Arcs with large conical subsets in Desarguesian planes of even order

Kris Coolsaet Heide Sticker

Department of Applied Mathematics, Computer Science and Statistics,
Ghent University,
Krijgslaan 281-S9, B-9000 Gent, Belgium
{Kris.Coolsaet, Heide.Sticker}@UGent.be

Submitted: Nov 20, 2012; Accepted: Jan 18, 2014; Published: Jan 24, 2014 Mathematics Subject Classification: 51E21

Abstract

We give an explicit classification of the arcs in PG(2,q) (q even) with a large conical subset and excess 2, i.e., that consist of q/2+1 points of a conic and two points not on that conic. Apart from the initial setup, the methods used are similar to those for the case of odd q, published earlier (Electronic Journal of Combinatorics, 17, #R112).

1 Introduction

Consider the Desarguesian projective plane PG(2,q) over the finite field of order q. An arc is a set of points of PG(2,q) with the property that no three points of this set are collinear. An arc is called complete if it is not contained in a bigger arc.

When q is odd it is well known that an arc can be of size at most q+1 and in that case always coincides with the set of points of some conic. When q is even, the maximum size of an arc is q+2 and again examples are known. (For instance, one can always add the nucleus to the conic.) For further information on the geometrical and combinatorial properties of arcs we refer to [2, Chapters 9–10].

Removing some points from a conic again yields an arc, but this arc is obviously not complete. However, after removing a sufficient number of points it may be possible to extend the set thus obtained to a nonconical arc by adding a point that does not belong to the original conic. This new arc might not be complete, but can be made complete by adding yet more points.

We shall be interested in arcs for which the conical part is as large as possible and that contain (at least) two points not on that conic. A simple result by B. Segre [4] and

L. Lombado-Radice [3] shows that the size of the conical part can be at most (q + 3)/2 when q is odd, and (q + 2)/2 when q is even.

In [1] we classified all arcs of this type with two points not on the conic, for odd q only. Our method made use of an initial step that needs an element of the field GF(q) that is not a square. We could therefore not immediately extend this technique to the case where q is even.

In this paper we show that this problem can be overcome by starting with a different setup, described in Section 2. The end result for q even turns out to be much simpler than that for q odd. For instance, instead of three different types of arcs for the odd case, there is only one case to consider when q is even (cf. Section 3). This is a consequence of the fact that there is no distinction between internal and external points of a conic in the even case.

2 Notation and preliminary definitions

(Where possible we have chosen notations in such a way that they conform to the notations for similar concepts in [1].)

Let S denote an arc of $\operatorname{PG}(2,q)$. We define a *conical subset* of S to be any subset R of S of the form $R=S\cap C$ where C is a conic. (Most of the time the conic C and the conical subset R will be clear from context. We will therefore usually leave out the reference to C when talking about tangents and secants of C and lines external to C.) The points of S that do not belong to R will be called *supplementary* points. The number $e=|S\setminus R|$ will be called the *excess* of the arc. We shall always assume that the arc S has at least one supplementary point, i.e., that S is not fully contained in a conic.

When q is even, all tangents to C go through a common point N (not on C) which is called the *nucleus* of C. Consider a point S of the plane. If Q does not belong to C and $Q \neq N$, then there is exactly one line through Q which is tangent to C, and there are q/2 lines that intersect C in two points. Each of these may intersect R in at most one point, and hence $|R| \leq q/2 + 1$. A conical subset that attains this bound will be called *large*. Arcs with large conical subsets are the subject of this paper.

Henceforth let K denote the finite field of order q, with q even.

Without loss of generality we may fix C to be the conic with equation $XZ = Y^2$. Mapping $t \in K$ to the point with (homogeneous) coordinates $(1:t:t^2)$ and ∞ to the point with coordinates (0:0:1) defines a one-to-one relation between $K \cup \{\infty\}$ and C. The nucleus N of C has coordinates (0:1:0). The tangent through the point $(1:t:t^2)$ has equation $Z = t^2X$. The tangent through the point (0:0:1) has equation X = 0.

