COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **26** (4) (2006) 379–394

BLOCKING SETS OF EXTERNAL LINES TO A CONIC IN $PG(2,q)$, q ODD

ANGELA AGUGLIA*, GÁBOR KORCHMÁROS*

Received October 17, 2003

We determine all point-sets of minimum size in $PG(2,q)$, q odd that meet every external line to a conic in $PG(2,q)$. The proof uses a result on the linear system of polynomials vanishing at every internal point to the conic and a corollary to the classification theorem of all subgroups of $PGL(2,q)$.

1. Introduction

Let $PG(2,q)$ be the desarguesian projective plane of order q over the finite field $GF(q)$. A point-set which blocks the lines, that is, is incident with each line, is called a blocking set of $PG(2,q)$. A blocking set is *trivial* when it contains a line.

A great deal of research in finite geometry has taken place focusing on small blocking sets. The main problem is to find the minimum size for non-trivial blocking sets in $PG(2,q)$, and to give a geometric construction for those which attain such a minimum. This problem has been completely solved for square q in the early Seventies, see [4,5], for $q=p^i$ with p prime and $i=1,3$ in recent years, see [10–12], but it remains unsolved for general values of q; see the recent survey papers [1–3] and [14,15].

Given a proper subset $\mathcal{L}$ of lines in $PG(2,q)$, it is natural to ask for a point-set of minimum size which blocks $\mathcal{L}$. The case where $\mathcal{L}$ consists of all

Mathematics Subject Classification (2000): 51E21, 05B25

* Research supported by the Italian Ministry MURST, Strutture geometriche, combinatoria e loro applicazioni and by the Hungarian-Italian Intergovernemental project "Algebraic and Geometric Structures".

external lines to a given irreducible conic $\mathcal{C}$ is the subject of this paper. We completely solve the main problem for every odd q.

Theorem 1.1. *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 chord 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.*

It should be noted that Theorem 1.1 does not hold true for any even square q, as a nonlinear example arises from every Baer subplane $PG(2,\sqrt{q})$ intersecting $\mathcal{C}$ in a conic $\mathcal{C}_0$ of $PG(2,\sqrt{q})$. The set consisting of all points of $PG(2,\sqrt{q})$ minus those in $\mathcal{C}_0$ and the nucleus of $\mathcal{C}$ indeed blocks every external line to $\mathcal{C}$.

Essential tools in the proof of Theorem 1.1 are a result on the linear system of polynomials vanishing at every internal point to $\mathcal{C}$ together with a corollary to the classification theorem of all subgroups of $PGL(2,q)$.

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

The degree of any nonzero 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 [6] 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 nonzero 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 nonzero 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, i.e. $q=p^h$ 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 2.1. *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

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

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 2.2. *If $\deg \Gamma = q-1$ in Theorem 2.1, then Γ has equation*

$$f(X,Y) = \sum_{t\in GF(q)} \lambda_t \varphi_t(X,Y) = 0. \tag{2}$$

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 [13], for instance.

Theorem 2.3. *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 2.1 is by contradiction. Let Γ be an algebraic curve containing all points of $\mathcal{I}(\mathcal{C})$ whose degree d satisfying

$$d < q-1. \tag{3}$$

The first step consists in proving the following.

Lemma 2.4. *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. Choose a frame in $AG(2,q)$ with origin O such that $\mathcal{C}$ has equation $Y = X^2$. Internal and external points to $\mathcal{C}$ can be described analytically, see [7]: a point $P(x,y)$ in $A(2,q)$ is internal or external to $\mathcal{C}$ according as $x^2 - y$ is a nonzero 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 the $d \geq \frac{1}{2}(q+1)$, 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 $(X,Y) \mapsto (uX, u^2Y)$ 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 $f'(X,Y) = \sum b_{ij} X^i Y^j$, we have $b_{ij} = (\sum_{u \in GF(q)^*} u^{i+2j}) a_{ij}$. By Lemma 6.3 in [9],

$$b_{ij} = \begin{cases} -a_{ij} & \text{when either } i = j = 0, \text{ or } i + 2j = q - 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

