Rendiconti
Accademia Nazionale delle Scienze detta dei XL
Memorie di Matematica e Applicazioni
125° (2009), Vol. XXXI, fasc. 1, pagg. 89-112

GÁBOR KORCHMÁROS(*)

Segre-Type Theorems in Finite Geometry(**)

Abstract. — Segre-type theorems related to blocking sets of lines chosen with respect to a conic in $PG(2,q)$ are currently under investigation. A detailed survey on results and methods used in the proofs is given.

1. - Introduction

In the joint paper [30], the following combinatorial characterisation of external lines to an irreducible conic in $PG(2,q)$ is given.

Theorem 1.1: *If every secant and tangent of an irreducible conic meets a point-set $\mathcal{L}$ in exactly one point, then $\mathcal{L}$ consists of all points of an external line to the conic.*

For even q, this has been proven by Bruen and Thas [13] independently.

In the abstract of [30], the following remark is made: "while the result admits no analogue in the real field, a number of similar properties can be established or investigated in any Galois geometry." In this spirit, combinatorial characterisations of geometric objects related to conics are *Segre-type theorems*.

The proof of Theorem 1.1 depends on Segre's "lemma of Tangents" which was the key idea in the proof of his famous combinatorial characterisation of conics of

(*) Indirizzo dell'Autore: Gábor Korchmáros, Dipartimento di Matematica, Università degli Studi della Basilicata, Contrada Macchia Romana, 85100 Potenza, Italy
e-mail: korchmaros@unibas.it

(**) The present research was performed within the activity of G.N.S.A.G.A. of the Italian INDAM with the financial support of the Italian Ministry M.I.U.R., project "Strutture geometriche, combinatorica e loro applicazioni", 2003–04.

A.M.S. Classification: 51E20 (primary) – 51A50 (secondary).

$PG(2,q)$ with q odd, see [28], [29] and Lemma 8.11 in [22]. Likewise, the proofs of the early Segre-type theorems dating back to the early Eighties, relied on Segre's lemma, see [1], [18].

The Jamison method, developed originally for the study of blocking sets by means of polynomials, was also a useful tool in proving Segre-type theorems. By using the Jamison method, Blokhuis and Wilbrink [10] were able to give a new, completely independent proof for Theorem 1.1, see also [9]. A nice presentation of the Jamison method is found in [12]. A recent survey on applications of polynomials in finite geometry is Blokhuis [8] which is, in some ways, a continuation of Ball's [5] and Blokhuis' [6], [7] surveys.

Some newer Segre-type theorems are related to blocking sets. Their study is a current research area in which the usual combinatorial and group theoretic methods are made more efficient by using algebraic curves defined over finite fields. Problems and results are described in the following sections.

Application of results and techniques from algebraic geometry to solving problems in finite geometry was a powerful tool in Segre's work. Especially his ingenious idea to link arcs to algebraic curves via Wilson's theorem, in such a manner to apply the profound Hasse-Weil bounds on the number of $GF(q)$-rational points of an algebraic curve, was seminal as demonstrated in Szönyi's survey [33].

2. - Blocking sets of line sets in $PG(2,q)$

Boros, Füredi and Kahn [11] relied on Theorem 1.1 to obtain the following result concerning an irreducible conic $\mathcal{C}$ in $PG(2,q)$.

The minimum size of a point set $\mathcal{B}$ in $PG(2,q)$ meeting every secant and tangent of $\mathcal{C}$ is $q+1$, the minimum value being attained only in a few cases, namely when

(i) $\mathcal{B}$ consists of all points of an external line to $\mathcal{C}$;
(ii) $\mathcal{B}$ contains m points from $\mathcal{C}$ and $q+1-m$ points from a line ℓ.

More precisely, in (ii), there is an abelian linear collineation group G of order m preserving both $\mathcal{C}$ and ℓ such that $\mathcal{B}\cap\mathcal{C}$ is an orbit under G while $\ell\setminus\mathcal{C}$ is the corresponding orbit on ℓ under G which consists of all points lying on secants of $\mathcal{B}\cap\mathcal{C}$.

It is worth mentioning that this theorem was the main ingredient in their investigation on the minimum number of members of a maximal k-clique, that is, a family of mutually intersecting k-sets.

The above theorem is closely related to results of Wettl [37] and of Szönyi and Wettl [34] about $(q+1)$-sets Q with the following property: for some line ℓ, the point set $Q\setminus\ell$ is an arc and every line containing two points of $Q\setminus\ell$ is disjoint from $\ell\setminus Q$. The same theorem was the starting point of Mazzocca's investigation in [27] on nuclei of $(q+1)$-sets in $PG(2,q)$.

Similar combinatorial questions can be posed. To do this it is useful to adopt the terminology introduced by Mazzocca in [27].

A *blocking set of a line set* $\mathcal{L}$ is any point set $\mathcal{B}$ in $PG(2,q)$ blocking $\mathcal{L}$, that is, meeting every line of $\mathcal{L}$. From a result of Erdös and Lovász [17], if $|\mathcal{L}| \geq q^2 - q$ then $\mathcal{B}$ is of linear type as it derives from a line by deleting and adding a few points.

Results of this kind are viewed as stability theorems in the very recent investigation by Szönyi and Weiner [35].

Blocking sets of line sets chosen with respect to an irreducible conic $\mathcal{C}$ in $PG(2,q)$ are currently under investigation. If the line set consists of all secants and tangents to $\mathcal{C}$, then the above theorem of Boros, Füredi and Kahn [11] provides a complete classification.

In [2], all point sets of minimum size blocking all external lines to $\mathcal{C}$ have been determined in $PG(2,q)$ with odd q. Apart from two sporadic cases occurring for $q = 5,7$, every such a point set is linear, that is, it consists of all points of a secant of $\mathcal{C}$ minus the two common points of the secant and $\mathcal{C}$, see Theorem 5.1. For q even the picture is richer although no sporadic example occurs, see [19]: two more infinite series of examples exist, namely all points of a tangent minus the tangency point and the nucleus; for q square, all points of a Baer subplane intersecting $\mathcal{C}$ in a subconic $\mathcal{C}_0$ minus the nucleus and the points of $\mathcal{C}_0$.

For q odd, a similar classification for point sets of minimum size blocking all external and tangent lines is given in [3]. Three cases (none of them sporadic) occur, namely all points of a tangent minus the tangency point; all points of a secant different from its two points on $\mathcal{C}$, plus the pole of the secant with respect to (the polarity associated with) $\mathcal{C}$; and all points of a Baer subplane intersecting $\mathcal{C}$ in a subconic $\mathcal{C}_0$ minus the points of $\mathcal{C}_0$, see Theorem 6.1.

The picture is quite different for minimum size blocking sets of secants to $\mathcal{C}$, since the following procedure provide several examples in $PG(2,q)$ with q even. Let $\mathcal{C}$ be given with its (affine) equation $Y = X^2$, that is, let $\mathcal{C}$ be a parabola in the affine plane $AG(2,q)$. For every $a \in GF(q)$,

$$\varphi_a : (X,Y) \longrightarrow (X+a, Y+a^2)$$

is a translation of the affine plane $AG(2,q)$. The center of φ_a, viewed as an elation in the projective closure $PG(2,q)$ of $AG(2,q)$, is the infinite point $B_a = (1,a,0)$. The translation group of $\mathcal{C}$ is $T = \{\varphi_a \mid a \in GF(q)\}$ and it is isomorphic to the additive group $(GF(q),+)$ of $GF(q)$. Take a subgroup $G = \{\varphi_a \mid a \in H\}$ of T where H is a subgroup in $(GF(q),+)$, and define Γ to be the set of all centers of all nontrivial translations in G. If $P = (u,u^2)$ is an affine point in $\mathcal{C}$, the orbit of P under G is $\Delta_u = \{(a+u,(a+u)^2) \mid a \in H\}$. Then, $\mathcal{B}(G,u) = (\mathcal{C} \setminus \Delta_u) \cup \Gamma$ is a blocking set of secants to $\mathcal{C}$. Since $\mathcal{B}(G,u)$ consists of q points, it is a blocking set of minimum size. In [4], it is shown that these are all minimum size blocking sets of all secants to $\mathcal{C}$ in $PG(2,q)$ with q even.

It may be noted that the above construction is related with sharply focused sets arising from a geometric based secret sharing used in cryptography, see [14], [15], [16], [20], [32].

3. - Polynomials vanishing at internal points to an irreducible conic in $PG(2,q)$, q odd

An essential tool in the above investigation is a result on the linear system of polynomials vanishing at every internal point to $\mathcal{C}$, appeared in [2] and [3]. We reproduce the proof in the present and the next sections.

The degree of any non-zero polynomial $f(X,Y) \in GF(q)[X,Y]$ vanishing at every (x,y) with $x,y \in GF(q)$ is at least q, and equality holds if and only if $f(X,Y) = = \lambda(X^q - X) + \mu(Y^q - Y)$ with $\lambda, \mu \in GF(q)$, see [21] p. 87.

Given a non-empty subset $\mathcal{I}$ of ordered pairs (x,y) with $x,y \in GF(q)$, one can ask for the minimum degree $d(\mathcal{I})$ of non-zero polynomials over $GF(q)$ vanishing on $\mathcal{I}$. By a classical result from projective geometry, if $\frac{1}{2}n(n+3) \geq |\mathcal{I}|$, then $d(\mathcal{I}) \leq n$. For $n = q-2$, this shows that $d(\mathcal{I}) \leq q-2$ as long as $|\mathcal{I}| \leq \frac{1}{2}(q^2 - q) - 1$.

It turns out that any point-set $\mathcal{I}$ of size $\frac{1}{2}(q^2 - q)$ with $d(\mathcal{I}) = q-1$ imposes the greatest possible number of independent conditions on the polynomials vanishing on $\mathcal{I}$. This suggests that such point-sets are rare and interesting objects.