The subgroup of $\operatorname{PGL}(3,q)$ that stabilizes C is isomorphic to $\operatorname{PGL}(2,q)$. The element of $\operatorname{PGL}(2,q)$ associated to the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ maps the point (1:t) of the projective line $\operatorname{PG}(1,q)$ onto the point $(1:\frac{b+dt}{a+ct})$. This yields a corresponding action on C that can be extended to an action on any point (x:y:z) of the whole plane $\operatorname{PG}(2,q)$, which

can be written as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \leftrightarrow \quad (x \ y \ z) \mapsto (x \ y \ z) \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix} \tag{1}$$

where 2 is obviously zero in even characteristic.

Let L denote the quadratic extension field of K and let $N(\cdot)$ and $\text{Tr}(\cdot)$ be the norm and trace function for this extension. Consider $\phi \in L$ such that ϕ has multiplicative order q+1 in L. Then $N(\phi)=\phi^{q+1}=1$ and $\text{Tr}(\phi)=\phi+\phi^q=T$, with $T\in K\setminus\{0\}$. The characteristic equation of ϕ is $X^2+TX+1=0$. In particular $\phi^2+T\phi+1=0$. Note that $1,\phi,\phi^2,\ldots$ runs through all elements of L with norm equal to 1. Since q is even, the only element of K with norm equal to 1 is 1 itself.

For any integer i define

$$f_i \stackrel{\text{def}}{=} \frac{1}{T} \text{Tr}(\phi^i) = \frac{1}{T} (\phi^i + \phi^{iq}) = \frac{1}{T} (\phi^i + \phi^{-i}).$$

We have the following properties:

$$f_0 = 0, \ f_1 = 1, \ f_2 = T, \ f_{i+2} = Tf_{i+1} + f_i,$$
 (2)

$$f_{i+q+1} = f_i, \ f_{-i} = f_i, \ f_{i+1} + f_{i-1} = Tf_i, \ f_{i+j} + f_{i-j} = Tf_i f_j.$$
 (3)

(Note that the index i of f_i can be treated as an element of \mathbf{Z}_{q+1} .)

From (3) we may easily compute

$$f_{i+j} = f_{i-1}f_j + f_i f_{j+1} = f_i f_{j-1} + f_{i+1}f_j,$$
(4)

and hence

$$f_{2i} = (f_{i-1} + f_{i+1})f_i = Tf_i^2$$

$$f_{2i-1} = f_i^2 + f_{i-1}^2 = (f_i + f_{i-1})^2,$$

$$f_{2i+1} = f_i^2 + f_{i+1}^2 = (f_i + f_{i+1})^2.$$
(5)

Consider the following element of PGL(2, q):

$$M_i' \stackrel{\text{def}}{=} \begin{pmatrix} f_{i-1} & f_i \\ f_i & f_{i+1} \end{pmatrix}. \tag{6}$$

It follows from (2–4) that

$$M'_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ M'_{i+j} = M'_i M'_j, \ M'_i = M'^i_1, \ \det M'_i = 1.$$

The equivalent action of PGL(3, q) has the following form:

$$\begin{pmatrix} f_{i-1}^2 & f_{i-1}f_i & f_i^2 \\ 0 & 1 & 0 \\ f_i^2 & f_{i+1}f_i & f_{i+1}^2 \end{pmatrix}.$$

Note that (1:0:1) is mapped to $(f_{2i-1}:f_{2i}:f_{2i+1})$. Moreover, all of these points lie on the line ℓ with equation x+Ty+z=0, which is an external line to the conic C.

We shall number the points of ℓ as Q_0, Q_1, \ldots, Q_q such that Q_i has coordinates $(f_{i-1}: f_i: f_{i+1})$. Note that all these points are different and hence $\ell = \{Q_0, Q_1, \ldots, Q_q\}$. The index i of Q_i will be called the *orbital index* of Q_i . Orbital indices can be treated as elements of \mathbf{Z}_{q+1} .

The tangent through $Q_0(1:0:1)$ is the line with equation X+Z=0 (i.e., X=Z) which intersects C in $P_0(1:1:1)$. Define P_i to be the image of P_0 under M_i' . Then P_i has coordinates

$$(f_{2i-1}: f_{2i}+1: f_{2i+1}) \approx (1:t_i:t_i^2),$$

by (5), with

$$t_i \stackrel{\text{def}}{=} \frac{f_i + f_{i+1}}{f_{i-1} + f_i}.$$

(The '≈'-sign denotes equality up to a scalar factor.)

