Arcs with large conical subsets

K. Coolsaet H. Sticker

Department of Applied Mathematics and Computer Science
Ghent University
Krijgslaan 281–S9, B–9000 Gent, Belgium

Kris.Coolsaet@UGent.be, Heide.Sticker@UGent.be

Submitted: Dec 16, 2009; Accepted: Jul 29, 2010; Published: Aug 9, 2010
Mathematics Subject Classification: 51E21

Abstract

We classify the arcs in $\mathrm{PG}(2,q)$, q odd, which consist of $(q+3)/2$ points of a conic C and two points not on te conic but external to C, or $(q+1)/2$ points of C and two additional points, at least one of which is an internal point of C. We prove that for arcs of the latter type, the number of points internal to C can be at most 4, and we give a complete classification of all arcs that attain this bound. Finally, we list some computer results on extending arcs of both types with further points.

1 Introduction

Consider the Desarguesian projective plane $\mathrm{PG}(2,q)$ over the finite field of order q, with q odd. For k a positive integer, define a *k-arc* to be a set S of points of $\mathrm{PG}(2,q)$ of size $|S|=k$, such that no three elements of S are collinear. An arc S 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 $k=q+1$ and that an arc in that case always coincides with the set of points of some conic C (and is complete). It is natural to ask what the second biggest size for a complete arc in $\mathrm{PG}(2,q)$ is.

Removing some points from a conic C yields an arc, but this arc is obviously not complete. However, removing a sufficient number of points (at least $(q-1)/2$, as will be shown later) it may be possible to extend the set thus obtained to an arc by adding a point that does not belong to C. This new arc might not be complete, but can be made complete by adding yet more points. This is the kind of arc we will study in this paper. For many values of q, arcs of this type are among the largest ones known.

Let S be any arc. Then we define a *conical subset* of S to be any subset T of S of the form $T=S\cap C$ where C is a conic. In this paper, most of the time the conic C and the conical subset T will be clear from context. We will therefore usually leave out the

reference to C when talking about internal or external points of C, tangents and secants of C and lines external to C.

The elements of $U \stackrel{\text{def}}{=} S \backslash T$ will be called *supplementary* points and the number $e = |U|$ of supplementary points will be called the *excess* of the arc. We shall always assume that $e \geqslant 1$, i.e., that S is not fully contained in a conic.

Arcs with excess 1 fall into two categories, depending on whether the supplementary point Q is an external or an internal point (of C). When Q is an external point, the arc property for S implies that the two tangents through Q, and each of the $(q-1)/2$ secants through Q, may intersect T in at most one point, and hence that $|T| \leqslant (q+3)/2$. Likewise, when Q is an internal point, the $(q+1)/2$ secants imply that $|T| \leqslant (q+1)/2$ (there are no tangents through Q in this case).

We call conical subsets which attain these bounds *large*. In this paper we divide the arcs with large conical subsets into three categories :

- An arc S of *type I* has a conical subset of size $(q+1)/2$ where all supplementary points are *internal* points of C.
- An arc S of *type E* has a conical subset of size $(q+3)/2$ where all supplementary points are *external* points of C.
- An arc S of *type M* (for 'mixed') has a conical subset of size $(q+1)/2$ where some of the supplementary points are *internal* points of C and some are *external* points.

Only a few arcs are known with large conical subsets and with an excess greater than 2. The primary purpose of this paper is to establish a simple theoretical framework for an extensive computer search for arcs of that type. In Sections 3, 4 and 5 we provide a complete (computer-free) classification of all such arcs with excess 2, up to projective equivalence (i.e., equivalence with respect to the group $\mathrm{PGL}(3,q)$). This classification forms the basis for a fast computer program that classifies arcs with larger excess, for specific values of q. Results of these searches are presented in Section 7.

Arcs of this type have also been studied by Pellegrino [5, 6], Korchmáros and Sonnino [3, 4] and Davydov, Faina, Marcugini and Pambianco [2]. In particular, our methods are similar to those of Korchmáros and Sonnino [4], except for a few differences which we think are important :

- Instead of using the group structure of a cyclic affine plane of order q, we use the properties of the cyclic group of norm 1 elements of the field $\mathrm{GF}(q^2)$. This has the advantage that much of the theory that is developed subsequently can be formulated in terms of integers modulo $q+1$, i.e., without the explicit use of groups.
- As a consequence, we were able to write down a complete classification of the arcs of excess 2 and obtain an explicit formula for the number of inequivalent arcs of that type.
- Korchmáros and Sonnino have used a computer algebra system (Magma) to implement their computer searches. Because we do not need the group functionality we could instead implement a very straightforward (and efficient) program in Java.

Also note that Korchmáros and Sonnino only treat arcs of type E.

2 Notation and preliminary definitions

Before we proceed to the main part of the paper, we shall first establish some notations and list some elementary results. Most of the properties described here belong to 'mathematical folklore' and shall be given without proof. Similar notation and properties are used in [5, 6].

Let K denote the field of order q. In what follows we shall use the abbreviation $r \stackrel{\text{def}}{=} \frac{1}{2}(q+1)$.

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–one relation between $K \cup \{\infty\}$ and C.

The subgroup of $\mathrm{PGL}(3, q)$ that stabilizes C is isomorphic to $\mathrm{PGL}(2, q)$. The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts on the point with coordinates $(1 : t : t^2)$ by sending t to $\dfrac{b+dt}{a+ct}$.

With every point Q of the plane that does not belong to C we associate an involution σ_Q on the points of C, as follows : if P is a point of C, then $\sigma_Q(P)$ is the second intersection of the line PQ with C (or equal to P when PQ is tangent to C). This involution can be extended to the entire plane and corresponds to the matrix

$$M_Q \stackrel{\text{def}}{=} \begin{pmatrix} b & c \\ -a & -b \end{pmatrix},$$

when Q has coordinates $(a : b : c)$. On the plane σ_Q has exactly $q+2$ fixed points: the point Q and the $q+1$ points on the polar line of Q with respect to C. The lines fixed by σ_Q are the $q+1$ lines through Q and the polar line of Q.