We show that the set consisting of all internal points to an irreducible conic is of this kind. Let $AG(2,q)$ be the affine plane coordinatised by $GF(q)$. Then $\mathcal{I}$ can be viewed as a point-set of $AG(2,q)$. Also, to a non-zero polynomial $f(X,Y) \in GF(q)[X,Y]$ there is associated the algebraic curve Γ of equation $f(X,Y) = 0$, and the condition $f(x,y) = 0$ means that Γ passes through the point $P(x,y)$. From now on we assume q to be odd, that is, $q = p^h$ with $p > 2$ prime. Let $\mathcal{C}$ be a parabola of $AG(2,q)$, that is an irreducible conic tangent to the infinite line of $AG(2,q)$. A point P in $AG(2,q)$ is *internal* to $\mathcal{C}$ if no tangent to $\mathcal{C}$ passes through P. There are $\frac{1}{2}(q^2 - q)$ such points, and we will take $\mathcal{I}$ to be the set of all internal points to $\mathcal{C}$. The main result is the following theorem.

Theorem 3.1: *Let Γ be an algebraic plane curve defined over the algebraic closure of $GF(q)$ of odd q order. If Γ passes through every internal point of a parabola $\mathcal{C}$ of $AG(2,q)$, then the degree d of Γ satisfies*

$$d \geq q-1.$$

For the extremal case $d = q-1$ we are able to provide an equation for Γ. To do this, for every $t \in GF(q)$, define the polynomial

$$\varphi_t(X,Y) = 1 - \left(Y - tX + \frac{1}{4}t^2\right)^{q-1} \tag{3.1}$$

over $GF(q)$. Note that $\varphi_t(X,Y)$ can be viewed as the characteristic function of the line r_t of equation $Y - tX + \frac{1}{4}t^2 = 0$. In fact, $\varphi_t(X,Y)$ equals 1 at the points of r_t and it vanishes elsewhere. Geometrically, the algebraic curve of equation $\varphi_t(X,Y) = 0$ splits into the $q-1$ nontangent lines through the infinite point $Q_t = (1,t,0)$.

THEOREM 3.2: *If* $\deg \Gamma = q-1$ *in Theorem* 3.1, *then* Γ *has equation*

$$f(X,Y) = \sum_{t\in GF(q)} \lambda_t \varphi_t(X,Y) = 0. \tag{3.2}$$

If, in addition, Γ *is defined over* $GF(q)$, *then* $\lambda_t \in GF(q)$, *for any* $t \in GF(q)$.

The above theorem may be rephrased using classical terminology from the theory of linear systems, see [31], for instance.

THEOREM 3.3: *The linear system of algebraic curves of degree* $q-1$ *passing through every internal point of a parabola of* $AG(2,q)$ *has dimension* $q-1$. *Such points impose independent conditions on the algebraic curves of degree* $q-1$ *which pass through them.*

The proof of Theorem 3.1 is by contradiction. Let Γ be an algebraic curve containing all points of $\mathcal{I}(\mathcal{C})$ whose degree d satisfies

$$d < q-1. \tag{3.3}$$

The first step consists in proving the following.

LEMMA 3.4: Γ *contains each point of* $\mathcal{C}$.

PROOF: Let $O \in \mathcal{C}$ be any point. Consider an affine plane $AG(2,q)$ whose infinite line ℓ_∞ is tangent to $\mathcal{C}$ with tangency point distinct from O and choose a frame in $AG(2,q)$ with origin O such that $\mathcal{C}$ has equation $Y = X^2$. External and internal points to $\mathcal{C}$ can be described analytically: a point $P(x,y)$ in $A(2,q)$ is external or internal to $\mathcal{C}$ according as $x^2 - y$ is a non-zero square or a non-square in $GF(q)$. Therefore, for each non-square element $v \in GF(q)$, the points $P(0,-v)$ are in $\mathcal{I}(\mathcal{C})$. Furthermore, for each non-square element $w \in GF(q)$, the points of the parabola of equation $Y = (1-w)X^2$ distinct from the origin are also contained in $\mathcal{I}(\mathcal{C})$. Actually, these are all points of $\mathcal{I}(\mathcal{C})$. Note that $d \geq \frac{1}{2}(q+1)$, since each external line to $\mathcal{C}$ contains $\frac{1}{2}(q+1)$ internal points to $\mathcal{C}$. Write the equation of Γ in the form

$$f(X,Y) = \sum a_{ij} X^i Y^j = 0.$$

Since the collineation $(X,Y) \mapsto (uX, u^2 Y)$ with $u \in GF(q)^*$ preserves $\mathcal{C}$, the same holds for the set of its internal points. Hence, for every nonzero element $u \in GF(q)$, the algebraic curve Γ_u of equation

$$f_u(X,Y) = \sum u^{i+2j} a_{ij} X^i Y^j = 0,$$

also contains each point in $\mathcal{I}(\mathcal{C})$. Therefore, the same holds for the algebraic curve Γ' of equation

$$f'(X,Y) = \sum_{u \in GF(q)^*} f_u(X,Y).$$

Writing $f'(X,Y) = \sum b_{ij}X^iY^j$, we have $b_{ij} = \Big(\sum\limits_{u\in GF(q)^*} u^{i+2j}\Big)a_{ij}$. By Lemma 6.3 on pg. 271 of [26],

$$b_{ij} = \begin{cases} -a_{ij} & \text{when either } i = j = 0, \text{ or } i + 2j = q - 1, \\ 0 & \text{otherwise.} \end{cases} \tag{3.4}$$

This shows that

$$f'(X,Y) = -a_{00} + \sum b_j X^{q-2j-1}Y^j,$$

with $b_j \in GF(q)$. Since $\deg f'(X,Y) \le d$ and $d < q-1$, so both $b_0 = 0$ and $j \le \frac{1}{2}(q-1)$ hold. For every non-square element $w \in GF(q)$, we have

$$f'(x,(1-w)x^2) = 0$$

provided that $x \in GF(q)$. Hence

$$-a_{00} + \sum b_j(1-w)^j = 0.$$

Since $w^{(q-1)/2} + 1 = 0$, this yields that the polynomial

$$g(T) = -a_{00} + \sum b_j(1-T)^j$$

is either identically zero or it has the same roots as $T^{(q-1)/2} + 1$. In the latter case,

$$g(T) = c(T^{(q-1)/2} + 1)$$

for a nonzero element c. Replacing T by $1 - T$, we obtain

$$-a_{00} + \sum b_j T^j = c((1-T)^{(q-1)/2} + 1).$$

In particular, $-a_{00} = 2c$ and $b_{(q-1)/2} = c(-1)^{(q-1)/2}$. By elimination of c we get

$$a_{00} + (-1)^{(q-1)/2} 2b_{(q-1)/2} = 0.$$

Furthermore, for every non-square element $v \in GF(q)$, we have $f'(0,-v) = 0$. Hence

$$-a_{00} + b_{(q-1)/2}(-v)^{(q-1)/2} = 0.$$

Since $v^{(q-1)/2} + 1 = 0$, we obtain $a_{00} = 0$. Therefore, Γ contains O. □

Lemma 3.5: *A point $O \in \mathcal{C}$ is either a singular point of Γ, or $\mathcal{C}$ and Γ have the same tangent at O.*

Proof: We use the same set-up and arguments as in the preceding proof. For each nonzero $u \in GF(q)$, set $g_u(X,Y) = u^{-1}f_u(X,Y)$. Also, let $g'(X,Y) = \sum\limits_{u\in GF(q)^*} g'_u(X,Y)$, and $g'(X,Y) = \sum b_{ij}X^iY^j$. Then

$$b_{ij} = \begin{cases} -a_{ij} & \text{when either } i = 1, j = 0, \text{ or } i + 2j = q, \\ 0 & \text{otherwise.} \end{cases} \tag{3.5}$$

This shows that

$$g'(X,Y) = -a_{10}X + \sum b_j X^{q-2j} Y^j$$

with $b_j \in GF(q)$. This time $b_0 = b_1 = 0$ and $j \le \frac{1}{2}(q-1)$, again by $\deg g'(X,Y) \le d$ and (3.3). Set

$$h'(X,Y) = -a_{10} + \sum b_j X^{q-2j-1} Y^j.$$

Then $g'(X,Y) = Xh'(X,Y)$. For every non-square element w of $GF(q)$, we have $h'(x,(1-w)x^2) = 0$ provided that $x \in GF(q)$. Arguing as in the preceding proof, this yields that either $h'(X,Y)$ is the zero polynomial, or

$$-a_{10} + \sum b_j T^j = c((1-T)^{(q-1)/2} + 1)$$

for a nonzero element c. In the latter case, the linear term T is missing on the left-hand side, but we have $-\frac{1}{2}(q-1)T$ on the other side. But this is impossible. Therefore, $a_{10} = 0$. If a_{01} also vanishes, then O is a singular point of Γ. Otherwise, $Y = 0$ is the tangent line to Γ at O. □

Now, assume Γ to be a counterexample of minimum degree. By Lemmas 3.4 and 3.5, the intersection number $I(\Gamma, \mathcal{C}; O) \ge 2$ for every point O of $PG(2,q)$ lying in $\mathcal{C}$. Since there are $q+1$ such points, Bézout's theorem yields that either $2d \ge 2(q+1)$, or $\mathcal{C}$ is a component of Γ. By (3.3) the former case does not occur. In the latter case, Γ splits into two components, namely $\mathcal{C}$ and another, say Δ, of degree $d-2$. Clearly, Δ contains all points in $\mathcal{I}(\mathcal{C})$. But this contradicts Γ being of minimal degree. In proving Theorem 3.3, we will also use homogeneous coordinates (X,Y,Z) in such a way that the infinity line ℓ_∞ has equation $Z = 0$. Let $Q_t = (1,t,0)$ be a point of ℓ_∞. As we have noted in Section 3, the totally reducible curve of degree $q-1$ whose components are the lines through the point Q_t different from the two tangents to $\mathcal{C}$ has equation $\varphi_t(X,Y) = 0$ with $\varphi_t(X,Y)$ defined in (3.1).