We have

$$t_{q/2} = 0$$
, $t_{q/2+1} = \infty$, $t_0 = 1$, $t_{-i} = 1/t_i$.

Again, the index i of P_i will be called its orbital index, and again it can be treated as an element of \mathbf{Z}_{q+1} .

Lemma 1. Let $i, j, k \in \mathbb{Z}_{q+1}$. Then

- P_i, P_j, Q_k are collinear if and only if $k \equiv i + j \pmod{q+1}$.
- P_iQ_k is a tangent to C if and only if $k \equiv 2i \pmod{q+1}$.

Proof. Indeed

$$\begin{vmatrix} f_{2i-1} & f_{2i} + 1 & f_{2i+1} \\ f_{2j-1} & f_{2j} + 1 & f_{2j+1} \\ f_{i+j-1} & f_{i+j} & f_{i+j+1} \end{vmatrix} = \begin{vmatrix} f_{2i-1} & f_{2i} + 1 & Tf_{2i} \\ f_{2j-1} & f_{2j} + 1 & Tf_{2j} \\ f_{i+j-1} & f_{i+j} & Tf_{i+j} \end{vmatrix} = T \begin{vmatrix} f_{2i-1} & 1 & f_{2i} \\ f_{2j-1} & 1 & f_{2j} \\ f_{i+j-1} & 0 & f_{i+j} \end{vmatrix}$$
$$= T \begin{vmatrix} f_{2i-1} & f_{2i} \\ f_{i+j-1} & f_{i+j} \end{vmatrix} + T \begin{vmatrix} f_{2j-1} & f_{2j} \\ f_{i+j-1} & f_{i+j} \end{vmatrix}$$

and this can be expanded to

$$f_{3i+j-1} + f_{i-j+1} + f_{3i+j-1} + f_{i-j-1} + f_{3j+i-1} + f_{j-i+1} + f_{3j+i-1} + f_{j-i+1} = 0.$$

This proves that P_i, P_j, Q_k are collinear when $k \equiv i+j \pmod{q+1}$. Because the line P_iP_j intersects the line ℓ in exactly one point, and the orbital index of that point is uniquely determined (mod q+1), P_i, P_j, Q_k cannot be collinear for other values of k.

The tangent through P_i has equation $Z = t_i^2 X$ which is clearly satisfied by the point Q_{2i} . Again, the intersection of this tangent with ℓ is a single point, and hence no other point Q_k can satisfy this property.

As in [1], apart from the 'rotations' M'_i defined in (6) we also introduce the 'symmetries' M_i , as follows:

$$M_i \stackrel{\text{def}}{=} \begin{pmatrix} f_i & f_{i+1} \\ f_{i-1} & f_i \end{pmatrix},$$

or represented as elements of PGL(3, q):

$$\begin{pmatrix} f_i^2 & f_{i+1}f_i & f_{i+1}^2 \\ 0 & 1 & 0 \\ f_{i-1}^2 & f_{i-1}f_i & f_i^2 \end{pmatrix}.$$

Note that M_0 interchanges X- and Z-coordinates, that $M_i = M_0 M_i'$ and $M_i' M_0 = M_{-i}$.

Lemma 2. Let H denote the subgroup of PGL(3,q) that leaves both the conic C and its external line ℓ invariant (and hence is a subgroup of PGL(2,q)). Then H consists of the elements $M_i, M'_i, i \in \mathbf{Z}_{q+1}$ and is a dihedral group of order 2(q+1).

The action of H on C and ℓ is given by

Proof. We leave it to the reader to prove that the action of H on the points of C and ℓ is indeed as given in (7).

