X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2005.03.010

Next, in [9] Lunardon and Polverino show that a line l of $PG(3,q)$ whose points belong to imaginary chords of a twisted cubic $\mathscr{C}$ of $PG(3,q)$ either is an imaginary chord of $\mathscr{C}$ or $q \equiv 1 \pmod 3$ and l is an imaginary axis of $\mathscr{C}$. 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, $q \geqslant 4n^2 - 8n + 2$ and $n > 2$, then an $\mathbb{F}_q$-linear subset of $PG(3,q^n)$ of rank $2n$ of $PG(3,q^n)$ whose points belong to imaginary chords of a twisted cubic $\mathscr{C}$ of $PG(3,q^n)$ 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, $q \geqslant 4n^2 - 8n + 2$ 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 $\mathscr{C}$ of $PG(3,q)$, $q = p^r$, p prime, can be described as

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

where $f_0(t), \ldots, f_3(t)$ are linearly independent cubic polynomials over $\mathbb{F}_q$. Let $\bar{\mathscr{C}}$ be the twisted cubic of $PG(3,\mathbb{F})$ defined by $\mathscr{C}$, where $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_q$. A line of $PG(3,q)$ is a *chord* of $\mathscr{C}$ if it contains two points of $\bar{\mathscr{C}}$. There are three possibilities: the two points are distinct and belong to $\mathscr{C}$, 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 $\mathscr{C}$ lies on exactly one chord (see e.g. [6, Theorem 21.1.9]). If $p \neq 3$, the tangents to $\mathscr{C}$ are self-polar lines of a non-singular symplectic polarity ω of $PG(3,q)$. An *axis* of $\mathscr{C}$ is a line l of $PG(3,q)$ whose polar line with respect to ω is a chord. We say that l is a real axis or an imaginary axis when l^ω 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 $PG(3,q)$ whose points belong to imaginary chords of $\mathscr{C}$, 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 $PG(r,q^n) = PG(V, \mathbb{F}_{q^n})$ of *rank k* is a set of points of $PG(r,q^n)$ 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 $PG(2,q^n)$ 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 $PG(2,q^n)$, 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 2.2 (*Ball et al.* [2]). *Let (q, n) be a pair of positive integers with $q = p^h$, p odd prime. If $q \geqslant 4n^2 - 8n + 2$, 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 $\mathscr{S}$ be an $\mathbb{F}_q$-linear set of $PG(3, q^n)$ of rank $2n$ whose points belong to imaginary chords of $\mathscr{C}$. If $q^n \equiv 1 \pmod 3$ and the pair (q, n) satisfies Property (K) with $n > 2$, then $\mathscr{S}$ is an $\mathbb{F}_{q^n}$-linear set and either $\mathscr{S}$ is an imaginary chord or $\mathscr{S}$ is an imaginary axis of $\mathscr{C}$.*

From Theorems 2.2 and 2.3 we get the following corollary.

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

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 $X_3^2 = X_0X_4 + X_1X_5 + X_2X_6$. 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* 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 $\mathbb{S}$ 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 $\mathbb{S}$ and acts transitively on the lines of $\mathbb{S}$ 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 $\mathbb{S}$ with respect to a line of $H(q)$ a subfield of $\mathbb{F}_q$, called the *kernel* of $\mathbb{S}$.