Conversely, every involution of $\mathrm{PGL}(2, q)$ has trace zero and must therefore be of the form σ_Q for some point Q not on C.

Q is an external point to C if and only if $-\det M_Q = b^2 - ac$ is a (non-zero) square of K. In that case the two points of C whose tangents go through Q have coordinates $(1 : t : t^2)$ with $t = c/(b \pm \sqrt{b^2 - ac})$.

Fix a non-square β of K and let $L = K[\sqrt{\beta}]$ denote the quadratic extension field of K. Let α be a primitive element of L. Then every element of L^* can be written as α^i for some exponent i which is unique modulo $q^2 - 1$. For $i \in \mathbf{Z}_{q^2-1}$ define $c_i, s_i \in K$ to be the 'real' and 'imaginary' part of α^i, i.e., $\alpha^i \stackrel{\text{def}}{=} c_i + s_i\sqrt{\beta}$. Note that c_i, s_i have properties that are similar to those of the cosine and sine, and therefore it is also natural to define a 'tangent' $t_i \stackrel{\text{def}}{=} s_i/c_i \in K \cup \{\infty\}$. We may express t_i directly in terms of $\phi \stackrel{\text{def}}{=} \alpha/\bar{\alpha}$, as follows :

$$t_i = \begin{cases} \dfrac{1}{\sqrt{\beta}} \dfrac{\phi^i - 1}{\phi^i + 1}, & \text{when } \phi^i \neq -1, \\ \infty, & \text{when } \phi^i = -1. \end{cases} \tag{1}$$

We have the following properties :

$$t_0 = t_{q+1} = 0, \quad t_{i+j} = \frac{t_i + t_j}{1 + t_i t_j \beta}, \quad t_{i+(q+1)} = t_i, \quad t_{-i} = -t_i, \quad t_r = \infty, \quad t_{i+r} = \frac{1}{t_i \beta}.$$

(Recall that $r = (q+1)/2$.) The index i of t_i can be treated as an element of $\mathbf{Z}_{q+1}$. The sequence $t_0, t_1, \ldots, t_q$ contains every element of $K \cup \{\infty\}$ exactly once.

Let ℓ be an external line of C. Without loss of generality we may assume that ℓ has equation $X = \beta Z$. The points of ℓ may be numbered as $Q_0, Q_1, \ldots, Q_q$ so that Q_i has coordinates $(s_i\beta : c_i : s_i)$. When $i \neq 0$, we may normalize these coordinates to $(\beta : 1/t_i : 1)$, while Q_0 has coordinates $(0 : 1 : 0)$. 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 point Q_i is an external (resp. internal) point of C if and only if its orbital index i is even (resp. odd).

In a similar way, we number the points of the conic C as $P_0, P_1, \ldots, P_q$ where P_i has coordinates $(1 : t_i : t_i^2)$, for $i \neq r$ and P_r has coordinates $(0 : 0 : 1)$. Again, the index i of P_i will be called its *orbital index*, and again it can be treated as an element of $\mathbf{Z}_{q+1}$.

The following lemma illustrates that orbital indices are a useful concept in this context.

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

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

The subgroup G of $\mathrm{PGL}(3, q)$ that leaves both the conic C and its external line ℓ invariant, is a dihedral group of order $2(q+1)$ whose elements correspond to matrices of the following type :

$$M_i \stackrel{\text{def}}{=} \begin{pmatrix} c_i & s_i \\ -s_i\beta & -c_i \end{pmatrix} \approx \begin{pmatrix} 1 & t_i \\ -t_i\beta & -1 \end{pmatrix}, \quad M_i' \stackrel{\text{def}}{=} \begin{pmatrix} c_i & s_i \\ s_i\beta & c_i \end{pmatrix} \approx \begin{pmatrix} 1 & t_i \\ t_i\beta & 1 \end{pmatrix}.$$

(The '$\approx$'-sign denotes equality upto a scalar factor.)

We have

$$M_0' = 1, \quad M_i' = {M_1'}^i, \quad M_{i+j}' = M_i' M_j'.$$

(Again indices can be treated as belonging to $\mathbf{Z}_{q+1}$.)

We shall call these group elements *reflections* and *rotations* (reminiscent of similar transformations in the Euclidian plane). Note that the reflections are precisely the involutions σ_Q for the points of ℓ. Indeed $M_i \approx M_{Q_i}$. Apart from these reflections, the group G contains one more involution: the element M_r' which could also be written as σ_R, where R is the pole of ℓ, with coordinates $(-\beta : 0 : 1)$.

The action of the reflections and rotations on C and ℓ is given by

$$\begin{array}{rcccccc} M_i & : & P_j & \mapsto & P_{i-j}, & \qquad Q_j & \mapsto & Q_{2i-j}, \\ M_i' & : & P_j & \mapsto & P_{j+i}, & \qquad Q_j & \mapsto & Q_{j+2i}. \end{array}$$

Note the factor 2 in the orbital index of the images of Q_j. This ensures that even orbital indices remain even and odd indices remain odd. Indeed, the group G has two orbits on

ℓ, one consisting of external points, the other of internal points. Note that M'_r stabilizes *every* point of ℓ.

The stabilizer G_k of Q_k in G has order 4 and consists of M'_0 (the identity), M'_r, M_k and M_{k+r}. G_k fixes Q_k and Q_{k+r} and interchanges Q_i and Q_{2k-i} for $i \neq a, a+r$.

3 Arcs of type I with excess two

In this and the following sections we shall treat arcs S with a large conical subset and excess two. Before we proceed to the case of arcs of type I, we first introduce the following definitions that will be useful in all three cases.

Let C be a conic and let U denote a set of points not on that conic (the supplementary points of an arc S, say). Define the graph $\Gamma(C, U)$ as follows :

- Vertices are the elements of $\mathbf{Z}_{q+1}$,
- Two different vertices i, j are adjacent if and only if the line P_iP_j contains a point of U.