Consider the action of a general element of PGL(2, q), as presented in (1), on the line ℓ (represented by a column vector):

$$\begin{pmatrix} a^2 & ab & b^2 \\ 0 & ad + bc & 0 \\ c^2 & cd & d^2 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ T \\ 1 \end{pmatrix} = \begin{pmatrix} d^2 & bd & b^2 \\ 0 & ad + bc & 0 \\ c^2 & ac & a^2 \end{pmatrix} \begin{pmatrix} 1 \\ T \\ 1 \end{pmatrix} = \begin{pmatrix} b^2 + Tbd + d^2 \\ T(ad + bc) \\ a^2 + Tac + c^2 \end{pmatrix}$$
(8)

It follows that ℓ is stabilized by this action if and only if

$$a^{2} + Tac + c^{2} = b^{2} + Tbd + d^{2} = ad + bc.$$
(9)

Note that

$$f_i^2 + Tf_{i+1}f_i + f_{i+1}^2 = f_i^2 + Tf_{i-1}f_i + f_{i-1}^2 = f_i^2 + f_{i-1}f_{i+1} = 1,$$

by (2–5). Hence M_i and M_i' satisfy this condition. It is easily seen that the set of all elements M_i, M_i' with $i \in \mathbf{Z}_{q+1}$ forms a group isomorphic to the dihedral group of order 2(q+1). It is therefore sufficient to show that no other elements leave both C and ℓ invariant, or equivalently, that the stabilizer of H of the point $Q_0 \in \ell$ has size at most 2.

The fact that $Q_0(1:0:1)$ is stabilized is expressed as follows:

$$a^{2} + c^{2} = b^{2} + d^{2}, \quad ab + cd = 0.$$
 (10)

This yields a + b + c + d = 0 and ab = cd, and therefore

$$0 = a(a + b + c + d) = a^2 + ab + ac + ad = a^2 + cd + ac + ad = (a + c)(a + d),$$

$$0 = b(a + b + c + d) = ab + b^2 + bc + bd = cd + b^2 + bc + bd = (b + c)(b + d),$$

$$0 = c(a + b + c + d) = ac + bc + c^2 + cd = ac + bc + c^2 + ab = (a + c)(b + c),$$

$$0 = d(a + b + c + d) = ad + bd + cd + d^2 = ad + bd + ab + d^2 = (a + d)(b + d),$$

and hence a = c or a = d, b = c or b = d, a = c or b = c and a = d or b = d. And therefore a = c and b = d, or a = d and b = c.

Together with (9), the first case leads to

$$a^{2} + Ta^{2} + a^{2} = b^{2} + Tb^{2} + b^{2} = ab + ba,$$

and then $Ta^2 = Tb^2 = 0$, implying a = b = c = d = 0, which is not allowed. The second case implies

$$a^{2} + Tab + b^{2} = b^{2} + Tab + a^{2} = a^{2} + b^{2},$$

and then ab = 0. When a = 0 this yields transformation M_0 , when b = 0 this yields M'_0 .

3 Classification up to projective equivalence

After these preliminaries we can continue with the classification up to projective equivalence of arcs with large conical subsets much in the same way as when q is odd. Because of the similarity with [1] we shall try to be brief.

First q must be large enough to ensure that the conic C is completely determined by the arc S. Let S be an arc with conical subset R and excess $|S \setminus R| = e$. If C' is another conic giving rise to the conical subset $R' = S \cap C'$ with $|S \setminus R'| = e'$. Then by [1, Lemma 3], we know that $e' \ge |R| - 4$. As an immediate consequence we obtain the following result.

Lemma 3. Let PG(2,q) be of even order. If $q \ge 16$ then an arc of PG(2,q) with a large conical subset of excess e < 5 can contain at most one such conical subset.

Proof. If S has a large conical subset of excess e, then by the above $e' \ge q/2 - 3$ and hence $e' \ge 5$ when $q \ge 16$. Hence, any other conical subset will have an excess that is too large.

In this section we shall consider an arc S with a large conical subset of excess 2. First note that the nucleus of the corresponding conic cannot be one of the supplementary points: otherwise the line joining the supplementary points would be a tangent to C and then 3 points of that tangent would belong to S.

Hence we may assume that the line joining the supplementary points is external to C, and without loss of generality we may assume that this line is the line ℓ introduced in the previous section. In fact, we may even assume that one of the supplementary points is Q_0 , and then the other is of the form Q_{2a} for some $a \in \mathbf{Z}_{q+1}$.

