LINE PARTITIONS OF INTERNAL POINTS TO A CONIC IN $PG(2,q)$

MASSIMO GIULIETTI

Abstract. All sets of lines providing a partition of the set of internal points to a conic C in $PG(2,q)$, q odd, are determined. There exist only three such linesets up to projectivities, namely the set of all nontangent lines to C through an external point to C, the set of all nontangent lines to C through a point in C, and, for square q, the set of all nontangent lines to C belonging to a Baer subplane $PG(2,\sqrt{q})$ with $\sqrt{q}+1$ common points with C. This classification theorem is the analogous of a classical result by Segre and Korchmáros [9] characterizing the pencil of lines through an internal point to C as the unique set of lines, up to projectivities, which provides a partition of the set of all noninternal points to C. However, the proof is not analogous, since it does not rely on the famous Lemma of Tangents of Segre which was the main ingredient in [9]. The main tools in the present paper are certain partitions in conics of the set of all internal points to C, together with some recent combinatorial characterizations of blocking sets of non-secant lines, see [2], and of blocking sets of external lines, see [1].

1. Introduction

In 1977 Segre and Korchmáros gave the following combinatorial characterization of external lines to an irreducible conic in $PG(2,q)$, see [9], [6] Theorem 13.40, and [8].

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

For even q, this was proven by Bruen and Thas [5], independently.

It is natural to ask for a similar characterization of a minimal pointset $\mathcal{L}$ meeting every *external line* to an irreducible conic C in exactly one point. In this case, we have two linear examples: a chord minus the common points with C, and a tangent minus the tangency point (and, for q even, minus the nucleus of C, as well).

For q even, it is shown in [7] that there is exactly one more possibility for $\mathcal{L}$, namely, for any even square q, the set consisting of the points of a Baer subplane π sharing $\sqrt{q}+1$ with C, minus $\pi \cap$ C and the nucleus of C.

The aim of the present paper is to prove an analogous result for q odd.

Henceforth, q is always assumed to be odd, that is, $q = p^h$ with $p > 2$ prime. Then the orthogonal polarity associated to C turns $\mathcal{L}$ into a *line partition* of the set of all internal points to C. In terms of a line partition, Theorem 1.1 states that if $\mathcal{L}$ is a line partition of the set of all noninternal points to C, then $\mathcal{L}$ is a pencil of lines through an internal point to C.

Our main result is the following theorem.

Theorem 1.2. *Let $\mathcal{L}$ be a line partition of the set of internal points to a conic* C *in $PG(2,q)$, q odd. Then either*

- *$\#\mathcal{L} = q-1$, and $\mathcal{L}$ consists of the $q-1$ lines through an external point of* C *which are not tangent to* C*, or*
- *$\#\mathcal{L} = q$, and $\mathcal{L}$ consists of the q lines through a point of* C *distinct from the tangent to* C*, or*
- *$\#\mathcal{L} = q$ for a square q, and $\mathcal{L}$ consists of all non tangent lines belonging to a Baer subplane $PG(2,\sqrt{q})$ with $\sqrt{q}+1$ common points with* C.

2. Internal points to a conic

In this section a certain partition in conics of the internal points to a conic C in $PG(2,q)$, q odd, is investigated.

Assume without loss of generality that C has affine equation $Y = X^2$, and denote by Y_∞ the infinite point of C. Consider the pencil of conics $\mathcal{F}$ consisting of the conics $\mathrm{C}_s : Y = X^2 - s$, with s ranging over $\mathbb{F}_q$.

First, an elementary property of $\mathcal{F}$ which will be useful in the sequel is pointed out.

Lemma 2.1. *Any line of $PG(2,q)$ not passing through Y_∞ is tangent to exactly one conic of $\mathcal{F}$.*

Proof. It is enough to note that the line of equation $Y = \alpha X + \beta$ is tangent to C_s if and only if $s = -\frac{\alpha^2+4\beta}{4}$. ■

Recall that in the finite field $\mathbb{F}_q$ half the non-zero elements are quadratic residues or squares, and half are quadratic non-residues or non-squares. The quadratic character of $\mathbb{F}_q$ is the function χ given by

$$\chi(x) = \begin{cases} 0 & \text{if } x = 0\,, \\ 1 & \text{if } x \text{ is a quadratic residue,} \\ -1 & \text{if } x \text{ is a quadratic non-residue.} \end{cases}$$

Lemma 2.2. *Let* C_s *and* $\mathrm{C}_{s'}$ *be two distinct conics in* $\mathcal{F}$. *Then the affine points of* $\mathrm{C}_{s'}$ *are all either external or internal to* C_s, *according to whether* $\chi(s'-s)=1$ *or* $\chi(s'-s)=-1$.