Using the construction of $H(q^n)$ as a coset geometry (see [1]) in [4] it is proved that each translation spread $\mathbb{S}$ with respect to a line of $H(q^n)$ with kernel $\mathbb{F}_q$ defines an $\mathbb{F}_q$-linear set $\mathscr{S}$ of $PG(3, q^n)$ of rank $2n$ whose points belong to imaginary chords of the twisted cubic $\mathscr{C}$ of $PG(3, q^n)$ having $\mathbb{F}_q$ as the maximal subfield of linearity, and conversely. If $\mathbb{S}$ is a translation spread of $H(q^n)$ with kernel $\mathbb{F}_q$, we say that $\mathbb{S}$ 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 $\mathscr{S}$ being an imaginary chord of $\mathscr{C}$ [4, Theorem 5], the spreads $\mathbb{S}_{[9]}$ constructed in [3] for $q \equiv 1 \pmod 3$, q odd, and the spreads $\mathbb{S}_l$ 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 $\mathbb{S}_\beta$ of $H(3^h)$, $h > 1$, constructed in [3]. The hermitian spreads, the spreads $\mathbb{S}_{[9]}$ and $\mathbb{S}_l$, 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 *semiclassical* spreads, which is equivalent by [12]), and to Lunardon–Polverino [9] for q even. In [11] it is proved that a spread $\mathbb{S}$ of $H(3^h)$ which is a translation spread with respect to a line is either hermitian or an $\mathbb{S}_\beta$. 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] $\mathbb{S}$ is an $\mathbb{F}_q$-translation spread of $H(q)$ with respect to a line if and only if $\mathscr{S}$ is a line of $PG(3, q)$ whose points belong to imaginary chords of $\mathscr{C}$.
(b) [4, Theorem 5] $\mathbb{S}$ is a hermitian spread of $H(q)$ if and only if $\mathscr{S}$ is an imaginary chord of $\mathscr{C}$.
(c) [4] If $q \equiv 1 \pmod 3$ and $\mathscr{S}$ is an imaginary axis l of $\mathscr{C}$, then $\mathscr{S}$ defines an $\mathbb{F}_q$-translation spread $\mathbb{S}_l$ of $H(q)$ with respect to a line. If q is odd, then $\mathbb{S}_l = \mathbb{S}_{[9]}$, and if q is even, then this is the same as the spread $\mathbb{S}_l$ 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* $q \geqslant 4n^2 - 8n + 2$, *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 $X = \{\langle \mathbf{w} \rangle : \mathbf{w} \in W^*\}$. 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 $|X| \equiv 1 \pmod q$. 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 $|X \cap L| \equiv 1 \pmod q$.

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 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 $rank_{\mathbb{F}_q}(X \cap P) = n$ and $rank_{\mathbb{F}_q}(X \cap Q) \geqslant 1$, we have $rank_{\mathbb{F}_q}(X \cap l) \geqslant n + 1$. This implies that $rank_{\mathbb{F}_q}(X \cap R) \geqslant 1$ for each point $R \in l$, i.e. $l \subseteq X$. So, X is a union of a certain number s of lines through P. Now, let H be a hyperplane of $PG(r, q^n)$ not containing P; then $|H \cap X| = s$, hence $s \equiv 1 \pmod q$. $\square$

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 $PG(2, q^n)$ becomes a $(3n - 1)$-dimensional projective space, the conic C becomes a *pseudo-oval* $\mathcal{O}$ [15] and the $\mathbb{F}_q$-linear set X defines a $(2n - 1)$-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 $X^\perp$, of $PG(2, q^n)$ of rank n contained in the set of internal points of C. If (q, n) satisfies Property (K), then $X^\perp$ is contained in a line l of $PG(2, q^n)$, i.e. $rank_{\mathbb{F}_q}(X^\perp \cap l) = n$. This implies that $rank_{\mathbb{F}_q}(X \cap l^\perp) = n$ and hence, by Property 4.1, X is a union of lines through the point $l^\perp$. 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 $rank_{\mathbb{F}_q}(X \cap P) = n$ 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 χ 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 $f(x) = ax^{p^j} + b$ for some j in the range $0 \leqslant j < n$, 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 $f(x) = ax^{q^t}$ for some $0 \leqslant t < n$ 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*

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

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

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

(i) *If $\sigma = \tau$, then either $A = \bar{A}$, $B = \bar{B}$, $C = \bar{C}$ or $g(y) = [(\bar{B} - B)/(A - \bar{A})]y^{\sigma} + [(\bar{C} - C)/(A - \bar{A})]y$ and $n = 2h$.*
(ii) *If $\sigma \neq \tau$, then $A^{\tau}\bar{A} - A\bar{A}^{\sigma} = 0$, $\bar{B}A^{\tau} - C^{\tau} = 0$ and $\bar{C}^{\sigma} - B\bar{A}^{\sigma} = 0$. Also, if $\tau\sigma \neq 1$, then $B^{\tau} = \bar{B}^{\sigma}$ and $\bar{C}A^{\tau} - \bar{A}^{\sigma}C = 0$.*

Proof. If $\sigma = \tau$ then by subtracting (**) from (*) we get that either $A = \bar{A}$, $B = \bar{B}$, $C = \bar{C}$ or $g(y) = [(\bar{B} - B)/(A - \bar{A})]y^{\sigma} + [(\bar{C} - C)/(A - \bar{A})]y$. In the latter case, substituting in (*), 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 (*) and (**), we get

$$A^{\tau}(**) - [(*)^{\tau} - (**)^{\sigma}] - \bar{A}^{\sigma}(*) = 0,$$

i.e.

