COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 12 (2) (1992) 143–147

CHARACTERIZATION OF COMPLETE EXTERIOR SETS OF CONICS

A. BLOKHUIS, Á SERESS*, and H. A. WILBRINK

Received July 11, 1989

Let $\mathcal{E}$ be a set of $\frac{q+1}{2}$ exterior points of a nondegenerate conic in $PG(2,q)$ with the property that the line joining any 2 points in $\mathcal{E}$ misses the conic. If $q \equiv 1 \pmod 4$ then $\mathcal{E}$ consists of the exterior points on a passant, if $q \equiv 3 \pmod 4$ then other examples exist (at least for $q = 7, 11, \ldots, 31$).

1. Introduction

The starting point of the investigations in this paper is the following problem: *Let $\mathcal{S}$ be a (nonempty) set of points in $PG(2,q)$ without tangents, i.e. no line intersects $\mathcal{S}$ in precisely one point. What is the minimal cardinality of $\mathcal{S}$?*. This problem is discussed in [1]. For $q = 7$ the minimal cardinality can be seen to be 12 and an example of such a configuration is obtained as follows: Take the set of 8 points of a conic, together with 4 exterior points such that each pair determines a passing line and furthermore no three of them are collinear. An analogous situation occurs for $q = 11$. Here we get a configuration $\mathcal{S}$ in $PG(2,11)$ of $18 = 12 + 6$ points consisting of the 12 points of a conic together with a set of 6 exterior points. This led us to the following problem:

Let $\mathcal{E}$ be a set of $(q+1)/2$ exterior points (with respect to a fixed nondegenerate conic in $PG(2,q)$) such that each pair determines a passing line (we call such a set a *complete exterior set*). Classify such sets.

It turns out that the situation is essentially different for $q \equiv 1$ and $3 \pmod 4$. In fact for $q \equiv 1 \pmod 4$ the only examples of complete exterior sets are the obvious ones, i.e., the set of exterior points on some passant of the conic.

2. The Theorem

Theorem. *Let $\mathcal{E}$ be a set of $\frac{q+1}{2}$ exterior points of a nondegenerate conic $\mathcal{C}$ in the desarguesian plane $PG(2,q), q \equiv 1 \pmod 4$ with the property that the line joining*

AMS subject classification code (1991): 05 B 25, 51 E 15

* Support from the Dutch organization for scientific Research (NWO) is gratefully acknowledged

any 2 points in $\mathcal{E}$ misses the conic. Then $\mathcal{E}$ consists of the exterior points on a passant.

Proof. Let the conic $\mathcal{C}$ have equation $xz = y^2$. The points on $\mathcal{C}$ can be identified with the elements of $PG(1,q)$ as follows: $(1,t,t^2)$ will be labeled (t), $(0,0,1)$ with (∞). An exterior point P of the conic is uniquely determined by the two points $P^\perp \cap \mathcal{C}$ i.e. the two points of $\mathcal{C}$ such that P is on the corresponding tangents. So exterior points of $\mathcal{C}$ correspond to pairs of points in $PG(1,q)$, which we identify with $GF(q) \cup \{\infty\}$. Let P correspond to the pair (a,b) and Q to the pair (c,d). Then we have the following characterization of passants:

The line joining P and Q is a passant if and only if the cross-ratio $\frac{a-c}{a-d}/\frac{b-c}{b-d}$ is a non-square in $GF(q)$.

To see this, first note that the exterior point labeled $(a,b), a,b \in GF(q)$ corresponds to the point with coordinates $\left(1, \frac{a+b}{2}, ab\right)$ in the plane, and (a,∞) corresponds to $(0,1,2a)$. For two points to determine a passant amounts to a certain quadratic not having a solution, i.e., the discriminant should be a non-square. This discriminant turns out to be $(a-c)(a-d)(b-c)(b-d)$ for the points (a,b) and (c,d) and $(a-c)(b-c)$ for the points (a,b) and (c,∞) from which the assertion follows. (In the result we wrote this expression as a ratio in order for it to make sense also if one of the letters equals ∞.)

It follows that a complete exterior set corresponds to a partition of $GF(q) \cup \{\infty\}$ in pairs, such that for each two pairs the cross-ratio is a non-square. Now it is well-known that the automorphism group of the conic is 3-transitive on $\mathcal{C}$ (in fact it is $PGL(2,q)$), so for the first point of our exterior set we may choose the pair $(0,\infty)$. It follows that all other pairs consist of one square and one non-square, so we may reformulate our problem as follows: characterize all bijections $\varphi : GF(q)^* \to GF(q)^*$ of order 2, sending squares to non-squares, and with the property that for any two squares s and t:

$$(s-t)(s-\varphi(t))(\varphi(s)-t)(\varphi(s)-\varphi(t)) = \square \tag{1}$$

Example: let φ be given by $\varphi(x) = n/x$, where n is a fixed non-square in $GF(q)$. Then for squares s and t condition (1) reads as follows:

$$(s-t)\left(s-\frac{n}{t}\right)\left(\frac{n}{s}-t\right)\left(\frac{n}{s}-\frac{n}{t}\right) = \square,$$

which is easily checked. These bijections correspond to the complete exterior sets that are of the form: all exterior points on a passant line. Our aim will be to show that there are no other examples, however, for this we essentially need that $q \equiv 1 (\mathrm{mod}\ 4)$. Note that in that case (since -1 is a square) in the examples we always have that $(s-t)\left(\frac{n}{s}-\frac{n}{t}\right)$ is a non-square (and consequently $\left(s-\frac{n}{t}\right)\left(\frac{n}{s}-t\right)$ is a square). The proof now proceeds as follows: First, assuming that this extra property holds, (i.e. for all s and t square we assume that $(s-t)(\varphi(s)-\varphi(t))$ is a non-square) we prove that φ is of the required form, and finally we show that φ indeed satisfies this extra property (the reason that we postpone this is that it is rather technical, and would interrupt the main line of the proof). We need the following result which is a direct consequence of a theorem of Carlitz and McConnel [3], [4] (also proved by Bruen and Levinger [3]):

Result. *Let $f : GF(q) \to GF(q)$ be a function with the property that for all $x, y \in GF(q)$ with $x \neq y$, $\frac{f(x)-f(y)}{x-y}$ is a non-square. Then f is of the form $f(x) = a + bx^{p^j}$. Here p is the characteristic of $GF(q)$, i.e. $q = p^n$ for some n, and b is a nonsquare in $GF(q)$.*

Now consider the function f on $GF(q)$ defined by $f(0) = 0$ and for $x \neq 0$: $f(x) = \frac{1}{\varphi(x)}$. The extra property and the fact that φ has order 2 implies that for all $x, y \in GF(q)$ indeed $\frac{f(x)-f(y)}{x-y}$ is a non-square, so we may apply the result. Since $f(0) = 0$ we immediately get $a = 0$ and for $x \in GF(q)^*$ we get $\varphi(x) = 1/(bx^{p^j})$. Using that φ is of order two it follows from this that $b^{p^j-1}x^{p^{2j}} = x$. From this we immediately get that $b^{p^j-1} = 1$, by just substituting $x = 1$, and then $x^{p^{2j}} = x$, i.e., $j = 0$ or $p^{2j} = q$ (in the conclusion of the theorem of Carlitz–McConnel we may assume $j < n$). Since $b^{p^j-1} = 1$, while on the other hand b is a non-square (i.e. $b^{\frac{q-1}{2}} = -1$,) it follows that the case $p^{2j} = q$ does not occur since $p^j - 1$ divides $\frac{1}{2}(p^{2j} - 1)$. Hence $j = 0$ and $\varphi(x) = n/x$ for some non-square n ($n = 1/b$).

We finish the proof by showing that the extra property holds, i.e. if s and t are squares, then $(\varphi(s) - \varphi(t))(s - t)$ is a non-square.

We define a graph Γ on the points of $GF(q)$ as follows: x is joined to y if and only if $x - y$ is a square (note that this defines an undirected graph since $q \equiv 1 \pmod 4$, i.e. -1 is a square). It is well known that this graph (usually called the Paley-graph) is strongly regular with parameters $k = (q-1)/2$, $\lambda = (q-5)/4$, $\mu = (q-1)/4$. (Here k is the valency of the graph, λ is the number of common neighbours of two adjacent points, and μ is the number of common neighbours of two non-adjacent points.) Now the existence of a complete exterior set corresponds to a partition of the points $\neq 0$ of Γ into pairs $(s_i, n_i), i = 1, \ldots, (q-1)/2$, with s_i square and n_i non-square, such that the number of edges between $\{s_i, n_i\}$ and $\{s_j, n_j\}$ is always odd (for $i \neq j$). Suppose now that (a, b) and (c, d) with a, c square belong to our complete exterior set and are such that $(a - c)(b - d)$ is a square. Without loss of generality we may assume that $a - c = \square$ and $b - d = \square$ (otherwise just replace each pair (s_i, n_i) in the set by the pair $(n/n_i, n/s_i)$ for some arbitrary but fixed nonsquare n). Now consider in the graph Γ the subgraph on the set $\{0, a, b, c, d\}$. There are edges going from 0 to a and c, and since $(a - d)(b - c) = \square$ precisely one of the pairs $\{a, d\}, \{b, c\}$ is joined by an edge, say $\{b, c\}$. About the adjacency of a and b, and similarly that of c and d we have no information, so let $[ab] := 1$ if a and b are adjacent, and 0 otherwise, and define $[cd]$ analogously.