This shows that

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

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

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

provided that $x \in GF(q) \setminus \{0\}$. 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 2.5. *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 $g'(X,Y)=\sum_{u\in GF(q)^*} g'_u(X,Y)$, and $g'(X,Y)=\sum b_{ij}X^iY^j$. Then

$$(5) \qquad b_{ij} = \begin{cases} -a_{ij} & \text{when either } i=1, j=0, \text{ or } i+2j=q, \\ 0 & \text{otherwise.} \end{cases}$$

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). 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 $x\in GF(q)\setminus\{0\}$. 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 2.4 and 2.5, the intersection number $I(\Gamma,\mathcal{C};O)\geq 2$ 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 $2d\geq 2(q+1)$, or $\mathcal{C}$ is a component of Γ. By (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.

3. Proof of Theorem 2.3

In this section 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 2, 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 (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 $\Psi_{q-1}(X,Y)=\sum_{i=0}^{q-1} a_iX^iY^{q-1-i}$ of degree $q-1$ can be written as

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

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

$$
\begin{aligned}
a_0 &= \binom{q-1}{0} \sum_{t\in GF(q)} \lambda_t,\\
a_1 &= \binom{q-1}{1} \sum_{t\in GF(q)} \lambda_t(-t),\\
&\vdots\\
a_{q-1} &= \binom{q-1}{q-1} \sum_{t\in GF(q)} \lambda_t(-t)^{q-1},
\end{aligned} \tag{6}
$$

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

$$c = (q-1)^q$$

this determinant is equal to a determinant of Vandermond type with generators w^i, where $i=1,\dots,q-1$ and w is a primitive element of $GF(q)$, which is different from 0. Therefore, (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

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

Note that the terms of degree $q-1$ in $\varphi_t(X,Y)$ are those in $(Y-tX)^{q-1}$. If the polynomial $a(X,Y) - \sum_{t\in GF(q)} \lambda_t \varphi_t(X,Y)$ 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 2.1. 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 $GF(q)$. Assume

$$\sum_{t\in GF(q)} \lambda_t \varphi_t(X,Y) = 0. \tag{7}$$

Let $P_t(\frac{1}{2}t, \frac{1}{4}t^2)$ be the tangency point of the tangent to $\mathcal{C}$ through the point Q_t but different from ℓ_∞. Since $\varphi_u(P_t)=0$ for all $u\neq t$ but $\varphi_t(P_t)=1$, from (7) $\lambda_t=0$ follows. Hence $\lambda_t=0$ for all $t\in GF(q)$, and this shows the linearly independence.

Remark 3.1. 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 3.2. *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

$$\varphi(X,Y) = \sum_{t\in GF(q)} \lambda_t\varphi_t(X,Y). \tag{8}$$

The point $P_t(\frac{t}{2}, \frac{t^2}{4})\in\mathcal{C}$ 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 3.3. *Let $\ell_1,\ldots,\ell_{q-1}$ 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 $\ell_1,\ldots,\ell_{q-1}$. 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. ∎

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

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 $c\neq 0$. An essential tool in the proof of Theorem 2.3 is the classification of all subgroups of $PGL(2,q)$, see [8,16].

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 $d\,|\,(q\pm 1)$, $N=1$;*
(II) *elementary abelian groups of order p^k with $k\leq h$, $N=0$;*
(III) *dihedral groups of order $2d$ with $d\,|\,(q\pm 1)$, $N=d+1$;*
(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 of 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 enter, 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 $L_1\cap L_2=\varnothing$ is *G-invariant* if every $g\in G$ either takes L_1 to L_2 and vice versa, 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 $i\le 2$.