Proof. Let $P=(a,a^2-s')$ be an affine point of $\mathrm{C}_{s'}$. The polar line l_P of P with respect to C_s has equation $Y=2aX-a^2+s'-2s$. Then it is straightforward to check that l_P does not meet C_s if and only if $s'-s$ is a non-square in $\mathbb{F}_q$. ∎

As a matter of terminology, we will say that a conic C_s is *internal* (*external*) to $\mathrm{C}_{s'}$ if all the affine points of C_s are internal (external) to $\mathrm{C}_{s'}$. Let $\mathcal{I}=\{\mathrm{C}_s \mid \chi(s)=-1\}$. Clearly, the set of internal points to C consists of the affine points of the conics in $\mathcal{I}$.

Throughout the rest of this section we assume that $q\equiv 3 \pmod 4$. Note that this is equivalent to $\chi(-1)=-1$, see [6]. Then Lemma 2.2 yields that C_s is internal to $\mathrm{C}_{s'}$ if and only if $\mathrm{C}_{s'}$ is external to C_s.

Lemma 2.3. *Let* C_s *be a conic in* $\mathcal{I}$. *If* $q\equiv 3 \pmod 4$, *then there are exactly* $\frac{q-3}{4}$ *conics in* $\mathcal{I}$ *that are internal to* C_s.

Proof. The hypothesis $q\equiv 3 \pmod 4$ yields that for any $s\in\mathbb{F}_q$, $s\neq 0$, there are exactly $\frac{q-3}{4}$ ordered pairs $(u,v)\in\mathbb{F}_q\times\mathbb{F}_q$ with $s=u-v$ and $\chi(u)=\chi(v)=1$ (see e.g. [10, Lemma 1.7]). Via the correspondence $s'=-v$, the number of such pairs equals the number of $s'\in\mathbb{F}_q$ satisfying $\chi(s')=\chi(s'-s)=-1$. Then the assertion follows from Lemma 2.2. ∎

Denote $\mathcal{I}_s$ the set of conics of $\mathcal{I}$ which are internal to C_s. The following lemma will be crucial in the proof of Theorem 1.2.

Lemma 2.4. *Let* $q\equiv 3 \pmod 4$. *Then the any integer function* φ *on* $\mathcal{I}$ *such that*

$$\sum_{\mathrm{C}_{s'}\in\mathcal{I}_s}\varphi(\mathrm{C}_{s'})=\sum_{\mathrm{C}_{s'}\in\mathcal{I}\setminus\mathcal{I}_s,\mathrm{C}_{s'}\neq\mathrm{C}_s}\varphi(\mathrm{C}_{s'}),\qquad \textit{for any } \mathrm{C}_s\in\mathcal{I}\tag{1}$$

is constant.

Proof. Let $\{s_1,s_2,\ldots,s_{\frac{q-1}{2}}\}$ be the set of non-squares in $\mathbb{F}_q$, and let $A=(a_{ij})$ be the $\frac{q-1}{2}\times\frac{q-1}{2}$ matrix given by

$$a_{ij}=\chi(s_i-s_j)\,.$$

Then by Lemma 2.2, condition (1) is equivalent to

$$\sum_{\chi(s_i-s_j)=-1}\varphi(\mathrm{C}_{s_i})=\sum_{\chi(s_i-s_j)=1}\varphi(\mathrm{C}_{s_i}),\qquad \text{for any } j=1,\ldots,\frac{q-1}{2}\,,$$

that is, the vector $(\varphi(\mathrm{C}_{s_1}),\ldots,\varphi(\mathrm{C}_{s_i}),\ldots,\varphi(\mathrm{C}_{s_{\frac{q-1}{2}}}))$ belongs to the null space of A. Clearly if φ is constant such a condition is fulfilled by Lemma 2.3.

Then to prove the assertion, it is enough to show that the real rank of A is at least $\frac{q-1}{2}-1$. As usual, denote $A_{1,1}$ the matrix obtained from A by dismissing the first row and the first column column. Note that as the entries of $A_{1,1}$ are integers, $Det(A_{1,1}) \pmod 2$ coincides with $Det(\tilde{A}_{1,1})$, where $\tilde{A}_{1,1}$ is the matrix over the finite field with 2 elements obtained from $A_{1,1}$ by substituting each entry m_{ij} with m_{ij} (mod 2). By definition of A, the entries of $\tilde{A}_{1,1}$ are equal to 1, except those in the diagonal which are equal to zero. As $\frac{q-1}{2}-1$ is even, it is straightforward to check that $\tilde{A}^2_{1,1}$ is the identity matrix, whence $Det(\tilde{A}_{1,1}) = Det(A_{1,1}) \pmod 2$ is different from 0. ■

3. Proof of Theorem 1.2

Throughout, C is an irreducible conic in $PG(2,q)$, q odd, and $\mathcal{L}$ is a line partition of the set of internal points to C. First, the possible sizes of $\mathcal{L}$ are determined.