We now proceed to obtain a contradiction as follows: Let x_i denote the number of points in $\Gamma \setminus \{0, a, b, c, d\}$ that are joined to precisely i points in the set $\{0, a, b, c, d\}$. The usual counting arguments (using the fact that Γ is strongly regular) yield:

$$\sum_{i=0}^{5} x_i = q - 5, \tag{2}$$

$$\sum_{i=0}^{5} i x_i = 5 \cdot \frac{q-1}{2} - 6 - 2[ab] - 2[cd], \tag{3}$$

$$(4) \qquad \sum_{i=0}^{5} \binom{i}{2} x_i = 10 \cdot \frac{q-1}{4} - 3 - [ab] - [cd] - 2 - 2[ab] - 2[cd].$$

Finally for each pair $(s_i,n_i) \neq (a,b),(c,d)$ the number of edges going inside $\{0,a,b,c,d\}$ is odd, i.e. if one of them contributes to some x_i with i even, the other contributes to an x_i with i odd. Hence

$$(5) \qquad (x_0 + x_2 + x_4 =)\ x_1 + x_3 + x_5 = \frac{q-5}{2}.$$

Now we compute $(4) - \frac{1}{2} \cdot ((3) - (5))$ which yields $2x_3 + 4x_4 + 8x_5 = \frac{3}{2}(q-1) - 3 - 2([ab] + [cd])$, but the right-hand side of this is odd, while the left-hand side is even, contradiction. ∎

3. Final Remarks

For $q \equiv 3 \pmod 4$ it turns out that there are some examples of complete exterior sets that do not consist of all exterior points of a passant, at least for small q. Two of those (the 4-arc in $PG(2,7)$ and the 6-arc in $PG(2,11)$) were already found by G. Korchmáros [5] because of a relation of these structures with chains of circles on an elliptic quadratic and translation planes, motivated by work of Bruen [2]. By computer search we found all such sets for $q = 7, 11, 19, 23, 27, 31$. It turns out that there are not that many. Andries Brouwer found that up to isomorphism there are the following possibilities : For $q = 7$ one configuration, consisting of 4 points, no 3 collinear. For $q = 11$ two configuration, one a 6-arc, the other a Pasch-configuration. For $q = 19$ a Pasch-configuration, with on one of the 2-secants 4 additional points. In $PG(2,23)$ two configurations, one consists of two Pasch-configurations joined by three transversals, i.e. each 2-secant of one of them is also a 2-secant of the other. The other configuration consists of 6 lines having four points, such that in each of the 12 points 2 of the 4-lines meet. For $q = 27$ one configuration, consisting of 3 Pasch-configuration on two points, with the further property that the have one further two-secant in common. Finally a configuration in $PG(2,31)$ consisting of 6 points forming an arc, and 10 points forming a Petersen graph, in the sense that every 2-secant of the 6-arc is also a 2-secant of the 10-set and the 15 pairs thus obtained yield the structure of a Petersen graph. Andries Brouwer showed, again by computer search that no other examples exist for $q = 43, \ldots, 131$, so we conjecture that for $q > 31$ there are no other complete exterior sets then the linear ones. How to prove this we have no idea.

References

[1] A. BLOKHUIS, Á. SERESS, and H.A. WILBRINK: On sets of points without tangents. *Mitt. Math. Sem. Giessen* **201** (1991), 39–44.

[2] A. A. BRUEN: Inversive Geometry and some New Planes, *Geom. Dedicata* **7** (1978), 81–98.

[3] A. A. BRUEN, and B. LEVINGER: A theorem on permutations of a finite field, *Canadian Journal of Mathematics* **25** (1973), 1060–1065.

[4] L. CARLITZ: A theorem on permutations in a finite field, *Proc. American Mathematical Society* **11** (1960), 456–459.

[5] G. KORCHMÁROS: Example of a chain of circles on an Elliptic Quadric of $PG(3,q)$, $q = 7, 11$ *Journal of Comb. Theory*, A **31** (1981), 98–100.

[6] R. MCCONNEL: Pseudo-ordered polynomials over a finite field, *Acta Arithmetica* **8** (1963), 127–151.

A. Blokhuis

Department of Mathematics
and Computing Science,
Eindhoven University of Technology,
Den Dolech 2,
The Netherlands
aartb@win.tue.nl

Á. Seress

Mathematical Institute
of the Hungarian Academy of Sciences,
Budapest, Hungary, H–1053

and

The Ohio State University,
Columbus, OH 43210
U. S. A.
akos@function.mps.ohio-state.edu

H. A. Wilbrink

Department of Mathematics
and Computing Science,
Eindhoven University of Technology,
Den Dolech 2,
The Netherlands
wsdwhb@urc.tue.nl