Note that the degree of a vertex of $\Gamma(C, U)$ is at most $|U|$.

Let S be an arc with corresponding conical subset $T = C \cap S$. Write $U = S \setminus T$. Denote by $N(T)$ the set of orbital indices of vertices of T, i.e., the unique subset of $\mathbf{Z}_{q+1}$ such that $T = \{P_i \mid i \in N(T)\}$. Since S is an arc, no pair of points of T can be collinear with one of the supplementary points. Therefore, in $\Gamma(C, U)$, vertices of $N(T)$ can never be adjacent. In other words, $N(T)$ is an *independent set* of $\Gamma(C, U)$.

We now turn to the case where S denotes an arc of type I with excess two, i.e., $|T| = r = (q+1)/2$ and U consists of two points that are internal to C.

As was explained in the introduction, each secant line through one of the supplementary points intersects C in exactly one point of T. In particular, since S is an arc, the line that joins the supplementary points cannot contain a third point of S, and hence is not a secant line of C. Because the supplementary points are internal, the line cannot be a tangent to C either and hence it must be an external line.

Without loss of generality we may assume this line to be ℓ. All internal points on ℓ lie in a single orbit of G, and therefore we may take the first of the supplementary points to be Q_1. The second supplementary point must have an odd orbital index, and therefore is of the form Q_{2a+1}. Note that the integer a is only determined up to a multiple of r.

Consider the graph $\Gamma = \Gamma(C, U) = \Gamma(C, \{Q_1, Q_{2a+1}\})$. The edges of Γ are of the form $\{j, 1-j\}$ and $\{j, 2a+1-j\}$ (by Lemma 1) and therefore Γ must be a regular graph of order $q+1$ and of degree 2, i.e., a disjoint union of cycles.

Consider the cycle which contains vertex i. We can enumerate the consecutive vertices in this cycle as follows :

$$\ldots, i, 1-i, 2a+i, 1-2a-i, 4a+i, 1-4a-i, \ldots$$

Eventually this sequence starts to repeat, hence either the cycle has length $2n$ with $i = (2na) + i \pmod{q+1}$, or length $2n+1$ with $i = 1 - (2na) - i \pmod{q+1}$. The latter

case would imply $2(na+i) = 1 \pmod{q+1}$ which is impossible as $q+1$ is even, hence the first case applies. Hence n is equal to the order of $2a \pmod{q+1}$, i.e., n is the smallest positive integer such that $na = 0 \pmod{r}$. Note that n is independent of the choice of i and therefore all cycles have the same size. This proves the following result.

Lemma 2 *If S is an arc of type I with supplementary points Q_1 and Q_{2a+1}, then $\Gamma(C,U)$ consists of d disjoint cycles of length $2n$, where n is the order of $a \pmod{r}$ and $d = r/n$, i.e., $d = \gcd(a,r)$.*

Note that the largest independent set in a cycle of size $2n$ has size n and consists of alternating vertices. We shall call these sets *half cycles*. There are two disjoint half cycles in each cycle. In our particular example, let $Z_k \stackrel{\text{def}}{=} k + 2a\mathbf{Z}_{q+1} = k + 2d\mathbf{Z}_{q+1}$. Define $Z_k^+ = Z_k$, $Z_k^- = Z_{1-k}$. Then $Z_k^+ \cup Z_k^-$, $k = 1, \ldots, d$, are the cycles that constitute Γ and Z_k^+, Z_k^- are the corresponding half cycles.

It is now easy to see that the largest possible independent set of Γ consists of d half cycles, one for each cycle, and therefore has size $dn = r$. Recall that $N(T)$ must be an independent set of Γ. This proves the following result.

Theorem 1 *Let $a \in \{1, \ldots, r-1\}$. Let $d = \gcd(a,r)$. Let $S = T \cup \{Q_1, Q_{2a+1}\}$, with $T \subset C$ and $|T| = (q+1)/2$. Then S is an arc of $\mathrm{PG}(2,q)$ if and only if $N(T)$ can be written as a disjoint union of the form*

$$N(T) = Z_1^{\pm} \cup \ldots \cup Z_d^{\pm},$$

with independent choices of sign.

Every arc listed in Theorem 1 can be uniquely described by its *signature* $I(a; \epsilon_1, \ldots, \epsilon_d)$, where $\epsilon_k = \pm 1$ depending on the choice made for the half cycle $Z_k^{\pm}$. Of course, arcs with different signature can still be projectively equivalent, even for fixed a. More work needs to be done to enumerate all arcs of this type up to equivalence only.

Before we proceed, we want to point out that some caution is necessary when q is small. Indeed, in the treatment above, we have always considered the conic C as fixed. However, there are many conics, and therefore for a given arc S there could be several conical subsets that are large. Fortunately, we have the following

Lemma 3 *Let S be an arc with a conical subset T with excess e. Then the excess e' of any other conical subset T' of S must satisfy*

$$e' \geqslant |S| - e - 4 = |T| - 4.$$

Proof : Two different conics can intersect in at most 4 points. Hence also T and T' can intersect in at most 4 points. We have

$$|S| + |S| = |T| + e + |T'| + e' = e + e' + |T \cup T'| + |T \cap T'| \leqslant e + e' + |S| + 4,$$

and therefore $|S| \leqslant e + e' + 4$. ∎

Corollary 1 *If $q \geqslant 13$, then an arc S of $\mathrm{PG}(2,q)$ of size $|S| = (q+5)/2$ can contain at most one conical subset with excess at most 2.*

Proof : Assume S has a conical subset T with excess $e \leqslant 2$. Then by Lemma 3, any other conical subset must have excess $e' \geqslant (q+5)/2 - e - 4 \geqslant 9 - 2 - 4 = 3$. ∎

Henceforth we shall assume that $q \geqslant 13$.