We are going to prove that any algebraic curve $\mathcal{D}$ of degree $q-1$ passing through every point in $\mathcal{I}$ belongs to the linear system Σ consisting of all curves with equation

$$\sum_{t \in GF(q)} \lambda_t \varphi_t(X,Y) = 0.$$

Assume that $\mathcal{D}$ has equation $a(X,Y) = 0$, where

$$a(X,Y) = \Psi_0(X,Y) + \cdots + \Psi_{q-1}(X,Y) = 0$$

and $\Psi_i(X,Y)$ is a homogeneous polynomial of degree i. We begin by showing that every polynomial $\Psi_{q-1}(X,Y)=\sum\limits_{i=0}^{q-1} a_i X^i Y^{q-1-i}$ of degree $q-1$ can be written as

$$\begin{aligned}\Psi_{q-1}(X,Y) &= \sum_{t\in GF(q)} \lambda_t (Y-tX)^{q-1} = \\ &= \sum_{t\in GF(q)} \lambda_t \sum_{i=0}^{q-1} \binom{q-1}{i} (-t)^i X^i Y^{q-1-i},\end{aligned}$$

for suitable $\lambda_t \in GF(q)$. To do this, we need to show that the system of linear equations

$$\begin{aligned} a_0 &= \binom{q-1}{0} \sum_{t\in GF(q)} \lambda_t, \\ a_1 &= \binom{q-1}{1} \sum_{t\in GF(q)} \lambda_t(-t), \\ &\vdots \\ a_{q-1} &= \binom{q-1}{q-1} \sum_{t\in GF(q)} \lambda_t(-t)^{q-1}, \end{aligned} \tag{3.6}$$

has a nontrivial solution, or, equivalently, its determinant does not vanish. Apart from the nonzero factor

$$c=\prod_{i=0}^{q-1}\binom{q-1}{i}$$

this determinant is of Vandermonde type with generators w^i, where $i=0,\dots,q-1$ and w is a primitive element of $GF(q)$, which is different from 0. Therefore, (3.6) has exactly one solution, that is there exists a unique homogeneous q-tuple $(\lambda_0,\lambda_1,\dots,\lambda_{q-1})$ with entries in $GF(q)$ such that

$$\Psi_{q-1}(X,Y)=\sum_{t\in GF(q)} \lambda_t (Y-tX)^{q-1}. \tag{3.7}$$

Note that the terms of degree $q-1$ in $\varphi_t(X,Y)$ are those in $(Y-tX)^{q-1}$. If the polynomial $a(X,Y)-\sum\limits_{t\in GF(q)} \lambda_t\varphi_t(X,Y)$ were not identically zero, then the curve of equation

$$a(X,Y)-\sum_{t\in GF(q)} \lambda_t\varphi_t(X,Y)=0$$

would have degree $q-2$ and would pass through every internal point of $\mathcal{C}$ contradicting Theorem 3.1. Therefore

$$a(X,Y)=\sum_{t\in GF(q)} \lambda_t\varphi_t(X,Y).$$

It remains to show that the polynomials $\varphi_t(X,Y)$ with t ranging over $GF(q)$ are linearly independent over the algebraic closure of $GF(q)$. It suffices to show that the polynomials $F_t(X,Y) = (Y - tX)^{q-1}$ are linearly independent. Assume on the contrary that

$$\sum_{t\in GF(q)} \lambda_t F_t(X,Y) = 0. \tag{3.8}$$

Substituting $Y = 1, X = 0$ we see that $\sum \lambda_t = 0$, while substituting $Y = u, X = 1$ we get $\lambda_u + \sum \lambda_t = 0$. Therefore, $\lambda_u = 0$. This of course also shows the independence of the polynomials $\varphi_t(X,Y)$.

Remark 3.6: By the geometric interpretation of the polynomials $\varphi_t(X,Y)$ it is obvious that $\mathcal{I}$ coincides with the set of all base points of the linear system Σ.

Proposition 3.7: *No curve in Σ passes through all affine points of $\mathcal{C}$, but there is exactly one containing $q-1$ given points from $\mathcal{C}$.*

Proof: Set

$$\varphi(X,Y) = \sum_{t\in GF(q)} \lambda_t \varphi_t(X,Y). \tag{3.9}$$

The point $P_t = \left(\frac{t}{2}, \frac{t^2}{4}\right) \in \mathcal{C}$ is in the curve of equation $\varphi(X,Y) = 0$ if and only if $\lambda_t = 0$. Therefore, it is possible to ensure that (exactly) one curve in Σ passes through $q-1$ (but not more than $q-1$) given points of $\mathcal{C}$. □

Lemma 3.8: *Let $\ell_1, \dots, \ell_{q-1}$ be $q-1$ pairwise distinct nontangent lines to $\mathcal{C}$ through an external point $P \notin \ell_\infty$ to $\mathcal{C}$. Let Γ be the algebraic curve of degree $q-1$ whose components are $\ell_1, \dots, \ell_{q-1}$. Then Γ has equation $\lambda_u\varphi_u(X,Y) + \lambda_v\varphi_v(X,Y) = 0$ with $\lambda_u + \lambda_v = 0$.*

Proof: Let r_u and r_v be the tangents to C through P, and let $Q_u(1,u,0)$ and $Q_v(1,v,0)$ be their infinite points. For any point $R(x,y)$ in $AG(2,q)$ not lying on these tangents, both $\varphi_u(X,Y)$ and $\varphi_v(X,Y)$ vanish. This together with $\lambda_u + \lambda_v = 0$ ensure that every line ℓ_i is a component of the curve of equation $\lambda_u\varphi_u(X,Y) + \lambda_v\varphi_v(X,Y) = 0$. Since Γ contains no multiple line, the assertion follows. □

A straightforward consequence of Proposition 3.7 is the following result.

Theorem 3.9: *Let Γ be an algebraic plane curve defined over the algebraic closure of $GF(q)$, q odd. If Γ passes through every point of an irreducible conic $\mathcal{C}$ of $PG(2,q)$, and through every internal point to $\mathcal{C}$, then the degree d of Γ satisfies*

$$d \geq q.$$

From now on we deal with the case $d = q$. To write an equation for Γ, choose a reference system in affine coordinates such that $\mathcal{C}$ is the parabola of equation $Y = X^2$.

Furthermore, for every $t \in GF(q)$, define the polynomial

$$\rho_t(X,Y) = \left[1 - \left(Y - tX + \frac{1}{4}t^2\right)^{q-1}\right]\left(X - \frac{t}{2}\right) \tag{3.10}$$

over $GF(q)$. Note that the algebraic curve of equation $\rho_t(X,Y) = 0$ is totally reducible, its components being the $q-1$ nontangent lines through the infinite point $Q_t = (1,t,0)$ and the polar line of $Q_t = (1,t,0)$ with respect to $\mathcal{C}$.

THEOREM 3.10: *Let $\mathcal{C}$ be the parabola of equation $Y = X^2$. If $\deg \Gamma = q$ in Theorem 3.9, then Γ has equation*

$$f(X,Y) = \sum_{t \in GF(q)} \lambda_t \rho_t(X,Y) = 0. \tag{3.11}$$

If, in addition, Γ is defined over $GF(q)$, then $\lambda_t \in GF(q)$, for any $t \in GF(q)$.

The above theorem may be rephrased using classical terminology from the theory of linear systems, see [31], for instance.

THEOREM 3.11: *The linear system of algebraic curves of degree q passing through every point of an irreducible conic $\mathcal{C}$ of $PG(2,q)$ and through every internal point of $\mathcal{C}$ has dimension $q-1$. Such points impose independent conditions on the algebraic curves of degree q which pass through them.*

We are going to prove that any algebraic curve $\mathcal{D}$ of degree q passing through every point of $\mathcal{I}(\mathcal{C}) \cup \mathcal{C}$ belongs to the linear system Σ consisting of all curves with equation

$$\sum_{t \in GF(q)} \lambda_t \rho_t(X,Y) = 0.$$

Write the equation of $\mathcal{D}$ in the form

$$a(X,Y) = \Psi_0(X,Y) + \cdots + \Psi_q(X,Y) = 0$$

where $\Psi_i(X,Y)$ is a homogeneous polynomial of degree i. We begin by showing that the polynomial $\Psi_q(X,Y) = \sum_{i=0}^{q} a_i X^i Y^{q-i}$ of degree q can be written as

$$\begin{aligned}\Psi_q(X,Y) &= \sum_{t \in GF(q)} \lambda_t X (Y - tX)^{q-1} = \\ &= \sum_{t \in GF(q)} \lambda_t X \sum_{i=0}^{q-1} \binom{q-1}{i} (-t)^i X^i Y^{q-1-i},\end{aligned} \tag{3.12}$$

for suitable $\lambda_t \in GF(q)$.

In homogeneous coordinates $\mathcal{D}$ has equation

$$a(X,Y,Z) = \Psi_0(X,Y)Z^q + \Psi_1(X,Y)Z^{q-1} \cdots + \Psi_q(X,Y) = 0.$$

Since the point $Q_\infty = (0,1,0)$ is the infinite point of $\mathcal{C}$, we have $Q_\infty \in \mathcal{D}$. Therefore $\Psi_q(0,1) = 0$ yielding $a_0 = 0$. Hence

$$\Psi_q(X,Y) = X\left[\sum_{i=1}^{q-1} a_i X^i Y^{q-1-i}\right].$$

Thus, to end the proof we only need eq. (3.7).