Lemma 3.1. *The size of $\mathcal{L}$ is either $q-1$ or q. In the latter case, $\mathcal{L}$ consists of q secant lines to* C.

Proof. The number of internal points to a conic is $q(q-1)/2$, see [6]. Also, a secant line of C contains $(q-1)/2$ internal points of C, whereas the number of internal points on an external line is $(q+1)/2$. No internal point belongs to a tangent to C. Let $\mathcal{L}$ consist of h secants together with k external lines to C. As $\mathcal{L}$ is a line partition of the internal points to C,

$$\frac{q(q-1)}{2} = h\frac{q-1}{2} + k\frac{q+1}{2},$$

that is

$$q = h + k + \frac{2k}{q-1}.$$

As $\frac{2k}{q-1}$ is an integer, either $k=0$ and $h=q$, or $k=(q-1)/2=h$. ■

The classification problem for $\#\mathcal{L} = q-1$ is solved via the characterization of blocking sets of minimal size of the external lines to a conic, as given in [1]. The dual of Theorem 1.1 in [1] reads as follows.

Proposition 3.2. *Let $\mathcal{R}$ be a lineset of size $q-1$ such that any internal point to* C *belongs to some line of $\mathcal{R}$. If either $q=3$ or $q>9$, then*

$\mathcal{R}$ consists of the $q-1$ lines through an external point of C *which are not tangent to* C*. For $q=5,7$ there exists just one more example, up to projectivities, for which some of the lines in $\mathcal{R}$ are external to* C*.*

From now on, assume that $\#\mathcal{L}=q$. Note that Lemma 3.1 yields that every line of $\mathcal{L}$ is a secant line of C. We first deal with the case $q \equiv 3 \pmod 4$.

Lemma 3.3. *Let $\#\mathcal{L}=q$. If $q\equiv 3 \pmod 4$, then the number of lines of $\mathcal{L}$ through any point P of* C *is 1, $\frac{q+1}{2}$ or q.*

Proof. We keep the notation of Section 2. Assume without loss of generality that C has equation $X^2-Y=0$, and that $P=Y_\infty$. Let $\mathcal{L}_P$ be the set of lines of $\mathcal{L}$ passing through P, and set $m=\#\mathcal{L}_P$. Also, for any $l\in\mathcal{L}\setminus\mathcal{L}_P$, denote $\mathrm{C}^{(l)}$ the conic of $\mathcal{F}$ which is tangent to l according to Lemma 2.1.

As any secant l of C not passing through P contains an odd number of internal points to C, the conic $\mathrm{C}^{(l)}$ belongs to $\mathcal{I}$. We claim that for any $\mathrm{C}_s\in\mathcal{I}$ and for any $l\in\mathcal{L}\setminus\mathcal{L}_P$, l not tangent to C_s,

$$\mathrm{C}_s \text{ is external to } \mathrm{C}^{(l)} \text{ if and only if } l \text{ is a secant of } \mathrm{C}_s\,. \tag{2}$$

Clearly, if l is a secant of C_s, then both the points of $\mathrm{C}_s\cap l$ are external to $\mathrm{C}^{(l)}$. Therefore C_s is external to $\mathrm{C}^{(l)}$. To prove the only if part of (2), note that for any $l\in\mathcal{L}\setminus\mathcal{L}_P$ the set of $\frac{q-1}{2}$ points of l which are internal to C consists of one point lying on $\mathrm{C}^{(l)}$ together with $\frac{q-3}{4}$ point pairs, each of which contained in a conic of $\mathcal{I}$. Taking into account Lemma 2.3, this means that l is a secant of all the conics of $\mathcal{I}$ that are external to $\mathrm{C}^{(l)}$.