By the above, S determines C uniquely. Any isomorphism between any of the arcs listed in Theorem 1 must therefore leave C invariant, and also the pair of supplementary points and the line ℓ. In other words, any isomorphism of this type must belong to the group G.

From Section 2 we know that the elements of G that fix Q_1 are the following :

$$\begin{array}{lcccccc} M_0' \text{ (the identity)} & : & P_j & \mapsto & P_j, & Q_j & \mapsto & Q_j, \\ M_r' & : & P_j & \mapsto & P_{j+r}, & Q_j & \mapsto & Q_j, \\ M_1 & : & P_j & \mapsto & P_{1-j}, & Q_j & \mapsto & Q_{2-j}, \\ M_{r+1} & : & P_j & \mapsto & P_{r+1-j}, & Q_j & \mapsto & Q_{2-j}. \end{array} \tag{2}$$

Note that the reflections M_1 and M_{r+1} interchange Q_{2a+1} and Q_{1-2a}. In other words, for every arc with a signature of the form $I(a;\epsilon_1,\cdots,\epsilon_d)$ there is an equivalent arc with a signature of the form $I(r-a;\epsilon_1',\cdots,\epsilon_d')$ (or $I(-a;\cdots)$, if you prefer). To enumerate all arcs up to isomorphism, it is therefore sufficient to consider only those a that satisfy $1 \leqslant a \leqslant r/2$.

We now consider the case where a is fixed.

Theorem 2 *Let $q \geqslant 13$, $a \in \{1,\ldots,r-1\}$ $d = \gcd(a,r)$ and $n = r/d$. Further, let H_a denote the subgroup of $\mathrm{PG}(3,q)$ that leaves the conic C invariant and fixes the pair $\{Q_1, Q_{2a+1}\}$. Then the elements of H_a are as follows :*

1. When $n \neq 2$

Element of H_a	*Image of $Z_k^{\pm}$*	*Image of $I(a;\epsilon_1,\ldots,\epsilon_d)$*	
M_0' *(the identity)*	$Z_k^{\pm}$	$I(a;\epsilon_1,\ldots,\epsilon_d)$	
M_r'	$Z_k^{\pm}$	$I(a;\epsilon_1,\ldots,\epsilon_d)$	*when n is even,*
	$Z_{d+k}^{\pm} = Z_{d+1-k}^{\mp}$	$I(a;-\epsilon_d,\ldots,-\epsilon_1)$	*when n is odd.*
M_{a+1}	$Z_{1-k}^{\pm} = Z_k^{\mp}$	$I(a;-\epsilon_1,\ldots,-\epsilon_d)$	*when a/d is even,*
	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$	*when a/d is odd.*
M_{a+r+1}	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$	*when n is even, a/d is odd,*
	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$	*when n is odd, a/d is even,*
	$Z_{1-k}^{\pm} = Z_k^{\mp}$	$I(a;-\epsilon_1,\ldots,-\epsilon_d)$	*when n is odd, a/d is odd.*

2. When $n = 2$

Element of H_a	*Image of* $Z_k^{\pm}$	*Image of* $I(a;\epsilon_1,\ldots,\epsilon_d)$
M'_0 *(the identity)*	$Z_k^{\pm}$	$I(a;\epsilon_1,\ldots,\epsilon_d)$
$M'_{r/2}$	$Z_{d+k}^{\pm} = Z_{d+1-k}^{\mp}$	$I(a;-\epsilon_d,\ldots,-\epsilon_1)$
M'_r	$Z_k^{\pm}$	$I(a;\epsilon_1,\ldots,\epsilon_d)$
$M'_{3r/2}$	$Z_{d+k}^{\pm} = Z_{d+1-k}^{\mp}$	$I(a;-\epsilon_d,\ldots,-\epsilon_1)$
M_1	$Z_{1-k}^{\pm} = Z_k^{\mp}$	$I(a;-\epsilon_1,\ldots,-\epsilon_d)$
$M_{r/2+1}$	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$
M_{r+1}	$Z_{1-k}^{\pm} = Z_k^{\mp}$	$I(a;-\epsilon_1,\ldots,-\epsilon_d)$
$M_{3r/2+1}$	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$

Proof : (Note that $n = r/d$ and a/d can not both be even, for otherwise $2d$ would be a divisor of both a and r, contradicting $d = \gcd(a, r)$. The case $n = 2$ is equivalent to $a = r/2$, and then $d = a$.)

Note that H_a fixes the line ℓ and hence is a subgroup of G. Any element of H_a must either fix the points Q_1 and Q_{2a+1} or interchange them.

From (2) we easily derive that the identity and M'_r will fix both points, and so will M_1 and M_{r+1} provided that $(2a + 1) = 2 - (2a + 1)$, i.e., when $4a = 0$, i.e., $a = r/2$.

Similarly, it is easily proved that the following elements of G are those that map Q_1 onto Q_{2a+1} :

$$\begin{array}{lcl} M'_a : P_j \mapsto P_{i+j}, & & Q_j \mapsto Q_{j+2a}, \\ M'_{a+r} : P_j \mapsto P_{a+r+j}, & & Q_j \mapsto Q_{j+2a}, \\ M_{a+1} : P_j \mapsto P_{a+1-j}, & & Q_j \mapsto Q_{2a+2-j}, \\ M_{a+r+1} : P_j \mapsto P_{a+r+1-j}, & & Q_j \mapsto Q_{2a+2-j}. \end{array}$$

and hence M_{a+1} and M_{a+r+1} interchange Q_1 and Q_{2a+1}, and so do M'_a and M'_{a+r} when $4a = 0$, i.e., $a = r/2$.

To complete the proof, we compute the action of these isomorphisms on the half cycles Z_k. (And from these, the action on the signatures can be easily computed.)

A rotation of the form M'_i maps a vertex k of Γ to the vertex $k + i$. Hence $Z_k = k + 2d\mathbf{Z}_{q+1}$ is mapped to $k + i + 2d\mathbf{Z}_{q+1} = Z_{k+i}$. Similarly, the reflection M_i maps k to $i - k$ and hence $Z_k = k + 2d\mathbf{Z}_{q+1}$ to $i - k - 2d\mathbf{Z}_{q+1} = Z_{i-k}$.