$$(A^{\tau}\bar{A} - A\bar{A}^{\sigma})g(y) + (\bar{B}A^{\tau} - C^{\tau})y^{\tau} - (B^{\tau} - \bar{B}^{\sigma})y^{\sigma\tau} + (\bar{C}^{\sigma} - B\bar{A}^{\sigma})y^{\sigma} + (\bar{C}A^{\tau} - \bar{A}^{\sigma}C)y = 0 \tag{1}$$

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

$$g(y) = ay + by^{\sigma} + cy^{\tau} + dy^{\sigma\tau}, \tag{2}$$

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

$$d^{\sigma}y^{\sigma^2\tau} + (c^{\sigma} + Ad)y^{\sigma\tau} + b^{\sigma}y^{\sigma^2} + (a^{\sigma} + Ab + B)y^{\sigma} + Acy^{\tau} + (Aa + C)y = 0 \tag{3}$$

$$d^{\tau}y^{\sigma\tau^2} + (b^{\tau} + \bar{A}d)y^{\sigma\tau} + c^{\tau}y^{\tau^2} + (a^{\tau} + \bar{A}c + \bar{B})y^{\tau} + \bar{A}by^{\sigma} + (\bar{A}a + \bar{C})y = 0. \tag{4}$$

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 $\bar{A}b + c^{\sigma^2} = 0$, which imply

$b(A^{\sigma^2}\bar{A}-1)=0$ and $c(\bar{A}^{\sigma}A-1)=0$. Since $A^{\tau}\bar{A}-A\bar{A}^{\sigma}\neq 0$, we have $b=c=0$, i.e. $g(y)$ is linear over $\mathbb{F}_{q^n}$: 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 $\mathbb{F}_{q^n}$: 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 $\sigma\tau^2=1$. 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 $c^{\sigma}+Ad=0$, $b^{\sigma^2}+\bar{A}d=0$ and $b^{\sigma}+Ac=0$ from which we have $\bar{A}=-A^{\sigma+1}$, which implies $A^{\tau}\bar{A}-A\bar{A}^{\sigma}=0$: a contradiction. In the second case, in a similar way, we again get a contradiction. Hence, we always have $A^{\tau}\bar{A}-A\bar{A}^{\sigma}=0$ and, in this case, from (1) we easily get (ii). □

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 $\mathbb{F}_q$-linear set of $PG(2,q^n)$ of rank n contained in the set of internal points of the irreducible conic C with equation $-3Y_1^2+4Y_2Y_0=0$. 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*

$$X=\left\{\left(x,\gamma x,\frac{m}{4}x^{\tau}+\frac{3}{4}\gamma^2x\right) : x\in\mathbb{F}_{q^n}^*\right\},$$

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

(3) *If $X=\{(\bar{f}(x),\bar{g}(x),x) : x\in\mathbb{F}_{q^n}^*\}$ and $(1,0,0)\in l$, then*

$$X=\left\{\left(\frac{3}{4}\rho^2x+\frac{m'}{4}x^{\sigma},\rho x,x\right) : x\in\mathbb{F}_{q^n}^*\right\},$$

where $\sigma=q^h$, $0\leqslant h<n$, $\rho\in\mathbb{F}_{q^n}$ and m' is a non-square in $\mathbb{F}_{q^n}$.

(4) *If $X=\{(\bar{f}(x),\bar{g}(x),x) : x\in\mathbb{F}_{q^n}^*\}$ and $(1,0,0)\notin l$, then*