Note that the terms of degree q in $\rho_t(X,Y)$ are those in $X(Y-tX)^{q-1}$. If the polynomial $a(X,Y) - \sum_{t\in GF(q)} \lambda_t\rho_t(X,Y)$ were not identically zero, then the curve of equation

$$a(X,Y) - \sum_{t\in GF(q)} \lambda_t\rho_t(X,Y) = 0$$

would have degree $q-1$ and would pass through every point of $\mathcal{I}(\mathcal{C}) \cup \mathcal{C}$ contradicting Theorem 3.9. Therefore

$$a(X,Y) = \sum_{t\in GF(q)} \lambda_t\rho_t(X,Y).$$

It remains to show that the polynomials $\rho_t(X,Y)$ with t ranging over $GF(q)$ are linearly independent over the algebraic closure of $GF(q)$. This follows from the independence of their homogeneous part of highest degree, which is equivalent to the independence of the polynomials φ_t.

Remark 3.12: By the geometric interpretation of the polynomials $\rho_t(X,Y)$ it is obvious that $\mathcal{I}(\mathcal{C}) \cup \mathcal{C}$ coincides with the set of all base points of the linear system Σ.

4. - Representation of involutions of $PGL(2,q)$

Another essential tool in the investigation of Segre type theorems related to blocking sets is Dickson's classification of all subgroups of $PGL(2,q)$, see [24], [36], together with some consequences on the geometry of a conic, as stated in [2] and [3]. For the seek of completeness, a detailed outline is given here.

As usual, $PGL(2,q)$ denotes the projective linear group of the projective line over $GF(q)$ consisting of all permutations $t' = (at+b)/(ct+d)$ on $GF(q)\cup\infty$ with coefficients $a,b,c,d \in GF(q)$ such that $ad-bc \neq 0$. Note that $t' = \infty$ for $t = -d/c$ when $c \neq 0$, and for $t = \infty$ when $c = 0$. Also, $t' = a/c$ for $t = \infty$ when $c \neq 0$.

Lemma 4.1: *For $q = p^h$ and p odd prime, a complete list of subgroups of $PGL(2,q)$ together with the number N of their involutions is as follows*:

(I) *cyclic groups of order d with $d \mid (q\pm1)$, $N = 1$;*
(II) *elementary abelian groups of order p^k with $k \leq h$, $N = 0$;*
(III) *dihedral groups of order $2d$ with $d \mid (q\pm1)$, $N = d+1$;*

(IV) *groups of order $p^k s$ with $s|(p^k - 1)$ and $s|(p^h - 1)$; they are semidirect products of an elementary abelian group of order p^k with a cyclic group of order s, $N = p^k$;*

(V) *alternating group A_4, $N = 3$;*

(VI) *symmetric group S_4, $N = 9$;*

(VII) *alternating group A_5 for $q^2 - 1 \equiv 0 \pmod 5$, $N = 15$;*

(VIII) *projective linear groups $PGL(2, p^k)$ with $k|h$ and $k < h$, $N = p^{2k}$;*

(IX) *projective special groups $PSL(2, p^k)$ with $k|h$ and $k \leq h$, $N = \frac{1}{2}(p^k \pm 1)$ for $p^k \equiv \mp 1 \pmod 4$.*

Furthermore, involutions in $PGL(2, q)$ are of two types, namely

(i) $t' = -t + 4u$ for every $u \in GF(q)$, and

(ii) $t' = (mt + 4b)/(t - m)$ for every $m, b \in GF(q)$ with $m^2 + 4b \neq 0$.

Note that the involution $t' = -t + 4u$ fixes both $2u$ and ∞, while $t' = (mt + 4b)/(t - m)$ has either 2 or 0 fixed points depending on whether $m^2 + 4b$ is a nonzero square or a non-square element in $GF(q)$. From Lemma 4.1 we deduce two results.

Lemma 4.2: *Let G be any intransitive subgroup of $PGL(2, q)$ containing at least $q - 1$ involutions. If some of such involutions have no fixed point, then G is a dihedral group of order $2(q - 1)$.*

Proof: Assume first that $q \geq 13$. From Lemma 4.1, subgroups of $PGL(2, q)$ containing at least $q - 1$ involutions are dihedral groups of order $2(q \pm 1)$, the projective special group $PSL(2, q)$, semidirect products of order sq with s as in (IV), and for square q groups isomorphic to $PGL(2, \sqrt{q})$. The dihedral subgroups of order $2(q + 1)$ as well as $PSL(2, q)$ are transitive subgroups. Semidirect products as in (IV) have a fixed point.

It remains to show that every involution in $PGL(2, \sqrt{q})$ has two fixed points. Since $PGL(2, q)$ contains only one conjugacy class of subgroups isomorphic to $PGL(2, \sqrt{q})$, it suffices to show the assertion for just one subgroup $G \cong PGL(2, \sqrt{q})$. The permutations $t' = (at + b)/(ct + d)$ of $GF(q) \cup \{\infty\}$ whose coefficients a, b, c, d are in $GF(\sqrt{q})$ and satisfy $ad - bc \neq 0$ constitute such a subgroup G. Since $m^2 + 4b$ with $m,\ b \in GF(\sqrt{q})$ is always a nonzero square in $GF(q)$, the assertion follows for $q \geq 13$.

Let $q = 9, 11$. By Lemma 4.1, there is just one new entry, namely $G \cong A_5$. In both cases, A_5 is a transitive subgroup of $PGL(2, q)$. Likewise, if $q = 5, 7$ then $G \cong S_4$ and in both cases S_4 is a transitive subgroup. □

Given a subgroup G of $PGL(2, q)$, a 2-component partition $\ell_\infty = L_1 \cup L_2$ with $L_1 \cap L_2 = \emptyset$ is *G-invariant* if every $g \in G$ either takes L_1 to L_2 and vice versa (and there is at least one $g \in G$ that does it), or it preserves both L_1 and L_2. The subgroup N of G consisting of all elements which preserve both L_1 and L_2 has index 2.

LEMMA 4.3: *If a proper subgroup G of $PGL(2,q)$ contains at least $q-1$ fixed-point-free involutions then either $q \equiv 3 \pmod 4$ and $G \cong PSL(2,q)$, or $q = 11$ and $G \cong A_5$, or $q = 5,7$ and $G \cong S_4$. If, in addition, there is a G-invariant partition with two components, then either $q = 5,7$ and $G \cong S_4$, or $q = 5$ and G is a dihedral group of order 12.*

PROOF: A dihedral group of order $2(q \pm 1)$ contains at most $\frac{1}{2}(q+1)+1$ fixed-point-free involutions. This number is $q-1$ only if $q=5$ and the group is dihedral of order 12. By the proof of Lemma 4.2, $PGL(2,\sqrt{q})$ cannot occur. An involution in $PSL(2,q)$ has 2 or 0 fixed points depending on whether $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$. Furthermore, the subgroups of $PGL(2,q)$ isomorphic to A_5 are contained in $PSL(2,q)$, and the same holds for S_4 when $q=7$. Also, every subgroups of $PGL(2,5)$ isomorphic to S_4 contains 3 involutions with 2 fixed points and 6 fixed-point-free involutions. Finally, both $PSL(2,q)$ and A_5 are simple groups, and hence they do not have any subgroup of index 2. Instead, S_4 has A_4 as subgroup. □

We give a geometric representation of the involutions in $PGL(2,q)$. As before, $AG(2,q)$ will stand for the affine plane over $GF(q)$, ℓ_∞ for its infinite line, $\mathcal{C}$ for the parabola of equation $Y = X^2$, and Q_∞ for the infinite point of $\mathcal{C}$. Furthermore, r_t will denote the line of equation $Y = tX - \frac{1}{4}t^2$, for every $t \in GF(q)$.

Note that r_t is the tangent to $\mathcal{C}$ at the point $\left(\frac{1}{2}t, \frac{1}{4}t^2\right)$ and that $Q_t = (1,t,0)$ is the infinite point of r_t. Obviously, Q_t is distinct from Q_∞. The lines r_t together with ℓ_∞ are all the tangents to $\mathcal{C}$ through Q_t.

Now, choose any nontangent line ℓ to $\mathcal{C}$. Then either ℓ is a vertical line of equation $X = u$ with $u \in GF(q)$, or its equation is $Y = mX + b$ with $m, b \in GF(q)$ and $m^2 + 4b \neq 0$. Let $t \neq m$. Then r_t meets ℓ in a point R. Let r' be the other tangent line to $\mathcal{C}$ through R when $R \notin \mathcal{C}$, and $r' = r_t$ when $R \in \mathcal{C}$. The infinite Q' point of r' is called the image of Q_t under the *axial symmetry* ψ_ℓ associated to ℓ. To recover the missing value $t = m$, define $\psi_\ell(Q_m) = Q_\infty$ and $\psi(Q_\infty) = Q_m$. Then $Q' = Q_{t'}$ with t' depending on t as in the same manner as in (i) or (ii). In other words, $\psi_\ell \in PGL(2,q)$.

This representation makes it possible to interpret properties of involutions in $PGL(2,q)$ in terms of geometric configurations of the corresponding symmetry axes. In this paper, the following case is relevant.

LEMMA 4.4: *If $\psi_1, \dots, \psi_{q-1}$ are the noncentral involutions of a dihedral subgroup of $PGL(2,q)$ of order $2(q-1)$, then the corresponding symmetry axes $\ell_1, \dots, \ell_{q-1}$ have a common point P. Furthermore, P is an external point to $\mathcal{C}$, and $\ell_1, \dots, \ell_{q-1}$ together with the two tangents to $\mathcal{C}$ through P form the full pencil with base point P.*

PROOF: For any two distinct points $A, B \in l_\infty$, the subgroup D of $PGL(2,q)$ which preserves the set $\{A, B\}$ is a dihedral subgroup of order $2(q-1)$. The $q-1$ elements interchanging A and B are the noncentral involutions in D while the cyclic subgroup of D of index 2 consists of the $q-1$ elements fixing both A and B. All dihedral subgroups of order $2(q-1)$ are obtained on this way. If $A = Q_\infty$ and $B = Q_0$, then D consists of all involutions $t' = 4b/t$ together with $t' = ut$ where both b and u range over $GF(q)^*$. Note that $t' = -t$ is the unique central involution in D while lines which are symmetry axes of the corresponding noncentral involutions in D have equation $Y = b$. Hence they are all the nontangent lines through the point Q_0 showing the assertion for this case.