Note that indices of half cycles can be treated modulo $2d$. For example, as r is a multiple of d, Z_{k+r} is equal to either Z_k or Z_{k+d}, depending on whether $n = r/d$ is even or odd. Similarly, Z_{a+1-k} is either Z_{1-k} or Z_{d+1-k} depending on the parity of a/d. ∎

(Although this theorem is valid for all $a \in \{1,\ldots,r\}$, we only need it when $a \leqslant r/2$, as explained earlier.)

The group H_a in Theorem 2 contains precisely the projective equivalences that exist among the arcs listed in Theorem 1, for fixed a. The information given on the images of the signatures in the various cases allows us to compute the automorphism groups of the corresponding arcs.

Corollary 2 *Let $q \geqslant 13$. Let H_S denote the subgroup of* $\mathrm{PGL}(3,q)$ *that leaves invariant the arc S with signature $I(a;\epsilon_1,\ldots,\epsilon_d)$.*

1. If n is even and $n \neq 2$, then

- $H_S = \{M'_0, M'_r, M_{a+1}, M_{a+r+1}\}$ *if and only if* $\epsilon_d = \epsilon_1, \epsilon_{d-1} = \epsilon_2, \ldots$,
- $H_S = \{M'_0, M'_r\}$ *otherwise.*

2. If n is odd and a/d is odd, then

- $H_S = \{M'_0, M'_r\}$ *if and only if* $\epsilon_d = -\epsilon_1, \epsilon_{d-1} = -\epsilon_2, \ldots$ *(d even),*
- $H_S = \{M'_0, M_{a+1}\}$ *if and only if* $\epsilon_d = \epsilon_1, \epsilon_{d-1} = \epsilon_2, \ldots$,
- $H_S = \{M'_0\}$ *otherwise.*

3. If n is odd and a/d is even, then

- $H_S = \{M'_0, M'_r\}$ *if and only if* $\epsilon_d = -\epsilon_1, \epsilon_{d-1} = -\epsilon_2, \ldots$ *(d even),*
- $H_S = \{M'_0, M_{a+r+1}\}$ *if and only if* $\epsilon_d = \epsilon_1, \epsilon_{d-1} = \epsilon_2, \ldots$,
- $H_S = \{M'_0\}$ *otherwise.*

4. If $n = 2$, then

- $H_S = \{M'_0, M'_{r/2}, M'_r, M'_{3r/2}\}$ *if and only if* $\epsilon_d = -\epsilon_1, \epsilon_{d-1} = -\epsilon_2, \ldots$ *(d even),*
- $H_S = \{M'_0, M'_r, M_{r/2+1}, M_{3r/2+1}\}$ *if and only if* $\epsilon_d = \epsilon_1, \epsilon_{d-1} = \epsilon_2, \ldots$,
- $H_S = \{M'_0, M'_r\}$ *otherwise.*

The theorems above provide us with sufficient information to count the number of arcs of type I for given q. Again we first consider the case where a is fixed.

Lemma 4 *Let $I_q(a)$ denote the number of projectively inequivalent arcs S with a signature of the form $I(a;\epsilon_1,\ldots,\epsilon_d)$, with $d = \gcd(a,(q+1)/2)$. Then*

$$I_q(a) = \begin{cases} 2^{d-2} + 2^{\lfloor \frac{d-2}{2} \rfloor}, & \text{when } \frac{q+1}{2d} \text{ is odd or } \frac{q+1}{2d} = 2, \\ 2^{d-1} + 2^{\lfloor \frac{d-1}{2} \rfloor}, & \text{when } \frac{q+1}{2d} \text{ is even and } \frac{q+1}{2d} \neq 2. \end{cases} \tag{3}$$

Proof : The number $I_q(a)$ is obtained by summing the value of $1/|S^{H_a}|$ over all arcs S with a signature of the form $I(a;\epsilon_1,\ldots,\epsilon_d)$, where H_a is as in Theorem 2 and $|S^{H_a}|$ is the size of the orbit of H_a on this arc. We have $|S^{H_a}| = |H_a|/|H_S|$, where $|H_S|$ can be derived from Corollary 2.

The number of signatures with $\epsilon_d = \epsilon_1, \epsilon_{d-1} = \epsilon_2, \ldots$ is equal to $2^{d/2}$ when d is even, and to $2^{(d+1)/2}$ when d is odd, i.e., $2^{\lfloor (d+1)/2 \rfloor}$ for general d. Similarly the number of signatures

with $\epsilon_d = -\epsilon_1, \epsilon_{d-1} = \epsilon_2, \ldots$ is equal to $2^{d/2}$ when d is even, and is zero when d is odd. The sum of these two values is equal to $2^{\lfloor (d+2)/2 \rfloor}$ for general d.

The four cases of Corollary 2 now lead to the following values for $I_q(a) = \sum |H_S|/|H_a|$:

1. If n is even and $n \neq 2$, then

$$I_q(a) = 2^{\lfloor \frac{d+1}{2} \rfloor} + \frac{1}{2}(2^d - 2^{\lfloor \frac{d+1}{2} \rfloor}) = 2^{d-1} + 2^{\lfloor \frac{d-1}{2} \rfloor}.$$

2 and 3. If n is odd, then

$$I_q(a) = \frac{1}{2}2^{\lfloor \frac{d+2}{2} \rfloor} + \frac{1}{4}(2^d - 2^{\lfloor \frac{d+2}{2} \rfloor}) = 2^{d-2} + 2^{\lfloor \frac{d-2}{2} \rfloor}.$$

4. If $n = 2$, then

$$I_q(a) = \frac{1}{2}2^{\lfloor \frac{d+2}{2} \rfloor} + \frac{1}{4}(2^d - 2^{\lfloor \frac{d+2}{2} \rfloor}) = 2^{d-2} + 2^{\lfloor \frac{d-2}{2} \rfloor}.$$

∎

Theorem 3 *Let $q \geqslant 13$. The number I_q of projectively inequivalent arcs S in $\mathrm{PG}(2,q)$ of size $|S| = (q+5)/2$, with a conical subset $T = S \cap C$ of size $|T| = (q+1)/2$ such that the elements of $S \setminus T$ are internal points of C, is given by*

$$\sum_d{}' \lceil \frac{1}{2}\phi\left(\frac{q+1}{2d}\right) \rceil I_q(d)$$

where the sum is taken over all proper divisors d of $(q+1)/2$, ϕ denotes Eulers totient function, and $I_q(d)$ is as given in Lemma 4.