$$X=\{(\alpha\bar{g}(x)+\beta x,\bar{g}(x),x) : x\in\mathbb{F}_{q^n}^*\},$$

where $\alpha,\beta\in\mathbb{F}_{q^n}$, $\Delta=\alpha^2+3\beta$ is a non-zero square of $\mathbb{F}_{q^n}$ and $\bar{g}(x)$ satisfies equality (*) *of Lemma* 5.3 *with $A=(\alpha+\sqrt{\Delta})^{2\sigma+2}/3m'\sqrt{\Delta}^{\sigma+1}$, $B=-2(\alpha+\sqrt{\Delta})^{\sigma}/3$, $C=2\beta(\alpha+\sqrt{\Delta})^{2\sigma+1}/3m'\sqrt{\Delta}^{\sigma+1}$, $\sigma=q^h$, $0\leqslant h<n$ 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 $\mathscr{F}$ of the quadratic cone $\mathscr{K}$ of $PG(3,q^n)$ whose planes all contain a common interior point of $\mathscr{K}$ (see, e.g., [8,16]). Then by [14, Section 1.5.6] $\mathscr{F}$ 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 $Y_1=\gamma Y_0$, where $\gamma \in \mathbb{F}_{q^n}$, and hence $f(x)=\gamma x$ and $-3\gamma^2x^2+4xg(x)$ is a non-square for all $x \in \mathbb{F}^*_{q^n}$, i.e.

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

for each $x \in \mathbb{F}^*_{q^n}$. Applying Corollary 5.2, we get $g(x)=(m/4)x^\tau+(3/4)\gamma^2x$ where $\tau=q^{h'}$, $0 \leqslant h' < n$, 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, $\Delta=\alpha^2+3\beta$ is a non-zero square in $\mathbb{F}_{q^n}$ and $l \cap C=\{P_1, P_2\}$, where $P_1=((\alpha+\sqrt{\Delta})^2, 2(\alpha+\sqrt{\Delta}), 3)$ and $P_2=((\alpha-\sqrt{\Delta})^2, 2(\alpha-\sqrt{\Delta}), 3)$. The linear transformation ω_c of $PG(2,q^n)$, mapping the point (y_0, y_1, y_2) into the point $(y_0, 2cy_0+y_1, 3c^2y_0+3cy_1+y_2)$, fixes the conic C for each $c \in \mathbb{F}_{q^n}$ and, if $\bar{c}=-1/(\alpha+\sqrt{\Delta})$, then $P_1^{\omega_{\bar{c}}}=(1,0,0)$. So, $X^{\omega_{\bar{c}}}$ is an $\mathbb{F}_q$-linear set of rank n of internal points of C contained in the line $l^{\omega_{\bar{c}}}$ and $(1,0,0) \in l^{\omega_{\bar{c}}}$. Hence, if $X^{\omega_{\bar{c}}}=\{(F(x'), G(x'), x') : x' \in \mathbb{F}_{q^n}\}$, by Case (3) we get $F(x')=(3/4)\rho^2x'+(m'/4)x'^\sigma$ and $G(x')=\rho x'$, where $\sigma=q^h$, $0 \leqslant h < n$, $\rho \in \mathbb{F}_{q^n}$ and m' is a non-square in $\mathbb{F}_{q^n}$. Applying $\omega_{\bar{c}}$ to l and X, respectively, we obtain $\rho=-\beta/\sqrt{\Delta}$ and

$$F(x')=\frac{3}{4}\rho^2x'+\frac{m'}{4}x'^\sigma=\alpha\bar{g}(x)+\beta x,$$
$$G(x')=\rho x'=(2\bar{c}\alpha+1)\bar{g}(x)+2\bar{c}\beta x,$$
$$x'=(3\bar{c}^2\alpha+3\bar{c})\bar{g}(x)+(3\bar{c}^2\beta+1)x.$$

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

$$\bar{g}^\sigma(x)+A\bar{g}(x)+Bx^\sigma+Cx=0, \tag{5}$$

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

If $A=0$, then $\alpha+\sqrt{\Delta}=0$ 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*

$$\mathcal{O}=\{(x, ax+h(y), bx^\tau+cx+k(y)) : x, y \in \mathbb{F}_{q^n}\}$$

be an $\mathbb{F}_q$-linear set of $PG(2,q^n)$ 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 $PG(2,q^n)$ such that $rank_{\mathbb{F}_q}(R \cap \mathscr{O}) = n$. 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:

$$k(y) = -\frac{bx_0^\tau}{h(y_0)^\tau} h(y)^\tau + \frac{bx_0^\tau + k(y_0)}{h(y_0)} h(y). \tag{6}$$

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

$$\begin{aligned}
&\lambda x_0 = x,\\
&\lambda(ax_0 + h(y_0)) = ax + h(y),\\
&\lambda(bx_0^\tau + cx_0 + k(y_0)) = bx^\tau + cx + k(y),\\
&\Updownarrow\\
&\lambda x_0 = x,\\
&\lambda h(y_0) = h(y),\\
&\lambda(bx_0^\tau + k(y_0)) = bx^\tau + k(y),
\end{aligned} \tag{7}$$

for each $\lambda \in \mathbb{F}_{q^n}^*$. If $h(y_0) = 0$, then $y_0 = 0$, $y = 0$ and from (7) we get $\lambda = \lambda^\tau$ 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). □