If $B \in \ell_\infty$ is distinct from Q_0, say $B = Q_u$, then the affinity with equation $(X, Y) \mapsto \left(X + \frac{1}{2}u, Y + uX + \frac{1}{4}u^2\right)$ preserves $\mathcal{C}$ and takes Q_0 to Q_u. This shows that the assertion holds true for the case where $A = Q_\infty$ and B is any infinite point distinct from Q_∞.

Next, let $A = Q_1$ and $B = Q_{-1}$. It is easily checked that every involution $t' = (mt-1)/(t-m)$ with $m \in GF(q) \setminus \{1, -1\}$ interchanges A and B. The same holds for the involution $t' = -t$. Thus these are all the noncentral involutions in D. Also, the axis ℓ of the axial symmetry corresponding to such an involution has equation $Y = mX - \frac{1}{4}$ and $X = 0$ respectively. All these axes pass through $P\left(0, -\frac{1}{4}\right)$. Thus they are all the nontangent lines through the point $P\left(0, -\frac{1}{4}\right)$ showing the assertion for this case.

Finally, let $A, B \in \ell_\infty \setminus \{Q_\infty\}$ any two distinct infinite points. Since $PGL(2,q)$ acts on ℓ_∞ as a 3-transitive permutation group, there is an element in $PGL(2,q)$ which fixes Q_∞ and takes Q_1 and Q_{-1} to A and B, respectively. Therefore, the assertion extends to the dihedral subgroup preserving $\{A, B\}$, and this completes the proof. □

For further results, an explicit description of the action of $PGL(2,q)$ is needed.

Let $PGL(3,q)$ be the projective linear group of the projective plane $PG(2,q)$ over $GF(q)$ and let $\mathcal{C}$ be an irreducible conic of $PG(2,q)$. Denote by Γ the subgroup of $PGL(3,q)$ preserving $\mathcal{C}$.

If $\mathcal{C}$ is the conic of equation $YZ = X^2$ then Γ consists of all linear collineations $\gamma(a,b,c,d)$ with matrix representation $x \mapsto xM$, $x = (X, Y, Z)$ and

$$M = \begin{pmatrix} ad + bc & 2ab & 2cd \\ ac & a^2 & c^2 \\ bd & b^2 & d^2 \end{pmatrix}$$

where $a, b, c, d \in GF(q)$ and $ad - bc \neq 0$, see [23], Theorem 2.37.

Let $PGL(2,q)$ be the projective linear group of the projective line ℓ_∞ over $GF(q)$. As it is well known $\Gamma \cong PGL(2,q)$ and Γ acts on $\mathcal{C}$ as $PGL(2,q)$ in its sharply 3-transitive permutation representation that is in its natural representation on ℓ_∞.

If ℓ_∞ is given by $Z = 0$, this representation is obtained in the following way. Identify points $P = (u, u^2, 1) \in \mathcal{C}$ with points $Q_u = (1, u, 0) \in \ell_\infty$, and $\gamma(a, b, c, d)$ with the linear fractional transformation

$$u' = (au + b)/(cu + d). \tag{4.1}$$

Then Γ acts on $\mathcal{C}$ as $PGL(2, q)$ on ℓ_∞.

Let Γ_0 be the subgroup of Γ consisting of all elements (4.1) with $a, b, c, d \in GF(\sqrt{q})$. Clearly $\Gamma_0 \cong PGL(2, \sqrt{q})$ and Γ_0 preserves the Baer subplane π_0 of the Baer involution $(X, Y, Z) \rightarrow (X^{\sqrt{q}}, Y^{\sqrt{q}}, Z^{\sqrt{q}})$, which is the canonical subplane $PG(2, \sqrt{q})$ of $PG(2, q)$ coordinatised by $GF(\sqrt{q})$.

Every involution in Γ_0 has two fixed points on $\mathcal{C}$. In fact $\gamma(a, b, c, d)$ is an involution if and only if $a = -d$. Then the point $P(u, u^2, 1)$ is a fixed point of $\gamma(a, b, c, d)$ when

$$cu^2 - 2au - b = 0. \tag{4.2}$$

Since $a, b, c \in GF(\sqrt{q})$, (4.2) has two solutions.

Note that $\mathcal{C}_0 = \mathcal{C} \cap \pi_0$ is a conic in π_0. Also, a line of π_0 is either a tangent or a secant of $\mathcal{C}_0$ or an external line to $\mathcal{C}_0$, and in the latter case the line is a secant of $\mathcal{C}$.

The previous geometric representation of $PGL(2, q)$ in which an involution ψ_ℓ of $PGL(2, q)$ is associated to each nontangent line ℓ to $\mathcal{C}$ can be made more explicit. In fact, ψ_ℓ is the restriction on $\mathcal{C}$ of the involutory homology $h_\ell \in \Gamma$ of axis ℓ whose centre is the pole of ℓ with respect to $\mathcal{C}$.

LEMMA 4.5: *Let $\psi_1, \ldots, \psi_s$ be involutions of $PGL(2, q)$. Then $\langle \psi_1, \ldots, \psi_s \rangle$ is isomorphic to $\langle h_1, \ldots, h_s \rangle$.*

PROOF: It suffices to note that the only collineation fixing $\mathcal{C}$ pointwise is the identity. □

In studying $\langle \psi_1, \ldots, \psi_s \rangle$ three cases are distinguished. Lemma 4.2 together with the following two lemmas depending on Dickson's classification will play a role.

LEMMA 4.6: *Let G be any intransitive subgroup of $PGL(2, q)$, containing at least q involutions. Then every involution in G has two fixed points if and only if either $G \cong PGL(2, \sqrt{q})$, q square, or G is a semidirect product of an elementary abelian group of order q with a cyclic group of even order.*

PROOF: Every involution in a subgroup of $PGL(2, q)$ isomorphic to $PGL\ (2, \sqrt{q})$ has two fixed points. A subgroup of $PGL(2, q)$ which is the semidirect product of an elementary abelian group of order q with a cyclic group of even order has a fixed point hence every involution must fix two points.

To prove the converse, assume first that $q \geq 13$. By the classification of subgroups of $PGL(2,q)$, see Lemma 4.1, the subgroups of $PGL(2,q)$ containing at least q involutions are dihedral groups of order $2(q \pm 1)$, groups isomorphic to $PSL(2,q)$, groups of order qs with $s|(q-1)$, which are semidirect products of an elementary abelian group of order q with a cyclic group of order s, and for square q, groups isomorphic to $PGL(2,\sqrt{q})$.

From this we infer Lemma 4.6 for $q \geq 13$ since dihedral subgroups of order $2(q+1)$ as well as subgroups isomorphic to $PSL(2,q)$ are transitive subgroups, whereas the dihedral subgroups of order $2(q-1)$ contain some fixed point free involution.

If $q = 9, 11$ then, G can also be isomorphic to A_5, see Lemma 4.1, but A_5 is a transitive subgroup of $PGL(2,q)$ for $q = 9, 11$.

Likewise, if $q = 5, 7$ then $G \cong S_4$ and in both cases again S_4 is a transitive subgroup. □

Lemma 4.7: *If $\psi_1, \dots, \psi_q$ are the involutions of a subgroup G of $PGL(2,q)$ isomorphic to $PGL(2,\sqrt{q})$, then the corresponding symmetry axes $\ell_1, \dots, \ell_q$ are lines of a Baer subplane of $PG(2,q)$. Such a Baer subplane meets $\mathcal{C}$ in a conic $\mathcal{C}_0$ and $\ell_1, \dots, \ell_q$ are all nontangent lines of $PG(2,\sqrt{q})$ to $\mathcal{C}_0$. In particular all the lines $\ell_1, \dots, \ell_q$ are secants to $\mathcal{C}$.*

Proof: $PGL(2,\sqrt{q})$ and hence G, is generated by its involutions. According to Lemma 4.5, let $H = < h_1, \dots, h_q >$ with $h_1, \dots, h_q \in \Gamma$ such that $G \cong H$. By the classification of subgroups of $PGL(2,q)$ any two subgroups isomorphic to $PGL(2,\sqrt{q})$ are conjugate in $PGL(2,q)$. Hence, $H = \alpha \Gamma_0 \alpha^{-1}$ for some $\alpha \in \Gamma$.

Furthermore, the Baer subplane preserved by H is the image of π_0 by α. Therefore, it suffices to show the assertion for Γ_0. The axes of involutions in Γ_0 are lines of π_0 which are not tangent to $\mathcal{C}_0 = \mathcal{C} \cap \pi_0$. Every nontangent line of $\mathcal{C}_0$ meets $\mathcal{C}$ in 2 points, and hence the result follows. □

The following two results come from [25] where a purely theoretic approach is used. An alternative proof using coordinates is also possible; the necessary computations can be carried out as in the proof of Lemma 4.4.

Lemma 4.8: *If $\psi_1, \dots, \psi_q$ are the involutions of a subgroup G of $PGL(2,q)$ of order sq with $s|q-1$, then the corresponding symmetry axes $\ell_1, \dots, \ell_q$ have a common point P on $\mathcal{C}$.*

Lemma 4.9: *Let $\psi_1, \dots, \psi_{q-1}$ be the noncentral involutions of a dihedral subgroup G of $PGL(2,q)$ of order $2(q-1)$. The following assertions hold.*

(i) *The symmetry axes $\ell_1, \dots, \ell_{q-1}$ of $\psi_1, \dots, \psi_{q-1}$ have a common point P;*

(ii) *P is an external point to $\mathcal{C}$, and $\ell_1, \dots, \ell_{q-1}$ together with the two tangents to $\mathcal{C}$ through P form the full pencil with base point P;*

(iii) *the polar line of P w.r.t $\mathcal{C}$ is the symmetry axes of the central involution of G.*

5. - Blocking sets of external lines

The following classification theorem comes from [2].