Proof : The total number of inequivalent arcs is given by $\sum_{a=1}^{\lfloor r/2 \rfloor} I_q(a)$. Note that $I_q(a)$ does not directly depend on a, but only on $d = \gcd(a,r)$. The number of integers a, $1 \leqslant a < r$ such that $d = \gcd(a,r)$ is equal to $\phi(r/d) = \phi(n)$. If we restrict ourselves to $a \leqslant r/2$ we obtain $\phi(n)/2$ values, except when $a = d = r/2$ (or equivalently $n = 2$) in which case there is 1 value. Note that $\phi(2) = 1$ and hence $\lceil \frac{1}{2}\phi(n) \rceil = 1$ in this case. ∎

4 Arcs of type E with excess two

The arcs of type E are in many aspects very similar to those of type I in the previous section. We shall therefore mainly focus on the differences between both cases.

Arcs of type E have a conical subset T of size $|T| = (q+3)/2$ (which is one larger than in the other cases). As a consequence, not only must all secants through a given supplementary point Q contain exactly one point of T, but also the tangents through Q must contain a point of T. (The points of T on these tangents will be called the *tangent points* of Q.) As a consequence, again any line through two supplementary points must be external.

Hence, for an arc of type E with two supplementary points, we may without loss of generality assume ℓ to be the line connecting these points, and assume that the supplementary points are Q_0 and Q_{2a} for some $a \in \mathbf{Z}_r, a \neq 0$. The tangent points for Q_0 are P_0 and P_r, and those of Q_{2a} are P_a and P_{a+r}.

Consider the graph $\Gamma = \Gamma(C, U) = \Gamma(C, \{Q_0, Q_{2a}\})$. The edges of Γ are of the form $\{j, -j\}$ or $\{j, 2a - j\}$, whenever such a set represents a pair and not a singleton. Every vertex of this graph has degree 2, except the four vertices 0, r, a and $a+r$ that correspond to the tangent points, which have degree 1. It follows that Γ is the disjoint union of two paths and some (possibily zero) cycles. We may enumerate the vertices of the cycle or path that contains i as follows :

$$\ldots, i, -i, 2a + i, -2a - i, 4a + i, -4a - i, \ldots \tag{4}$$

For a cycle, this sequence eventually starts to repeat. For a path this sequence stops at one of the values $0, r, a$ or $a + r$.

As before, define n to be the order of $2a \pmod{q+1}$ and let $d = \gcd(a, r) = r/n$. Note that each of the vertices in (4) is equal to $\pm i \pmod{d}$. Also note that $0, r, a, a + r$ are all divisible by d. Hence, if $i \neq 0 \pmod{d}$, then (4) denotes a cycle, and not a path. As in Section 3 it is easy to prove that this cycle must have length $2n$ and must contain all vertices that are equal to $\pm i \pmod{d}$.

Also, if (4) would denote a cycle also in the case that $i = 0 \pmod{d}$, then again it would have length $2n$ and contain all vertices that are divisible by d, including $0, r, a$ and $a + r$. This is a contradiction, and it follows that the two paths together contain all vertices that are multiples of a. The following lemma provides further information on the composition of these paths.

Lemma 5 *The two paths that are components of Γ each contain n vertices. The endpoints of these paths are as follows :*

n even	*n odd*	
	a/d even	*a/d odd*
$0 \cdots r$	$0 \cdots a$	$0 \cdots a + r$
$a \cdots a + r$	$r \cdots a + r$	$r \cdots a$

Proof : Consider the path that has vertex 0 as one of its endpoints. The vertices of this path are $0, 2a, -2a, 4a, -4a, \ldots$ and hence the other endpoint must be an element of $\{r, a, a + r\}$ that is a multiple of $2a \pmod{q+1}$). We consider three cases :

1. Assume that r is a multiple of $2a$, say $r = 2ak \pmod{q+1}$ for some k. Note that k can always be chosen to satisfy $0 < k < n$. We have $4ak = 2r = 0 \pmod{q+1}$ and hence $2k$ must be a multiple of the order of $2a \pmod{q+1}$, which is n. Because $0 < k < n$, this is only possible when $k = n/2$, hence when n is even.

2. Assume that a is a multiple of $2a$, say $a = 2ak' \pmod{q+1}$, with $0 < k' < n$. Then $(2k'-1)a = 0 \pmod{q+1}$ and n divides $2k'-1$. Hence n must be odd and $k' = (n+1)/2$. Note that in this case $an = 2ank' = 0 \pmod{q+1}$, and hence $an/r = 0 \pmod{(q+1)/r}$, i.e., $an/r = a/d$ is even.

3. Assume that $a+r$ is a multiple of $2a$, say $a+r = 2ak'' \pmod{q+1}$, with $0 < k'' < n$. Then $(2k''-1)2a = 0 \pmod{q+1}$ and n divides $2k''-1$. Hence n must be odd and $k'' = (n+1)/2$. In this case $an = 2ank'' - rn = r \pmod{q+1}$, and then $an/r = a/d$ is odd.

It follows that the end point of the path that starts with 0 is completely determined by the parity of n and of a/d, and must be as in the statement of this lemma. To prove that each path contains exactly n vertices, it is sufficient to show that each path has the same size. To prove this we shall establish an automorphism of Γ that interchanges the two paths.