6. Proof of Theorem 2.3

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

$$F(X_0, X_1, X_2, X_3) = X_3^2 X_0^2 - 3X_2^2 X_1^2 - 6X_0X_1X_2X_3 + 4X_3X_1^3 + 4X_2^3X_0 = 0$$

(see, e.g., [6, p. 240]). For each osculating plane π_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 $PG(3,q^n)$, $p \neq 2$, belongs to an imaginary chord of $\mathscr{C}$ if and only if P lies on a line with coordinate vector $(\alpha_2^2, \alpha_1\alpha_2, \alpha_1^2 - \alpha_2, \alpha_2, \alpha_2, -\alpha_1, 1)$ where $\alpha_1, \alpha_2 \in \mathbb{F}_{q^n}$ and $\alpha_1^2 - 4\alpha_2$ 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 $\mathscr{C}$ if and only if $F(a_0, a_1, a_2, a_3)$ is a non-square in $\mathbb{F}_{q^n}$.

Let $\mathscr{S}$ be an $\mathbb{F}_q$-linear set of $PG(3,q^n)$ of rank $2n$ whose points belong to imaginary chords of $\mathscr{C}$ and suppose that $\mathbb{F}_q$ is the maximal subfield of $\mathbb{F}_{q^n}$ with respect to which $\mathscr{S}$ 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 $\mathscr{S}$, then $(0, a_1 - a_1', a_2 - a_2', 0) \in \mathscr{S}$ 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 $\mathscr{S}$ 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 $f(x, y), g(x, y)\colon \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ such that

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

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 $\mathscr{S}$ belong to imaginary chords of $\mathscr{C}$, we have that

$$F\,(x, f(x, y), g(x, y), y) \text{ is a non-square for all } (x, y) \neq (0, 0). \tag{8}$$

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

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

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

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

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

Proof. The conic C_∞ has equations $-3X_1^2 + 4X_0X_2 = X_3 = 0$, and hence, since $p \neq 2, 3$, C_∞ is an irreducible conic of π_∞. 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 $\mathscr{S}_\infty$ is an $\mathbb{F}_q$-linear set of rank *n* of internal points of C_∞. By Property (K), $\mathscr{S}_\infty$ is contained in a line *r* of π_∞ and, applying Lemma 5.4, we have that either $\mathscr{S}_\infty$ is a point or *r* is a secant line to C_∞. In this case, since the stabilizer G_{P_∞} of the full automorphism group *G* of $\mathscr{C}$ acts transitively on $C_\infty \backslash \{P_\infty\}$, we can suppose, without loss of generality, that the point $(0, 0, 1, 0)$ of C_∞ belongs to the line *r*. Hence, by (2) of Lemma 5.4, we can write

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

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

Let $\mathscr{S}_0 = \mathscr{S} \cap \pi_0$ and let $f_2(y) = f(0, y)$ and $g_2(y) = g(0, y)$. Since π_0 has equation $X_0 = 0$, we can write

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

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

(1) *$\mathscr{S}_0$ is a point, i.e. $f_2(y)$ and $g_2(y)$ are linear over $\mathbb{F}_{q^n}$.*
(2) *$\mathscr{S}_0 = \{(0, (3/4)\rho^2 y + (m'/4)y^\sigma, \rho y, y) : y \in \mathbb{F}_{q^n}\}$ where $\sigma = q^h$, $0 \leqslant h < n$, $\rho \in \mathbb{F}_{q^n}$ and m' is a non-square in $\mathbb{F}_{q^n}$.*

(3) $\mathscr{S}_0=\{(0, \alpha g_2(y)+\beta y, g_2(y), y) : y \in \mathbb{F}_{q^n}\}$, *where* $\Delta=\alpha^2+3\beta$ *is a non-zero square of* $\mathbb{F}_{q^n}$ *and* $g_2(y)$ *satisfies equality* (*) *of Lemma* 5.3 *with* $A=(\alpha+\sqrt{\Delta})^{2\sigma+2}/3m'\sqrt{\Delta}^{\sigma+1}$, $B=-2(\alpha+\sqrt{\Delta})^{\sigma}/3$, $C=2\beta(\alpha+\sqrt{\Delta})^{2\sigma+1}/3m'\sqrt{\Delta}^{\sigma+1}$, $\sigma=q^h$, $0\leqslant h<n$ 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 π_0. By (8) we get that

$$-3g_2^2(y)+4yf_2(y) \text{ is a non-square for all } y\in\mathbb{F}_{q^n}^*. \tag{9}$$