Theorem 5.1: *Let $\mathcal{C}$ be an irreducible conic in $PG(2,q)$, q odd. Let $\mathcal{B}$ be a point-set in $PG(2,q)$ which meets every external line to $\mathcal{C}$. Then $|\mathcal{B}| \geq q-1$ with equality occurring for $q=3$ and $q \geq 9$ in the "linear" case only, that is when $\mathcal{B}$ consists of all points of a secant r of $\mathcal{C}$ minus the two common points of r and $\mathcal{C}$. For $q=5,7$ there exists just one more example, up to projectivities.*

The proof given here is essentially the same as in [2] and uses the results stated in the previous sections.

Since q is odd, an orthogonal polarity is associated with $\mathcal{C}$. This allows us to state Theorem 5.1 and prove it in its dual form: if a line-set $\mathcal{L}$ covers the set $I(\mathcal{C})$ of all internal points to $\mathcal{C}$, then $|\mathcal{L}| \geq q-1$, and equality only holds when $\mathcal{L}$ consists of all lines through an external point P minus the two tangents to $\mathcal{C}$ through P. In other words, $\mathcal{L}$ together with the tangents to $\mathcal{C}$ constitute the full pencil with base point P.

The first statement in the dual of Theorem 5.1 is a corollary to Theorem 3.1. Henceforth we assume $|\mathcal{L}| = q-1$.

Lemma 5.2: *At least half of the lines in $\mathcal{L}$ are external to $\mathcal{C}$.*

Proof: Assume that $\mathcal{L}$ consists of n secants together with $q-1-n$ external lines to $\mathcal{C}$. Since each external line contains $\frac{1}{2}(q+1)$ internal points to $\mathcal{C}$ whereas each secant contains $\frac{1}{2}(q-1)$ internal points

$$(q-1-n)\frac{(q+1)}{2} + n\frac{(q-1)}{2} \geq \frac{q(q-1)}{2},$$

hence $n \leq \frac{1}{2}(q-1)$. □

We continue to work on an affine plane $AG(2,q)$ whose infinite line ℓ_∞ is tangent to $\mathcal{C}$. The conic $\mathcal{C}$ is a parabola and we may assume $\mathcal{C}$ to be in its canonical position with equation $Y=X^2$. Let $\ell_1, \ldots, \ell_{q-1}$ denote the lines in $\mathcal{L}$. Then ℓ_i has equation $L_i(X,Y) = Y - u_iX + v_i$ with $u_i\, v_i \in GF(q)$, and the infinite point Q_i of ℓ_i has homogeneous coordinates $(1, u_i, 0)$. Set $L(X,Y) = L_1(X,Y) \cdots L_{q-1}(X,Y)$. For any $t \in GF(q)$, let Q_t denote the point of homogeneous coordinates $(1,t,0)$. Clearly, Q_t is the infinite point of the tangent line r_t to $\mathcal{C}$ at the point $P\Big(\frac{1}{2}t, \frac{1}{4}t^2\Big)$. Note that r_t has equation $Y - tX + \frac{1}{4}t^2 = 0$. By Theorem 3.2, there are $\lambda_t \in GF(q)$ such that

$$L(X,Y) = \sum_{t \in GF(q)} \lambda_t \Big(1 - \Big(Y - tX + \frac{1}{4}t^2\Big)^{q-1}\Big). \tag{5.1}$$

Lemma 5.3: *$\mathcal{L}$ contains a secant of $\mathcal{C}$ if and only if $\lambda_t = 0$ for at least one $t \in GF(q)$.*

Proof: Assume that $\mathcal{L}$ contains a secant of $\mathcal{C}$ and let P denote one of their common points. Write $P = \left(\frac{1}{2}u, \frac{1}{4}u^2\right)$ with $u \in GF(q)$. Then $L\left(\frac{1}{2}u, \frac{1}{4}u^2\right) = 0$. Furthermore, $1 - \left(\frac{1}{4}u^2 - \frac{1}{2}ut + \frac{1}{4}t^2\right)^{q-1} = 1 - \left[\frac{1}{2}(u-t)\right]^{2(q-1)}$ is equal to 1 for $u = t$, and it vanishes otherwise. By (5.1), $\lambda_u = 0$. Conversely, if $\lambda_u = 0$, then (5.1) yields that $L\left(\frac{1}{2}u, \frac{1}{4}u^2\right) = 0$, and hence some line in $\mathcal{L}$ contains the point $P = \left(\frac{1}{2}u, \frac{1}{4}u^2\right)$ of $\mathcal{C}$. □

Set $\lambda = \sum_{t \in GF(q)} \lambda_t$.

Lemma 5.4: *The infinite point Q_u, $u \in GF(q)$, is covered by some line of $\mathcal{L}$ if and only if $\lambda_u = \lambda$.*

Proof: Write (5.1) in homogeneous coordinates:

$$L(X,Y,Z) = \prod_{j=1}^{q-1}(Y - u_jX + v_jZ) = \sum_{t \in GF(q)} \lambda_t \left(Z^{q-1} - \left(Y - tX + \frac{1}{4}t^2Z\right)^{q-1}\right).$$

The point Q_u lies on some line in $\mathcal{L}$ if and only if $L(1,u,0) = 0$. On the other hand, $L(1,u,0) = -\lambda + \lambda_u$ since $(u-t)^{q-1}$ equals 0 for $u = t$ and 1 otherwise. □

For the rest of the proof we distinguish two cases according as λ vanishes or does not.

Case $\lambda = 0$. Define Λ to be the set of all infinite points Q_u covered by lines in $\mathcal{L}$ together with the tangency point Q_∞ of ℓ_∞ on $\mathcal{C}$. Note that Λ does not contain all infinite points.

As we have seen in Section 4, every line $\ell_j \in \mathcal{L}$ defines an involution ψ_j in $PG(2,q)$ viewed as the linear collineation group of the infinite line ℓ_∞.

Lemma 5.5: *Each involution ψ_j preserves Λ.*

Proof: Let Q_u be the infinite point of ℓ_j. By a previous result, ψ_j interchanges Q_u with Q_∞. For any point $Q_t \neq Q_u$, let Q_v be the image of Q_t by ψ_j. If $Q_t = Q_v$, then the assertion trivially holds. Otherwise, the tangent lines r_t and r_v are distinct and they meet in a point $P(x,y)$ of ℓ_j. Hence $L(x,y) = 0$. Let $w \in GF(q)$. Then $\left(y - wx + \frac{1}{4}w^2\right)^{q-1}$ vanishes for $w = t$ and $w = v$, otherwise it is equal to 1. From (5.1), $\lambda_t + \lambda_v = 0$. By Lemma 5.4, $Q_t \in \Lambda$ yields $\lambda_t = 0$. Hence $\lambda_v = 0$, and by Lemma 5.4 the assertion follows. □

Lemma 5.5 implies that Λ is invariant under the subgroup G of $PGL(2,q)$ generated by the involutions $\psi_1, \ldots, \psi_{q-1}$. According to Lemma 5.2, some of these involutions have no fixed points. Hence, from Lemmas 4.2 and 4.4 we obtain Theorem 5.1 in its dual form.

CASE $\lambda \neq 0$. This time, we define Λ^+ to be the set of all infinite points Q_t covered by lines in $\mathcal{L}$. By Lemma 5.4, Λ^+ comprises all Q_t such that $\lambda_t = \lambda$. We will also need the set Λ^- consisting of all infinite points Q_t with $\lambda_t = -\lambda$ together with Q_∞.

LEMMA 5.6: *Each involution ψ_j takes Λ^+ to Λ^-.*

PROOF: Let $Q_u \in \Lambda^+$. If Q_u lies in ℓ_j, then ψ_j interchanges Q_u with Q_∞. For any point $Q_u \notin \ell_j$ let Q_v the image of Q_u under ψ_j. We show that $Q_u \neq Q_v$. If $Q_u = Q_v$ then ℓ_j contains the tangency point $P\left(\frac{1}{2}u, \frac{1}{4}u^2\right)$ of the affine tangent line to $\mathcal{C}$ through Q_u. Therefore $L\left(\frac{1}{2}u, \frac{1}{4}u^2\right) = 0$. By (5.1),

$$0 = \sum_{t \in GF(q)} \lambda_t \left(1 - \left(\frac{1}{4}u^2 - \frac{1}{2}ut + \frac{1}{4}t^2\right)^{q-1}\right) = \sum_{t \in GF(q)} \lambda_t (1 - (u-t)^{q-1}).$$

Since, $(u-t)^{q-1} = 1$ for every t distinct from u, this yields $\lambda_u = 0$, a contradiction with $\lambda \neq 0$. So, we may assume $Q_u \neq Q_v$.

Now, arguing as in the proof of Lemma 5.5, $\lambda_u + \lambda_v = 0$ follows. Since $\lambda_u = \lambda$, this yields $\lambda_v = -\lambda$ showing indeed that $Q_v \in \Lambda^-$. Conversely, if $Q_v \in \Lambda^-$, then the image of Q_v under ψ_j is in Λ^+. This has already been noted for $Q_v = Q_\infty$ at the beginning. Also, the preceding arguments remain valid when $+$ and $-$ are interchanged giving a proof for the assertion. □

Set $\Lambda = \Lambda^+ \cup \Lambda^-$. Then the previous lemma shows that Lemma 5.5 holds true for the case $\lambda \neq 0$. As before, this yields that Λ is invariant under the subgroup G of $PGL(2,q)$ generated by the involutions $\psi_1, \ldots, \psi_{q-1}$.