Consider the map $i \mapsto a - i \pmod{q+1}$. Note that $i + j = 0$ if and only if $(a - i) + (a - j) = 2a$ and that $i + j = 2a$ if and only if $(a - i) + (a - j) = 0$. Hence, this is an automorphism of Γ. Similarly, consider the map $i \mapsto i + r \pmod{q+1}$. We have $(r + i) + (r + j) = i + j$, and therefore again this is an automorphism of Γ, and so is the product of these two maps, i.e., the map $i \mapsto a + r - i \pmod{q+1}$. In each of the three cases, two of these maps interchange the paths, and one leaves them invariant (but interchanges their endpoints). ∎

This provides us with the analogue of Lemma 2 :

Corollary 3 *If S is an arc of type E with supplementary points Q_0 and Q_{2a}, then $\Gamma(C, S \setminus C)$ is the disjoint union of $d-1$ cycles of length $2n$ and two paths of n vertices each, where n is the order of $a \pmod r$ and $d = r/n$, i.e., $d = \gcd(a, r)$.*

As in Section 3, we introduce the half cycles $Z_k \stackrel{\text{def}}{=} k + 2a\mathbf{Z}_{q+1} = k + 2d\mathbf{Z}_{q+1}$. The cycles of Γ can now be written as $Z_k \cup Z_{-k}$, with k in the range $1, \ldots, d-1$.

Note that the largest independent set in a path with n vertices has size $n/2$ when n is even and size $(n+1)/2$ when n is odd. To have an independent set $N(T)$ of size $(q+3)/2 = 2an+1$ in Γ it is therefore necessary that n is odd, and then we need to take the largest possible independent set for each component. This proves

Theorem 4 *Let $a \in \{1, \ldots, r-1\}$. Let $d = \gcd(a, r)$, $n = r/d$. Let $S = T \cup \{Q_1, Q_{2a+1}\}$, with $T \subset C$ and $|T| = (q+3)/2$. Then S is an arc of $\mathrm{PG}(2, q)$ if and only if n is odd and $N(T)$ can be written as a disjoint union of the form*

$$N(T) = \Pi \cup \Pi' \cup Z_{\pm 1} \cup \ldots \cup Z_{\pm(d-1)},$$

with independent choices of sign, and

$$\begin{aligned} \Pi &= \{0, -2a, -4a, \cdots r + a \text{ or } a\}, \\ \Pi' &= \{r, r-2a, r-4a, \cdots a \text{ or } r + a\} (= \Pi + r). \end{aligned}$$

(Theorem 3 of [2] corresponds to the special case $n = 3$ of this result.)

Corollary 4 *When $q+1$ is a power of 2 there are no arcs of type E with excess larger than 1.*

We shall identify the arcs in Theorem 4 by their signature $E(a;\epsilon_1,\ldots,\epsilon_{d-1})$, where $\epsilon_k = \pm 1$ depends on the choice made for the half cycle $Z_{\pm k}$.

As before, we shall now determine what isomorphisms exist between arcs of this type. Lemma 3 in this case has the following

Corollary 5 *If $q \geqslant 11$, then an arc S of $\mathrm{PG}(2,q)$ of size $|S| = (q+7)/2$ can contain at most one conical subset with excess at most 2.*

We shall therefore assume that $q \geqslant 11$ for the remainder of this section.

From Section 2 we obtain the elements of G that fix Q_0 :

$$\begin{array}{lcccccc} M_0' \text{ (the identity)} & : & P_j & \mapsto & P_j, & Q_j & \mapsto & Q_j, \\ M_r' & : & P_j & \mapsto & P_{j+r}, & Q_j & \mapsto & Q_j, \\ M_0 & : & P_j & \mapsto & P_{-j}, & Q_j & \mapsto & Q_{-j}, \\ M_r & : & P_j & \mapsto & P_{r-j}, & Q_j & \mapsto & Q_{-j}. \end{array} \tag{5}$$

The reflections M_0 and M_r interchange Q_{2a} and Q_{-2a}, and hence to enumerate all arcs up to isomorphism, it is therefore sufficient to consider only one of a and $r-a$. Because n must be odd, $r = nd$ is an odd multiple of d and hence one of a/d and $(r-a)/d$ must be odd and the other one must be even. In other words, we may always assume that a/d is odd, without loss of generality.

Theorem 5 *Let $q \geqslant 11$, $a \in \{1,\ldots,r-1\}$ $d = \gcd(a,r)$ and $n = r/d$. Further, let H_a denote the subgroup of $\mathrm{PG}(3,q)$ that leaves the conic C invariant and fixes the pair $\{Q_0, Q_{2a}\}$. If n and a/d are odd, then the elements of H_a are as follows :*

Element of H_a	*Image of* Π	*Image of* Π'	*Image of Z_k*	*Image of* $E(a;\epsilon_1,\ldots,\epsilon_{d-1})$
M_0' *(the identity)*	Π	Π'	Z_k	$E(a;\epsilon_1,\ldots,\epsilon_{d-1})$
M_r'	Π'	Π	$Z_{d+k} = Z_{-(d-k)}$	$E(a;-\epsilon_{d-1},\ldots,-\epsilon_1)$
M_a	Π'	Π	Z_{d-k}	$E(a;\epsilon_{d-1},\ldots,\epsilon_1)$
M_{a+r}	Π	Π'	Z_{-k}	$E(a;-\epsilon_1,\ldots,-\epsilon_{d-1})$

Proof : From (5) we easily derive that the identity and M_r' are the only transformations that will fix both Q_0 and Q_{2a}. Similarly, M_a and M_{a+r} are the only transformations that interchange Q_0 and Q_{2a}. (We need not consider the case $2a = r$ which would result in a larger subgroup, because then n would be even.)

The reflection M_a maps Z_k onto Z_{a-k}. Now, recall that half cycle indices are determined modulo $2d$. Because a/d is odd, we have $a = d \pmod{2d}$ and therefore $Z_{a-k} = Z_{d-k}$.