As in the previous case, since $q^n \equiv 1 \pmod 3$, from the above condition we get that $\mathscr{S}_0$ is an $\mathbb{F}_q$-linear set of rank n of internal points of C_0. Hence, by Property (K), $\mathscr{S}_0$ is contained in a line l of π_0. Now, applying Lemma 5.4 to the $\mathbb{F}_q$-linear set $\mathscr{S}_0$, we obtain (1), (2) and (3). □

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

(a) $\mathscr{S}=\{(x, \gamma x+(3/4)\rho^2y+(m'/4)y^\sigma, (m/4)x^\tau+(3/4)\gamma^2x+\rho y, y) : x, y\in\mathbb{F}_{q^n}\}$,
(b) $\mathscr{S}=\{(x, \gamma x+\alpha g_2(y)+\beta y, (m/4)x^\tau+(3/4)\gamma^2x+g_2(y), y) : x, y\in\mathbb{F}_{q^n}\}$,

where $g_2(y)$ is a polynomial satisfying equality (*) of Lemma 5.3. Also, since $\mathscr{S}$ is not a line, $\mathscr{S}_0$ and $\mathscr{S}_\infty$ 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 $\mathscr{S}$ and $\mathscr{C}$ from the point $P_t=(t^3,t^2,t,1)$ onto the plane π_∞ we get, respectively, the $\mathbb{F}_q$-linear set of rank $2n$

$$\mathscr{O}_t=\{(x-t^3y, f(x,y)-t^2y, g(x,y)-ty, 0) : x, y\in\mathbb{F}_{q^n}\}$$

and the irreducible conic Γ_t with equations $t^2X_2^2+X_1^2-tX_1X_2-X_0X_2=X_3=0$. Since the points of $\mathscr{S}$ belong to imaginary chords of $\mathscr{C}$, the $\mathbb{F}_q$-linear set $\mathscr{O}_t$ and the irreducible conic Γ_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 $rank_{\mathbb{F}_q}(R_t\cap\mathscr{O}_t)=n$. By using this condition for suitable values of t, we can exclude Cases (a) and (b).

Proposition 6.3. *If* $q^n\equiv 1 \pmod 3$ *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

$$\mathscr{O}_0=\left\{\left(x, \gamma x+\frac{3}{4}\rho^2y+\frac{m'}{4}y^\sigma, \frac{m}{4}x^\tau+\frac{3}{4}\gamma^2x+\rho y, 0\right) : x, y\in\mathbb{F}_{q^n}\right\}.$$

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 $rank_{\mathbb{F}_q}(R_0 \cap \mathcal{O}_0) = n$. Therefore, since $f_2(y) = (3/4)\rho^2 y + (m'/4)y^\sigma$ 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

$$\rho y = -\frac{m}{4}\frac{x_0^\tau}{f_2(y_0)^\tau}\left(\frac{3}{4}\rho^{2\tau} y^\tau + \frac{m'^\tau}{4} y^{\sigma\tau}\right) + \frac{\frac{m}{4}x_0^\tau + \rho y_0}{f_2(y_0)}\left(\frac{3}{4}\rho^2 y + \frac{m'}{4} y^\sigma\right) \tag{10}$$

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 $\mathcal{O}_0 \cap \Gamma_0 = \emptyset$, we have

$$\frac{m'^2}{16} y^{2\sigma} + \gamma\frac{m'}{2} x y^\sigma - \left(\frac{m}{4} x^{\tau+1} - \frac{\gamma^2}{4} x^2\right) \neq 0$$

for each $x, y \in \mathbb{F}_{q^n}$ with $(x, y) \neq (0, 0)$. This implies that $(m'^2 m/16)x^{\tau+1} + (3\gamma^2 m'^2/16)x^2$ 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 $\bar{t}^{3\tau+1} \neq m'/m$ and $\bar{t}^{\tau-1} \neq 16/mm'^\tau$ and let $z = x - \bar{t}^3 y$; we can write

$$\mathcal{O}_{\bar{t}} = \left\{\left(z, \frac{m'}{4} y^\sigma - \bar{t}^2 y, \frac{m}{4} z^\tau + \frac{m}{4}\bar{t}^{3\tau} y^\tau - \bar{t} y, 0\right) : y, z \in \mathbb{F}_{q^n}\right\},$$