Now, for any $\mathrm{C}_s\in\mathcal{I}$ let $\varphi(\mathrm{C}_s)$ be the number of lines of $\mathcal{L}$ which are tangent to C_s. Then,

$$\sum_{\mathrm{C}_{s'}\in\mathcal{I}_s}\varphi(\mathrm{C}_{s'}) = \sum_{\mathrm{C}_{s'}\in\mathcal{I}\setminus\mathcal{I}_s,\mathrm{C}_{s'}\neq\mathrm{C}_s}\varphi(\mathrm{C}_{s'}), \qquad \text{for any } \mathrm{C}_s\in\mathcal{I}\,. \tag{3}$$

In fact, (2) yields that $\sum_{\mathrm{C}_{s'}\in\mathcal{I}_s}\varphi(\mathrm{C}_{s'})$ equals the number of lines in $\mathcal{L}\setminus\mathcal{L}_P$ which are secants to C_s, that is $\frac{q-m-\varphi(\mathrm{C}_s)}{2}$. As the total number of lines in $\mathcal{L}$ which are tangent to a conic of $\mathcal{I}$ distinct from C_s is $q-m-\varphi(\mathrm{C}_s)$, Equation (3) follows. Then by Lemma 2.4, $\varphi(\mathrm{C}_s)$ is an integer which is independent of C_s. Denote t such an integer. By Lemma 2.1,

$$\sum_{\mathrm{C}_s\in\mathcal{I}}\varphi(\mathrm{C}_s) = t\frac{q-1}{2} = q-m\,, \tag{4}$$

which implies that either (a) $t = 2$, $m = 1$, (b) $t = 0$, $m = q$, or (c) $t = 1$, $m = \frac{q+1}{2}$. ■

Lemma 3.4. *Let $\#\mathcal{L} = q$. If $q \equiv 3 \pmod 4$, then no point of* C *belongs to exactly $\frac{q+1}{2}$ lines of $\mathcal{L}$.*

Proof. We keep the notation of the proof of Lemma 3.3. Also, for $Q \in \mathrm{C}$ let m_Q be the number of lines of $\mathcal{L}$ passing through Q.

Assume that $m_P = \frac{q+1}{2}$, with $P = Y_\infty$. As $\sum_{Q\in \mathrm{C}} m_Q = 2q$, Lemma 3.3 yields that there exists another point $\bar{P} \in \mathrm{C}$ belonging to exactly $\frac{q+1}{2}$ lines of $\mathcal{L}$, and that $m_Q = 1$ for any point $Q \in \mathrm{C}$, $Q \notin \{P, \bar{P}\}$. As the projective group of C is sharply 3-transitive on the points of C (see e.g. [6]), we may assume that $\bar{P}$ coincides with $(0, 0)$.

Let $\mathcal{A}$ be the subset of $\mathbb{F}_q \setminus \{0\}$ consisting of the $\frac{q-1}{2}$ non-zero elements u for which the line $Y = uX$ belongs to $\mathcal{L}$. Then the lines in $\mathcal{L}_P$ are those of equation $X = v$, with v ranging over $\mathbb{F}_q \setminus \mathcal{A}$. Actually, $\mathbb{F}_q \setminus \mathcal{A}$ coincides with $\{-u \mid u \in \mathcal{A}\} \cup \{0\}$. In fact, $u \in \mathcal{A}$ yields $-u \notin \mathcal{A}$, otherwise the two lines of equation $Y = uX$ and $Y = -uX$ would be both lines of $\mathcal{L}$ tangent to the same conic $\mathrm{C}_{-u^2/4}$. By the proof of Lemma 3.3 this is impossible, as $m_P = \frac{q+1}{2}$ yields that each conic in $\mathcal{I}$ has exactly one tangent in $\mathcal{L} \setminus \mathcal{L}_P$.

Then, for any $u_1, u_2 \in \mathcal{A}$, $u_1 \neq u_2$, the lines $Y = u_1X$ and $X = -u_2$, as well as the lines $Y = u_2X$ and $X = -u_1$, meet in an external point to C, that is

$$\chi(u_1^2 + u_1u_2) = \chi(u_2^2 + u_2u_1) = 1\,.$$

Equivalently, for any $u_1, u_2 \in \mathcal{A}$, $u_1 \neq u_2$,

$$\chi(u_1)\chi(u_1 + u_2) = \chi(u_2)\chi(u_1 + u_2) = 1\,,$$

whence all the elements in $\mathcal{A}$ and all the sums of two distinct elements in $\mathcal{A}$ have the same quadratic character. But this is actually impossible, as $q \equiv 3 \pmod 4$ yields that for any $u_1 \in \mathbb{F}_q \setminus \{0\}$, $\epsilon \in \{-1, 1\}$, the number of $u_2 \in \mathbb{F}_q$ such that $\chi(u_2) = \chi(u_1 + u_2) = \epsilon$ is $\frac{q-3}{4}$ (see e.g. [10, Lemma 1.7]). ■

Proposition 3.5. *Let $\#\mathcal{L} = q$. If $q \equiv 3 \pmod 4$, then $\mathcal{L}$ consists of the q lines through a point of* C *distinct from the tangent to* C.