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 $2(q\pm1)$ 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 $P_t(\frac{1}{2}t,\frac{1}{4}t^2)$ 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 $\psi_1,\ldots,\psi_{q-1}$ are the noncentral involutions of a dihedral subgroup of $PGL(2,q)$ of order $2(q-1)$, then the corresponding symmetry axes $\ell_1,\ldots,\ell_{q-1}$ have a common point P. Furthermore, P is an external point to $\mathcal{C}$, and $\ell_1,\ldots,\ell_{q-1}$ 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 $(X,Y)\mapsto(X+\frac{1}{2}u, Y+uX+\frac{1}{4}u^2)$ 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 $P(0,-\frac{1}{4})$. Thus they are all the nontangent lines through the point $P(0,-\frac{1}{4})$ showing the assertion for this case.

Finally, let $A,B\in\ell_\infty\setminus\{Q_\infty\}$ be 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. ∎

5. Proof of Theorem 1.1

Since q is odd, an orthogonal polarity is associated with $\mathcal{C}$. This allows us to state Theorem 1.1 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 for $q \neq 5,7$, equality only holds when $\mathcal{L}$ consists of all lines through an external point P minus the two tangents to $\mathcal{C}$ through P. For $q=5,7$ there exists just one more example, up to projectivities.

An essential tool in the proof is given by the involutions associated with the lines of $\mathcal{L}$, viewed as elements of the linear group $PGL(2,q)$ of the projective line over $GF(q)$, especially Lemma 4.2 in Section 4.

The first statement in the dual of Theorem 1.1 is a corollary to Theorem 2.1. Henceforth we assume $|\mathcal{L}|=q-1$.

Lemma 5.1. *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 $P(\frac{1}{2}t,\frac{1}{4}t^2)$. Note that r_t has equation $Y-tX+\frac{1}{4}t^2=0$.

By Theorem 2.2, there are $\lambda_t \in GF(q)$ such that

$$L(X,Y) = \sum_{t\in GF(q)} \lambda_t (1-(Y-tX+\tfrac{1}{4}t^2)^{q-1}). \tag{9}$$

Lemma 5.2. *$\mathcal{L}$ contains a chord 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 chord of $\mathcal{C}$ and let P denote one of their common points. Write $P=(\frac{1}{2}u,\frac{1}{4}u^2)$ with $u\in GF(q)$. Then $L(\frac{1}{2}u,\frac{1}{4}u^2)=0$. Furthermore, $1-(\frac{1}{4}u^2-\frac{1}{2}ut+\frac{1}{4}t^2)^{q-1}=1-[\frac{1}{2}(u-t)]^{2(q-1)}$ is equal to 1 for $u=t$, and it vanishes otherwise. By (9), $\lambda_u=0$. Conversely, if $\lambda_u=0$, then (9) yields that $L(\frac{1}{2}u,\frac{1}{4}u^2)=0$, and hence some line in $\mathcal{L}$ contains the point $P=(\frac{1}{2}u,\frac{1}{4}u^2)$ of $\mathcal{C}$. ∎

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

Lemma 5.3. *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 (9) in homogeneous coordinates:

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

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 $\boldsymbol{\lambda=0}$. 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 5.4. *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 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 $(y-wx+\frac{1}{4}w^2)^{q-1}$ vanishes for $w=t$ and $w=v$, otherwise it is equal to 1. From (9), $\lambda_t+\lambda_v=0$. By Lemma 5.3, $Q_t\in\Lambda$ yields $\lambda_t=0$. Hence $\lambda_v=0$, and by Lemma 5.3 the assertion follows. ∎

Lemma 5.4 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 5.1, some of these involutions have no fixed points. Hence, from Lemmas 4.2 and 4.4 we obtain Theorem 1.1 in its dual form.