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

$$\frac{m}{4}\bar{t}^{3\tau} y^\tau - \bar{t} y = -\frac{m}{4}\frac{z_0^\tau}{h(y_0)^\tau}\left(\frac{m'^\tau}{4} y^{\sigma\tau} - \bar{t}^{2\tau} y^\tau\right) + \frac{m z_0^\tau + 4k(y_0)}{4h(y_0)}\left(\frac{m'}{4} y^\sigma - \bar{t}^2 y\right), \tag{11}$$

for each $y \in \mathbb{F}_{q^n}$, where $h(y) = (m'/4)y^\sigma - \bar{t}^2 y$ and $k(y) = (m/4)\bar{t}^{3\tau} y^\tau - \bar{t} y$. If $z_0 = 0$, we get $\sigma = \tau$ and $\bar{t}^{3\tau+1} = m'/m$, 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 $\bar{t}^{\tau-1} = 16/mm'^\tau$: a contradiction. Hence, Case (a) does not occur. □

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

Proof. Suppose Case (b) occurs. Then

$$\mathcal{O}_t = \left\{\left(x - t^3 y, \gamma x + \alpha g_2(y) + \beta y - t^2 y, \frac{m}{4} x^\tau + \frac{3}{4}\gamma^2 x + g_2(y) - t y, 0\right) : x, y \in \mathbb{F}_{q^n}\right\}.$$

From (9) we easily get that $f_2(y) = \alpha g_2(y) + \beta y$ 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

$$g_2(y) = -\frac{m}{4}\frac{x_0^\tau}{f_2(y_0)^\tau}(\alpha g_2(y) + \beta y)^\tau + \left(\frac{m x_0^\tau + 4 g_2(y_0)}{4 f_2(y_0)}\right)(\alpha g_2(y) + \beta y)$$

for each $y \in \mathbb{F}_{q^n}$. If $\alpha = 0$, then $g_2(y) = -(m/4)(x_0^\tau \beta^\tau / f_2(y_0)^\tau) y^\tau + ((mx_0^\tau + 4g_2(y_0))/4 f_2(y_0))\beta y$. This implies that $g.c.d.(h, h', n) = 1$ and, substituting in (*), we either get that $g_2(y)$ is linear over $\mathbb{F}_{q^n}$ or $n = 2$: a contradiction. Hence $\alpha \neq 0$, and $g_2(y)$ satisfies the equality

$$g_2^\tau(y) + \bar{A} g_2(y) + \bar{B} y^\tau + \bar{C} y = 0, \tag{12}$$

where $\bar{A} = [(4\beta y_0 - m\alpha x_0^\tau)/m x_0^\tau \alpha^\tau] f_2(y_0)^{\tau-1}$, $\bar{B} = (\beta/\alpha)^\tau$, $\bar{C} = -[(mx_0^\tau + 4g_2(y_0))/m x_0^\tau]\beta/\alpha^\tau f_2(y_0)^{\tau-1}$. If $\bar{A} = 0$, then $g_2(y) = -\bar{B}^{\tau^{-1}} y - \bar{C}^{\tau^{-1}} y^{\tau^{-1}}$. 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 $\bar{A} \neq 0$ and we can apply Lemma 5.3 to the polynomial $g_2(y)$. Since $\bar{B}^\sigma \neq B^\tau$, if Case (i) of Lemma 5.3 occurs, then $g_2(y) = [(\bar{B} - B)/(A - \bar{A})] y^\sigma + [(\bar{C} - C)/(A - \bar{A})] y$ 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 $\bar{B} A^\tau - C^\tau = 0$ from which we get $\beta = 0$. In this case, since $\mathcal{O}_0$ and Γ_0 are disjoint, we can write

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

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

$$\mathcal{O}_{\gamma^{-1}} = \left\{ \left(z, \gamma z + \alpha g_2(y), \frac{m}{4} z^\tau + \frac{3}{4}\gamma^2 z + \frac{m}{4\gamma^{3\tau}} y^\tau - \frac{1}{4\gamma} y + g_2(y), 0 \right) : \ y, z \in \mathbb{F}_{q^n} \right\}.$$