Proof. By Lemmas 3.3 and 3.4 the number m_P of lines of $\mathcal{L}$ through a given point $P \in \mathrm{C}$ is either 1 or q. As $\#\mathcal{L} = q > \frac{q+1}{2}$ it is impossible that $m_P = 1$ for every $P \in \mathrm{C}$. Then there exists a point P_0 with $m_{P_0} = q$, which proves the assertion. ■

Assume now that $q \equiv 1 \pmod 4$. We first prove that any line partition of size q of the internal points of C actually covers all the points of C as well.

Lemma 3.6. *Let $\#\mathcal{L} = q$. If $q \equiv 1 \pmod 4$, then any point of* C *belongs to some line of $\mathcal{L}$.*

Proof. We keep the notation of Section 2. Assume that a point $P \in \mathrm{C}$ does not belong to any line of $\mathcal{L}$. Without loss of generality, let $P = Y_\infty$. Then the q affine points of any conic $\mathrm{C}_s \in \mathcal{I}$ partition into sets $l \cap \mathrm{C}_s$, with l ranging over $\mathcal{L}$. As q is odd, there exists a line $l_s \in \mathcal{L}$ which is tangent to C_s. Any line of $\mathcal{L}$ has an even number of internal points to C, as $(q-1)/2$ is even. Then some line of $\mathcal{L}$ must be tangent to more than one conic of $\mathcal{F}$, which is a contradiction to Lemma 2.1.■

To complete our investigation for $q \equiv 1 \pmod 4$, the combinatorial characterization of blocking sets of non-secant lines to C, as given in [2], is needed. The dual of Theorem in [2] reads as follows.

Lemma 3.7. *Let $\mathcal{R}$ be a lineset of size q such that any non-external point to* C *belongs to some line of $\mathcal{R}$. Then one of the following occurs.*

(a) *$\mathcal{R}$ consists of q lines through a point of* C *distinct from the tangent to* C*,*
(b) *$\mathcal{R}$ consists of the lines of a subgeometry $PG(2, \sqrt{q})$ which are not tangent to* C*.*
(c) *$\mathcal{R}$ consists of the $q-1$ lines through an external point P to* C *which are not tangent to* C*, together with the polar line of P with respect to* C*.*

Proposition 3.8. *Let $\#\mathcal{L} = q$. If $q \equiv 1 \pmod 4$, then $\mathcal{L}$ consists either of the q lines through a point of* C *distinct from the tangent to* C*, or of the lines of a subgeometry $PG(2, \sqrt{q})$ which are not tangent to* C*.*

Proof. Lemma 3.6 yields that $\mathcal{L}$ satisfies the hypothesis of Lemma 3.7. Actually, (c) of Lemma 3.7 cannot occur as in this case not every line of $\mathcal{R}$ is a secant line to C. Hence the assertion is proved. ■

Theorem 1.2 now follows from Propositions 3.2, 3.5, 3.8.

References

[1] A. Aguglia, G. Korchmáros, *Blocking sets of external lines to a conic in PG(2,q), q odd*, Combinatorica (to appear).
[2] A. Aguglia, G. Korchmáros, *Blocking sets of nonsecant lines to a conic in PG(2,q), q odd*, Journal of Combinatorial Designs (to appear).

[3] A. Aguglia, G. Korchmáros, A. Siciliano, *Minimal covering of all chords of a conic in $PG(2,q)$, q even*, Bulletin of the Belgian Mathematical Society, (to appear).

[4] E. Boros, Z. Fűredi, J. Kahn, *Maximal Intersecting Families and Affine Regular Polygons in $PG(2,q)$*, Journal of Combinatorial Theory, Series A **52**, 1–9 (1989).

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

[6] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford (1998).

[7] M. Giulietti, *Blocking sets of external lines to a conic in $PG(2,q)$, q even*, submitted.

[8] G. Korchmáros *Segre's type theorems*, invited lecture at the International Conference "Trends in Geometry, in Memory of Beniamino Segre", 7-8 June 2004 Rome, to appear in a special issue of Rendiconti di Matematica e delle sue applicazioni.

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

[10] W.D. Wallis, A. Penfold Street, J. Seberry Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, volume 292 of *Lecture Notes in Math.*, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

Author's address:

Massimo GIULIETTI
Dipartimento di Matematica
Università degli studi di Perugia
Via Vanvitelli 1
06123 Perugia (Italy).
E–mail: `giuliet@dipmat.unipg.it`