If Λ is a proper subset of ℓ_∞, we may argue as before by using Lemmas 5.2, 4.2 and 4.4. The conclusion is that the lines of $\mathcal{L}$ are those of a pencil with an external base point P minus the two tangents to $\mathcal{C}$ through P. But this cannot actually occur in the present situation by Lemma 3.8.

If Λ consists of all points in ℓ_∞, then no λ_t vanishes. By Lemma 5.3, every line in $\mathcal{L}$ is external to $\mathcal{C}$ showing that no involution ψ_i has fixed point on $\mathcal{C}$. By Lemma 4.3, we are left with three sporadic cases, namely $q = 5, 7$ and $G \cong S_4$, and $q = 5$ and G is a dihedral group of order 12.

CASE $q = 5$. A nonlinear example of a line-set $\mathcal{L}$ covering $\mathcal{I}(\mathcal{C})$ consists of the four external lines to $\mathcal{C}$:

$$\ell_1 : Y = 4X + 4; \;\; \ell_2 : Y = 3X + 2; \;\; \ell_3 : Y = X + 3; \;\; \ell_4 : Y = X + 4.$$

Set

$$f(X,Y) = (Y - (4X+4))(Y - (3X+2)((Y - (X+3))(Y - (X+4)).$$

As before, let

$$\varphi_t(X,Y) = 1 - \left(Y - tX + \frac{1}{4}t^2\right)^4$$

for $t \in GF(5)$. It is straightforward to check that

$$f(X,Y) = \sum_{t \in GF(5)} \lambda_t \varphi_t(X,Y)$$

with $\lambda_0 = \lambda_2 = 1$ and $\lambda_1 = \lambda_3 = \lambda_4 = -1$. In particular,

$$\lambda = \sum_{t \in GF(5)} \lambda_t = -1.$$

The involutions in $PGL(2,5)$ which correspond to the lines $\ell_1, \ldots, \ell_4$ are

$$\psi_1 : t' = \frac{4t+1}{t+1}; \qquad \psi_2 : t' = \frac{3t+3}{t+2}; \qquad \psi_3 : t' = \frac{t+2}{t+4}; \qquad \psi_4 : t' = \frac{t+1}{t+4}.$$

The subgroup $G = \langle \psi_1, \psi_2, \psi_3, \psi_4 \rangle$ is a dihedral group of order 12. In $PGL(2,5)$, there exist 10 dihedral subgroups of order 12, and they are pairwise conjugate under $PGL(2,5)$. So, we have 10 projectively equivalent nonlinear examples. A computer aided exhaustive search shows that no more nonlinear example exists. In particular, the possibility $G \cong S_4$ does not actually occur for $q = 5$.

Case $q = 7$. A nonlinear example of a line-set $\mathcal{L}$ covering $\mathcal{I}(\mathcal{C})$ consists of six external lines to $\mathcal{C}$:

$$\begin{cases} \ell_1 : Y = 5; & \ell_2 : Y = 2X + 2; \quad \ell_3 : Y = 2X + 4; \\ \ell_4 : Y = 2X + 5; & \ell_5 : Y = 5X + 5; \quad \ell_6 : Y = X + 1. \end{cases}$$

Set

$$\begin{aligned} f(X,Y) = {} & (Y-5)(Y-(2X+2))(Y-(2X+4)) \times \\ & \times (Y-(2X+5))(Y-(5X+5))(Y-(X+1)), \end{aligned}$$

and

$$\varphi_t(X,Y) = 1 - \left(Y - tX + \frac{1}{4}t^2\right)^6$$

for $t \in GF(7)$. It is easy to check that $f(X,Y) = \sum_{t \in GF(7)} \lambda_t \varphi_t(X,Y)$ with $\lambda_0 = = \lambda_1 = \lambda_3 = \lambda_6 = 2$ and $\lambda_2 = \lambda_4 = \lambda_5 = 5$. In particular, $\lambda = \sum_{t \in GF(5)} = \lambda_t = 2$. The involutions in $PGL(2,7)$ which correspond to the lines $\ell_1, \ldots, \ell_6$ are

$$\begin{aligned} &\psi_1 : t' = \frac{6}{t}; \qquad \psi_2 : t' = \frac{2t+1}{t+5}; \qquad \psi_3 : t' = \frac{2t+2}{t+5}; \\ &\psi_4 : t' = \frac{2t+6}{t+5}; \qquad \psi_5 : t' = \frac{5t+6}{t+2}; \qquad \psi_6 : t' = \frac{t+4}{t+6}. \end{aligned}$$

Furthermore, $G = \langle \psi_1, \dots, \psi_6 \rangle \cong S_4$. In $PGL(2,7)$, there exist 14 subgroups isomorphic to S_4, and they are pairwise conjugate under $PGL(2,7)$. So, we have 14 projectively equivalent nonlinear examples. As for $q = 5$, a computer-aided exhaustive search shows that no other nonlinear example exists.

6. - Blocking sets of nontangent lines

The classification theorem and its proof come from [3].

THEOREM 6.1: *Let $\mathcal{C}$ be an irreducible conic in $PG(2,q)$, q odd and let $\mathcal{B}$ be a point set in $PG(2,q)$ which meets every external and tangent line to $\mathcal{C}$. Then $|\mathcal{B}| \geq q$ with equality occurring in the following cases*:

- *$\mathcal{B}$ consists of all points of a tangent to C minus the tangency point*;
- *$\mathcal{B}$ consists of all points of a secant r of $\mathcal{C}$ different from the two common points of r and $\mathcal{C}$, plus the pole of r with respect to $\mathcal{C}$*;
- *$\mathcal{B}$ consists of all points of a Baer subplane $PG(2,\sqrt{q})$ intersecting $\mathcal{C}$ in a conic $\mathcal{C}_0$ of $PG(2,\sqrt{q})$, minus the points of $\mathcal{C}_0$.*

As in the preceding section, Theorem 6.1 is stated and proven in its dual form: let $\mathcal{I}(\mathcal{C})$ be the set of all internal points of $\mathcal{C}$. If a line set $\mathcal{L}$ covers the set $I(\mathcal{C}) \cup \mathcal{C}$ then $|\mathcal{L}| \geq q$, and equality holds in the following cases:

- $\mathcal{L}$ consists of all lines through a point P on $\mathcal{C}$ minus the tangent at P to $\mathcal{C}$;
- $\mathcal{L}$ consists of all lines through an external point P different from the two tangents to $\mathcal{C}$, plus the polar line of P with respect to $\mathcal{C}$;
- $\mathcal{L}$ consists of all lines of a Baer subplane $PG(2,\sqrt{q})$ intersecting $\mathcal{C}$ in a conic $\mathcal{C}_0$ of $PG(2,\sqrt{q})$ different from the tangent lines to $\mathcal{C}_0$.

The first statement in the dual of Theorem 6.1 is a corollary to Theorem 3.9. Henceforth we assume $|\mathcal{L}| = q$.

LEMMA 6.2: *No line in $\mathcal{L}$ is tangent to $\mathcal{C}$.*

PROOF: In the preceding section, sets of $q-1$ lines covering all internal points to $\mathcal{C}$ are classified. If $\mathcal{L}'$ denotes such a set then, either there is an external point P to $\mathcal{C}$ such that $\mathcal{L}'$ consists of all nontangent lines to $\mathcal{C}$ through P, or $q = 5,7$ and all the lines of $\mathcal{L}'$ are external to $\mathcal{C}$.

Now, assume on the contrary that a line $\ell \in \mathcal{L}$ is tangent to $\mathcal{C}$ at L. Removing ℓ from $\mathcal{L}$ gives a set of lines $\mathcal{L}'$ covering all internal points to $\mathcal{C}$ and all points of $\mathcal{C}$ different from L. Therefore $\mathcal{L}'$ consists of all nontangent lines to $\mathcal{C}$ through an external point P to $\mathcal{C}$.

Let P_1, P_2 be the tangency points of the tangents to $\mathcal{C}$ through P. Then neither P_1 nor P_2 is covered by $\mathcal{L}'$, and hence both must be covered by ℓ. But this is impossible as ℓ is a tangent to $\mathcal{C}$. □

We continue to work on an affine plane $AG(2,q)$ whose infinite line ℓ_∞ is tangent to $\mathcal{C}$. The conic $\mathcal{C}$ is a parabola and we may assume $\mathcal{C}$ to be in its canonical position with equation $Y = X^2$. Let $\ell_1, \dots, \ell_q$ denote the lines in $\mathcal{L}$. Then ℓ_i has either equation $L_i(X,Y) = Y - u_iX + v_i = 0$ with $u_i\, v_i \in GF(q)$, and the infinite point Q_i of ℓ_i has homogeneous coordinates $(1, u_i, 0)$, or ℓ_i has equation $L_i(X,Y) = X - u_i = 0$ with $u_i \in GF(q)$ and $Q_\infty = (0,1,0)$ is its infinite point.

Set $L(X,Y) = L_1(X,Y) \cdots L_q(X,Y)$. For any $t \in GF(q)$, let Q_t denote the point of homogeneous coordinates $(1,t,0)$. Clearly, Q_t is the infinite point of the tangent line q_t to $\mathcal{C}$ at the point $P\Big(\frac{1}{2}t, \frac{1}{4}t^2\Big)$. Note that q_t has equation $Y - tX + \frac{1}{4}t^2 = 0$.

By Theorem 3.10, there are $\lambda_t \in GF(q)$ such that

$$L(X,Y) = \sum_{t \in GF(q)} \lambda_t \Big[1 - \Big(Y - tX + \frac{1}{4}t^2\Big)^{q-1}\Big]\Big(X - \frac{t}{2}\Big). \tag{6.1}$$

Set $\lambda = \sum\limits_{t \in GF(q)} \lambda_t$.