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

$$\frac{m}{4\gamma^{3\tau}} y^\tau - \frac{1}{4\gamma} y + g_2(y) = -\frac{m}{4} \frac{z_0^\tau}{h(y_0)^\tau} \alpha^\tau g_2^\tau(y) + \left(\frac{m z_0^\tau + 4k(y_0)}{4h(y_0)} \right) \alpha g_2(y)$$

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

$$g_2(y)^\tau + \overline{\overline{A}} g_2(y) + \overline{\overline{B}} y^\tau + \overline{\overline{C}} y = 0 \tag{13}$$

for each $y \in \mathbb{F}_{q^n}$, where $\overline{\overline{A}} = (4h(y_0)^{\tau-1}/m z_0^\tau \alpha^\tau)[h(y_0) - \alpha((m/4) z_0^\tau + k(y_0))]$, $\overline{\overline{B}} = (h(y_0)^\tau / \gamma^{3\tau} z_0^\tau \alpha^\tau)$ $\overline{\overline{C}} = -h(y_0)^\tau / m\gamma z_0^\tau \alpha^\tau$. If $\overline{\overline{A}} = 0$ (similar to the case $\bar{A} = 0$), we get $n = 2$, contradicting our assumption. Hence $\overline{\overline{A}} \neq 0$ and we can apply Lemma 5.3 to the polynomial $g_2(y)$. Since $C = 0$ and $\overline{\overline{C}} \neq 0$, in our hypotheses, Case (ii) of Lemma 5.3 occurs, from which we get $\overline{\overline{B}} = 0$, i.e. $h(y_0) = 0$: a contradiction. This proves that Case (b) does not occur. □

From the previous results Theorem 2.3 follows.

References

[1] L. Bader, G. Lunardon, Generalized hexagons and polar spaces, Discrete Math. 208/209 (1999) 13–22.
[2] S. Ball, A. Blokhuis, M. Lavrauw, On the classification of semifield flocks, Adv. Math. 180 (2003) 104–111.
[3] I. Bloemen, J.A. Thas, H. Van Maldeghem, Translation ovoids of generalized quadrangles and hexagons, Geom. Dedicata 72 (1998) 19–62.
[4] I. Cardinali, G. Lunardon, O. Polverino, R. Trombetti, Translation spreads of the classical generalized hexagon, European J. Combin. 23 (2002) 367–376.
[5] L. Carlitz, A theorem on "ordered" polynomials in a finite field, Acta Arith. VII (1962) 167–172.
[6] J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions, The Clarendon Press, Oxford University Press, New York, 1985.
[7] R. Lidl, H. Niedirreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[8] G. Lunardon, Flocks ovoids of $Q(4, q)$ and designs, Geom. Dedicata 66 (2) (1997) 163–173.
[9] G. Lunardon, O. Polverino, On the twisted cubic of $PG(3, q)$, J. Algebraic Combin. 18 (2003) 255–262.
[10] G. Lunardon, O. Polverino, Translation ovoids of orthogonal polar spaces, Forum Math. 16 (5) (2004) 255–262.
[11] A.D. Offer, Translation ovoids and spreads of the generalized hexagon $H(q)$, Geom. Dedicata 85 (1–3) (2001) 135–145.
[12] A.D. Offer, Translation spreads of the split Cayley hexagon, Adv. Geom. 3 (2) (2003) 105–121.
[13] J.A. Thas, Polar spaces, generalized hexagons and perfect codes, J. Combin. Theory Ser. A 29 (1980) 87–93.
[14] J.A. Thas, Generalized quadrangles and flocks of cones, European J. Combin. 8 (1987) 441–452.
[15] J.A. Thas, Generalized quadrangles of order (s, s^2). I, J. Combin. Theory Ser. A 67 (1994) 140–160.
[16] J.A. Thas, Generalized quadrangles of order (s, s^2). II, J. Combin. Theory Ser. A 79 (1997) 223–254.
[17] J. Tits, Sur la trialité et certains groupes qui s'en déduisent, Inst. Hautes Études Sci. Publ. Math. 2 (1959) 14–60.
[18] H. Van Maldeghem, Generalized Polygons, Monogr. Math., vol. 93, Birkhäuser Verlag, Basel, 1998.