Consider the following graph Γ :

- Vertices are the elements of \mathbf{Z}_{q+1} ,
- Two different vertices i, j are adjacent if and only if the line $P_i P_j$ contains either Q_0 or Q_{2a} , i.e., if and only if $i + j \equiv 0$ or $2a \pmod{q+1}$. (Cf. Lemma 1.)

Note that the degree of a vertex of Γ is 2 in most cases, except for the vertices 0 and a which are of degree 1, because they lie on a tangent through Q_0 or Q_{2a} . It follows that Γ is the disjoint union of one path and a number (possibily zero) of cycles. We may enumerate the vertices of the cycle or path that contains i as follows:

$$\dots, i, -i, 2a+i, -2a-i, 4a+i, -4a-i, \dots$$
 (11)

For a cycle, this sequence eventually starts to repeat. For the path this sequence stops at 0 and a.

Define n to be the order of $2a \pmod{q+1}$ and let $d = \gcd(a, q+1) = (q+1)/n$. (n and d will always be odd.) Note that each of the vertices in (11) is equal to $\pm i \pmod{d}$. Also note that 0 and a are both divisible by d. Hence, if $i \not\equiv 0 \pmod{d}$, then (11) denotes a cycle, and not a path. The cycle either has length $2n \pmod{i} \equiv 2na + i \pmod{q+1}$, or length $2n + 1 \pmod{i} \equiv -2na - i \pmod{q+1}$. The latter case is impossible as the graph only has two types of edges and two consecutive edges never are of the same type, i.e. the number of edges in the cycle must be even. Hence the cycle has length 2n and must contain all vertices that are equal to $\pm i \pmod{d}$. The path has endpoints 0 and a and contains all points that are multiple of 2a. This implies that the path has size n.

This proves the following lemma.

Lemma 4. Γ is the disjoint union of (d-1)/2 cycles of length 2n and one path of n vertices, where n is the order of $2a \pmod{q+1}$ and d=(q+1)/n, i.e. $d=\gcd(a,q+1)$.

Define the set $Z_k \stackrel{\text{def}}{=} k + 2a\mathbf{Z}_{q+1} = k + d\mathbf{Z}_{q+1}$. We call Z_k a half cycle of Γ . The cycles of Γ are precisely the sets $Z_k \cup Z_{-k}$, with k in the range $1, \ldots, (d-1)/2$.

Denote by N(R) the set of orbital indices of vertices of the large conical subset R. Since S is an arc, N(R) must be an *independent set* of Γ . To have an independent set of size q/2+1 we need to take the largest possible independent set for each component of Γ .

When n is odd, as is the case here, the largest independent set in a path with n vertices is unique and has size (n+1)/2. The largest independent set in a cycle is one of its two half cycles and has length n. This proves the following result.

Theorem 5. Let $a \in \{1, ..., q\}$. Let $d = \gcd(a, q + 1)$, n = (q + 1)/d. Let $S = R \cup \{Q_0, Q_{2a}\}$, with $R \subset C$ and |R| = q/2 + 1. Then S is an arc of PG(2, q) if and only if N(R) can be written as the union of pairwise disjoint sets, of the form

$$N(R) = \Pi \cup Z_{\pm 1} \cup \ldots \cup Z_{\pm (d-1)/2},$$

with independent choices of sign, and

$$\Pi = \{0, -2a, -4a, \cdots, a\}.$$

Every arc listed in Theorem 5 can be denoted by its signature $(a; \epsilon_1, \ldots, \epsilon_{(d-1)/2})$, where $\epsilon_k = \pm 1$ depending on the choice made for the half cycle $Z_{\pm k}$.