Lemma 6.3: *The infinite point Q_u, $u \in GF(q)$, is covered by some line of $\mathcal{L}$ if and only if $\lambda_u = \lambda$.*

Proof: Write (6.1) in homogeneous coordinates:

$$L(X,Y,Z) = \sum_{t \in GF(q)} \lambda_t \Big[Z^{q-1} - \Big(Y - tX + \frac{1}{4}t^2Z\Big)^{q-1}\Big]\Big(X - \frac{t}{2}Z\Big).$$

The point Q_u lies on some line in $\mathcal{L}$ if and only if $L(1,u,0) = 0$. On the other hand, $L(1,u,0) = -\lambda + \lambda_u$ since $(u-t)^{q-1}$ equals 0 for $u = t$ and 1 otherwise. □

Define Λ to be the set of all infinite points Q_u covered by lines in $\mathcal{L}$ together with the tangency point Q_∞ of ℓ_∞ on $\mathcal{C}$. Note that Λ does not contain all infinite points.

As we have seen in Section 4, every line $\ell_j \in \mathcal{L}$ defines an involution ψ_j in $PGL(2,q)$ viewed as the linear collineation group of the infinite line ℓ_∞.

Lemma 6.4: *Each involution ψ_j preserves Λ.*

Proof: Let Q_u be the infinite point of ℓ_j. By a previous result, ψ_j interchanges Q_u with Q_∞. For any point $Q_t \neq Q_u$, let Q_v be the image of Q_t by ψ_j. If $Q_t = Q_v$, then the assertion trivially holds. Otherwise, the tangent lines q_t and q_v are distinct and they meet in a point $P(x,y)$ of ℓ_j where $x = \frac{1}{4}(t+v)$. Hence $L(x,y) = 0$. Let $w \in GF(q)$. Then $\Big(y - wx + \frac{1}{4}w^2\Big)^{q-1}$ vanishes for $w = t$ and $w = v$, otherwise it is equal to 1. From (6.1),

$$\lambda_t\Big(x - \frac{t}{2}\Big) + \lambda_v\Big(x - \frac{v}{2}\Big) = \frac{1}{4}(v-t)(\lambda_t - \lambda_v) = 0.$$

By Lemma 6.3, $Q_t \in \Lambda$ yields $\lambda_t = \lambda$. Hence also $\lambda_v = \lambda$, and by Lemma 6.3 the assertion follows. □

Lemma 6.4 implies that Λ is invariant under the subgroup G of $PGL(2, q)$ generated by the involutions $\psi_1, \dots, \psi_q$. If $\mathcal{L}$ contains some external lines then some of these involutions have no fixed point. Hence, from Lemmas 4.2, and 4.9, $\mathcal{L}$ consists of all lines through an external point P different from the two tangents to $\mathcal{C}$, plus the polar line of P with respect to $\mathcal{C}$.

Otherwise, $\mathcal{L}$ consists of all secant lines to C and every involution ψ_i has two fixed points. Hence from Lemma 4.6, G is either a group of order qs with $s|q-1$, or it is isomorphic to $PGL(2, \sqrt{q})$. In the former case, from Lemma 4.8, $\mathcal{L}$ consists of all lines through a point P on $\mathcal{C}$ minus the tangent at P to $\mathcal{C}$.

Finally, when G is isomorphic to $PGL(2, \sqrt{q})$, then from Lemma 4.7 we have that $\mathcal{L}$ is the set of lines of a Baer subplane π_0 minus the tangents to the conic $\mathcal{C} \cap \pi_0$ and Theorem 6.1 follows.

REFERENCES

[1] L. M. Abatangelo - G. Raguso, *Una caratterizzazione degli archi chiusi giacenti su una conica di piano pascaliano di caratteristica due*, Rend. Mat., **1** (7) (1981), 39-45.

[2] A. Aguglia - G. Korchmáros, *Blocking sets of external lines to a conic in PG(2, q), q odd*, Combinatorica, **26** (2006), 379-394.

[3] A. Aguglia - G. Korchmáros, *Blocking-sets of nonsecant lines to a conic in PG(2, q), q odd*, J. Combin. Des., **13** (2005), 292-301.

[4] A. Aguglia - G. Korchmáros - A. Siciliano Minimal covering of all chords of a conic in *PG*$(2, q)$, q even Bull. Belgian Math. Soc. Simon Stevin, **12** (2005), 651-655.

[5] S. Ball, *Polynomials in finite geometries*, in "Surveys in combinatorics", Canterbury, 1999, pp. 17-35, London Math. Soc. Lecture Note Ser., 267, Cambridge Univ. Press, Cambridge, 1999.

[6] A. Blokhuis, *Extremal problems in finite geometries*, Bolyai Soc. Mathematical Studies, **3** (1991), 111-135.

[7] A. Blokhuis, *Polynomials in finite geometries and combinatorics*, in "Surveys in combinatorics", Keele, 1993, pp. 35-52, London Math. Soc. Lecture Note Ser., **187**, Cambridge Univ. Press, Cambridge, 1993.

[8] A. Blokhuis, *Combinatorial problems in finite geometry and lacunary polynomials*, Proceedings of the International Congress of Mathematicians, Vol. III, Beijing, 2002, pp. 537-545, Higher Ed. Press, Beijing, 2002.

[9] A. Blokhuis - F. Mazzocca, *Lifts of nuclei in finite projective spaces*, Finite Geometry and Combinatorics, Deinze, 1992, London Math. Soc. Lecture Note Ser., **191**, 31-36, Cambridge Univ. Press, Cambrige, 1993.

[10] A. Blokhuis - H. A. Wilbrink, *A characterization of exterior lines of certain sets of points in* PG$(2, q)$, Geom. Dedicata, **23** (1987), 253-254.

[11] E. Boros - Z. Füredi - J. Kahn, *Maximal intersecting families and affine regular polygons in* PG$(2, q)$, J. Combin. Theory Ser. A, **52** (1989), 1-9.

[12] A. Bruen - J. C. Fisher, *The Jamison method in Galois geometries*, Des. Codes Cryptogr., **1** (1991), 199-205.

[13] A. Bruen - J. A. Thas, *Flocks, chains and configurations in finite geometries*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur., **59** (8) (1975), 744-748 (1976).

[14] W. E. Cherowitzo - L. D. Holder, *Hyperfocused Arcs*, Bull. Belgian Math. Soc. Simon Stevin, to appear.

[15] D. Drake, *Hyperovals in nets of small degree*, J. Combin. Des., **10** (2002), 322-334.

[16] D. Drake - K. Keating, *Ovals and hyperovals in Desarguesian nets*, Des. Codes Cryptogr., **31** (2004), 195-212.

[17] P. Erdös - L. Lovász, *Problems and results on 3-chromatic hypergraphs and some related questions*, Colloq. Math. Soc. János Bolyai, **10**, 609-627, North-Holland, Amsterdam, 1975.

[18] G. Faina - G. Korchmáros, *Risultati intorno ad una congettura su archi chiusi*, Rend. Mat., **1** (7) (1981), 55-61.

[19] M. Giulietti, *Blocking Sets of External Lines to a Conic in $PG(2, q)$, q even*, European J. Combin. Des., **28** (2007), 36-42.

[20] M. Giulietti - E. Montanucci, *On hyperfocused arcs in $PG(2, q)$*, Discrete Math., **306** (2006), 3307-3314.

[21] V. D. Goppa, *Geometry and Codes*, Kluwer, 1988.

[22] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second Edition, Oxford Mathematical monographs, New York, 1985.

[23] D. R. Hughes - F. C. Piper, *Projective Planes*, Springer Verlag, 1982.

[24] B. Huppert, *Endliche Gruppen I*, Springer Verlag, 1967.

[25] G. Korchmáros, *A combinatorial characterization of the dihedral subgroups of order $2(p^r + 1)$ of $PGL(2, p^r)$*, Geom. Dedicata, **9** no. 3 (1980), 381-384.

[26] R. Lidl - H. Niederreiter, *Finite Fields*, Cambridge University Press, 1984.

[27] F. Mazzocca, *Blocking sets with respect to special families of lines and nuclei of θ_n-sets in finite n-dimensional projective and affine spaces*, Mitt. Math. Sem. Giessen, **201** (1991), 109-117.

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

[29] B. Segre, *Le geometrie di Galois*, Ann. Mat. Pura Appl., **48** (4) 1959, 1-96.

[30] B. Segre - G. Korchmáros, *Una proprietà degli insiemi di punti di un piano di Galois caratterizzante quelli formati dai punti delle singole rette esterne ad una conica*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur., **62** (8) (1977), 613-619.

[31] A. Seidenberg, *Elements of the Theory of Algebraic Curves*, Addison Wesley, Reading, Massachusetts, 1969.

[32] G. J. Simmons, *Sharply focused sets of lines on a conic in $PG(2, q)$*, Combinatorics, graph theory, and computing, Proc. 20th Southeast Conf., Boca Raton/FL, USA, 1989, Congr. Numerantium, **73** (1990), 181-204.

[33] T. Szönyi, *Some applications of algebraic curves in finite geometry and combinatorics*, Surveys in combinatorics, London, 1997, pp. 197-236, London Math. Soc. Lecture Note Ser., **241**, Cambridge Univ. Press, Cambridge, 1997.

[34] T. Szönyi - F. Wettl, *On complexes in a finite abelian group, I and II*, Proc. Japan Acad. Ser. A Math. Sci., **64** (1988), 245-248 and **64** (1988), 286-287.

[35] T. Szönyi - Zs. Weiner, *On some stability theorems in finite geometry*, preprint.

[36] R. C. Valentini - M. L. Madan, *A Hauptsatz of L. E. Dickson and Artin-Schreier extensions*, J. Reine Angew. Math., **318** (1980), 156-177.

[37] F. Wettl, *On the nuclei of a pointset of a finite projective plane*, J. Geom., **30** (1987), 157-163.

Direttore responsabile: Prof. A. Ballio - Autorizz. Trib. di Roma n. 7269 dell'8-12-1959
«Monograf» - Via Collamarini, 5 - Bologna