Case $\boldsymbol{\lambda \neq 0}$. This time, we define Λ^+ to be the set of all infinite points Q_t covered by lines in $\mathcal{L}$. By Lemma 5.3, 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 5.5. *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 be 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 $P(\frac{1}{2}u, \frac{1}{4}u^2)$ of the affine tangent line to $\mathcal{C}$ through Q_u. Therefore $L(\frac{1}{2}u, \frac{1}{4}u^2) = 0$. By (9), $0 = \sum_{t \in GF(q)} \lambda_t (1 - (\frac{1}{4}u^2 - \frac{1}{2}ut + \frac{1}{4}t^2)^{q-1}) = \sum_{t \in GF(q)} \lambda_t (1 - (u-t)^{q-1})$. 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 5.4, $\lambda_u + \lambda_v = 0$ 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 5.4 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 5.1, 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 3.3.

If Λ consists of all points in ℓ_∞, then no λ_t vanishes. By Lemma 5.2, 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 $\boldsymbol{q = 5}$. A nonlinear example of a line-set $\mathcal{L}$ covering $\mathcal{I}(\mathcal{C})$ consists of the four external lines to $\mathcal{C}$:

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

Set

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

As before, let

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

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 $\ell_1, \dots, \ell_4$ are

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

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

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

and

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

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 $\ell_1, \dots, \ell_6$ are

$$\psi_1 : t' = \frac{6}{t}; \quad \psi_2 : t' = \frac{2t+1}{t+5}; \quad \psi_3 : t' = \frac{2t+2}{t+5};$$
$$\psi_4 : t' = \frac{2t+6}{t+5}; \quad \psi_5 : t' = \frac{5t+6}{t+2}; \quad \psi_6 : t' = \frac{t+4}{t+6}.$$

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.

References

[1] A. Blokhuis, A. Brouwer and H. Wilbrink: Blocking sets in PG$(2,p)$ for small p, and partial spreads in PG$(3,7)$; *Adv. Geom.*, Special issue dedicated to Adriano Barlotti, (2003), suppl., 245–253.

[2] A. Blokhuis: On the size of a blocking set in PG$(2,p)$, *Combinatorica* **14(1)** (1994), 111–114.

[3] A. Blokhuis: Blocking-sets in Desarguesian planes, in: *Combinatorics, Paul Erdős is Eighty, Volume 2 (eds. D. Miklós, V. T. Sós, T. Szőnyi)*, Bolyai Society Mathematical Studies, **2**, Bolyai Society, Budapest (1996), 133–155.

[4] A. Bruen: Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.

[5] A. Bruen: Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.

[6] V. D. Goppa: *Geometry and Codes*, Kluwer (1988).

[7] J. W. P. Hirschfeld: *Projective Geometries over Finite Fields*, Second Edition, Oxford Mathematical Monographs, New York (1985).

[8] B. Huppert: *Endliche Gruppen I*, Springer Verlag (1967).

[9] R. Lidl and H. Niederreiter: *Finite Fields*, Cambridge University Press (1984).

[10] O. Polverino: Small minimal blocking sets and complete k-arcs in PG$(2,p^3)$, *Discrete Math.* **208/209** (1999), 469–476.

[11] O. Polverino: Small blocking sets in PG$(2,p^3)$, *Des. Codes Cryptogr.* **20** (2000), 319–324.

[12] O. Polverino and L. Storme: Minimal blocking sets in PG$(2,q^3)$, *Europ. J. Combin.* **23** (2002), 83–92.

[13] A. Seidenberg: *Elements of the Theory of Algebraic Curves*, Addison Wesley, Reading (Massachusetts) (1969).

[14] T. Szőnyi: Some applications of algebraic curves in finite geometry and combinatorics, *Surveys in Combinatorics*, 1997, (Edited by R. A. Bailey), London Mathematical Society, Lecture Note Series **241** (1997), 197–236.

[15] T. Szőnyi: Blocking sets in Desarguesian affine and projective planes, *Finite Fields Appl.* **3(3)** (1997), 187–202.

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

Angela Aguglia

Dipartimento di Matematica
Politecnico di Bari
Via Orabona 4
7 0125 Bari
Italy
aguglia@dm.uniba.it

Gábor Korchmáros

Dipartimento di Matematica
Università della Basilicata
Contrada Macchia Romana
85100 Potenza
Italy
korchmaros@unibas.it