Theorem 6. Let q be even, $a \in \{1, ..., q\}$, $d = \gcd(a, q + 1)$ and n = (q + 1)/d. Let H_a denote the subgroup of $\operatorname{PGL}(3, q)$ that leaves the conic C invariant and fixes the pair $\{Q_0, Q_{2a}\}$. Then $H_a = \{M'_0, M_a\}$ and acts as follows on the components of Γ and the arc with signature $(a; \epsilon_1, ..., \epsilon_{(d-1)/2})$

Element of H_a	Image of Z_k	Image of	
		$(a;\epsilon_1,\ldots,\epsilon_{\frac{d-1}{2}})$	
M_0' (the identity)	Z_k	$(a; \epsilon_1, \dots, \epsilon_{\frac{d-1}{2}})$	
M_a	Z_{-k}	$\left (a; -\epsilon_1, \dots, -\epsilon_{\frac{d-1}{2}}) \right $	

Proof. Note that H_a must fix the line joining Q_0 and Q_{2a} , i.e., ℓ , and hence is a subgroup of H. From (7) it follows that the identity is the only transformation that fixes both Q_0 and Q_{2a} and that M_a is the only element of H that interchanges Q_0 and Q_{2a} .

By (7), M_a maps Z_k onto Z_{a-k} . Half cycle indices are determined modulo d, and a is a multiple of d. Hence $Z_{a-k} = Z_{-k}$

Corollary 7. Let $q \ge 16$, q even. Let H_S denote the subgroup of PG(3,q) that leaves invariant the arc S with signature $(a; \epsilon_1, \ldots, \epsilon_{d-1})$. If d = 1, then $H_S = H_a$. Otherwise, H_S is trivial.

Lemma 8. Let $L_q(a)$ denote the number of projectively inequivalent arcs S with a signature of the form $(a; \epsilon_1, \ldots, \epsilon_{(d-1)/2})$, with $d = \gcd(a, q+1)$. Then

$$L_q(a) = \begin{cases} 1, & when \ d = 1, \\ 2^{\frac{d-3}{2}}, & when \ d > 1. \end{cases}$$
 (12)

Proof. If d=1, then there is clearly the one signature (a). Otherwise, when d>1, the number of signatures is equal to $2^{(d-1)/2}$ and the value of $|S^{H_a}|=|H_a|/|H_S|$ is equal to 2 for each such arc. Hence, $L_q(a)=\frac{2^{(d-1)/2}}{2}$ for d>1.

Theorem 9. Let $q \ge 16$, q even. The number L_q of projectively inequivalent arcs S in PG(2,q) of size |S| = q/2 + 3, with a conical subset $R = S \cap C$ of size |R| = q/2 + 1, is given by

$$L_q = \frac{1}{2} \sum_{d}' \phi \left(\frac{q+1}{d} \right) L_q(d) \tag{13}$$

where the sum is restricted to all proper divisors d of q + 1, ϕ denotes Eulers totient function, and $L_q(d)$ is as given in Lemma 8.

Proof. Note that M_0 interchanges Q_{2a} and Q_{-2a} and fixes Q_0 , and hence to enumerate all arcs up to isomorphism, we should consider only one of a and q+1-a. In other words, we may take a in the range $1, \ldots, q/2$.

The total number of inequivalent arcs is then given by $\sum_{a=1}^{q/2} L_q(a)$. Note that $L_q(a)$ does not directly depend on a, but only on $d = \gcd(a, q+1)$. The number of integers a, $1 \le a \le q/2$ such that $d = \gcd(a, q+1)$ is equal to $\frac{1}{2}\phi((q+1)/d)$.

The table below lists the values of L_q for small values of q.

q	16	32	64	128	256
L_q	8	31	100	1048639	128

For larger values of q the value of L_q becomes very large, unless q+1 is a (Fermat) prime, in which case $L_q = q/2$.

For $32 \leqslant q \leqslant 256$ we have checked by computer that all of these arcs are complete. For q=16 four of the eight arcs are complete and there exist three inequivalent arcs of excess 3, all of them complete.

Acknowledgements

We would like to thank the anonymous referees for helpful comments and suggestions and for correcting an error in the original proof of Lemma 2.

References

- [1] K. Coolsaet and H. Sticker. Arcs with Large Conical Subsets. Electron. J. Combin. 17 (2010), #R112
- [2] J. W. P. Hirschfeld. *Projective geometries over finite fields* (second edition) (1988). Clarendon Press, Oxford.
- [3] L. Lombardo-Radice. Sul problema dei k-archi completi in $S_{2,q}$. Boll. Un. Mat. Ital. (3)11 (1956), pp. 178–181.
- [4] B. Segre. *Introduction to Galois geometries*. Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8)8 (1967), pp. 133–236.