By Lemma 5 we know that the other endpoint of the path that starts in 0 is $a+r$. Hence

$$\Pi = \{0, -2a, -4a, \cdots, r+5a, r+3a, r+a\}$$

is mapped by M_a to

$$\{a, 3a, 5a, \cdots, r-4a, r-2a, r\} = \Pi'.$$

The action of M'_r on Π, Π' and Z_k is reasonably straightforward to compute and then the last line of the table can be obtained from the identity $M_{a+r} = M_a M'_r$. ∎

Corollary 6 *Let $q \geqslant 11$. Let H_S denote the subgroup of $\mathrm{PGL}(3,q)$ that leaves invariant the arc S with signature $E(a; \epsilon_1, \ldots, \epsilon_{d-1})$.*

If n and a/d are odd, and $d > 1$, then

- *$H_S = \{M'_0, M'_r\}$ if and only if $\epsilon_{d-1} = -\epsilon_1, \epsilon_{d-2} = -\epsilon_2, \ldots$ (d odd),*
- *$H_S = \{M'_0, M_a\}$ if and only if $\epsilon_{d-1} = \epsilon_1, \epsilon_{d-2} = \epsilon_1, \ldots$,*
- *$H_S = \{M'_0\}$ otherwise.*

Otherwise, if n and a are odd and $d = 1$, then $H_S = \{M'_0, M'_r, M_a, M_{a+r}\} = H_a$.

Lemma 6 *Let $E_q(a)$ denote the number of projectively inequivalent arcs S with a signature of the form $E(a; \epsilon_1, \ldots, \epsilon_{d-1})$, with $d = \gcd(a, (q+1)/2)$. Then*

$$E_q(a) = \begin{cases} 1, & \text{when } d = 1, \\ 2^{d-3} + 2^{\lfloor \frac{d-3}{2} \rfloor}, & \text{when } d > 1. \end{cases} \tag{6}$$

Proof : As in the proof of Lemma 3, we sum the values of $|H_S|/|H_a|$ for all possible signatures.

If $d = 1$, then there is clearly the one signature $E(a)$.

Otherwise, when $d > 1$, the number of signatures with $\epsilon_{d-1} = \epsilon_1, \epsilon_{d-2} = \epsilon_2, \ldots$ is equal to $2^{(d-1)/2}$ when d is odd, and to $2^{d/2}$ when d is even. Similarly the number of signatures with $\epsilon_{d-1} = -\epsilon_1, \epsilon_{d-2} = \epsilon_2, \ldots$ is equal to $2^{(d-1)/2}$ when d is odd, and is zero when d is even. The sum of these two values is equal to $2^{\lfloor (d+1)/2 \rfloor}$ for general d.

It follows that

$$E_q(a) = \frac{1}{2} 2^{\lfloor (d+1)/2 \rfloor} + \frac{1}{4}(2^{d-1} - 2^{\lfloor (d+1)/2 \rfloor}) = 2^{d-3} + 2^{\lfloor (d-3)/2 \rfloor}.$$

∎

And using an argument similar to that of Section 4, this yields

Theorem 6 *Let $q \geqslant 11$. The number E_q of projectively inequivalent arcs S in $\mathrm{PG}(2,q)$ of size $|S| = (q+7)/2$, with a conical subset $T = S \cap C$ of size $|T| = (q+3)/2$ such that the elements of $S \setminus T$ are external points of C, is given by*

$$\sum_d{}' \frac{1}{2} \phi\left(\frac{q+1}{2d}\right) E_q(d)$$

where the sum is restricted to all proper divisors d of $(q+1)/2$ such that $(q+1)/(2d)$ is odd, and where ϕ denotes Eulers totient function, and $E_q(d)$ is as given in Lemma 6.

5 Arcs of type M with excess two

Again, in many respects the arcs of type M are similar to those of type I and type E from the previous sections, and therefore again we will focus mainly on the differences.

An arc S of type M has a conical subset T of size $|T| = (q+1)/2$ and without loss of generality we may assume that the external supplementary point is Q_0 and the internal supplementary point is Q_{2a+1} for some $a \in \mathbf{Z}_r$. Every vertex of the graph $\Gamma = \Gamma(C, S \setminus C)$ has degree 2, except the two vertices $0, r$ that correspond to the tangent points of Q_0, which have degree 1. The graph is therefore the disjoint union of a path and zero or more cycles.

The vertices of the path or cycle that contains vertex i are the following :

$$\ldots, i, -i, 2a+1-i, -2a-1-i, 4a+2-i, -4a-2-i, \ldots$$

Note that every vertex in this path or cycle is equal to $\pm i \bmod 2a+1$, and using similar arguments as in the previous section, we may conclude

Lemma 7 *If S is an arc of type M with supplementary points Q_0 and Q_{2a+1}, then $\Gamma(C, S \setminus C)$ is the disjoint union of $h = (f-1)/2$ cycles of length $2m$ and one path of m vertices, where m is the order of $2a+1 \pmod{q+1}$ and $f = (q+1)/m$, i.e., $f = \gcd(2a+1, q+1)$.*

Note that in particular f must be odd and m must be even.

It also follows that $N(T)$ is a union of half cycles $Z'_k \stackrel{\text{def}}{=} k + (2a+1)\mathbf{Z}_{q+1} = k + f\mathbf{Z}_{q+1}$ and one *half path*, i.e., an independent set of size $m/2$ in the path that joins 0 and r.

There are exactly $m/2+1$ half paths, which we will denote by Π_k with $k = 0, \ldots, m/2$. We have

$$\Pi_k \stackrel{\text{def}}{=} \{0, -2a-1, -2(2a+1), \ldots, -(k-1)(2a+1)\} \cup \{(k+1)(2a+1), \ldots, r\},$$

with special cases

$$\begin{aligned} \Pi_0 &= \{2a+1, 2(2a+1), \ldots, r\}, \\ \Pi_{m/2} &= \{0, -2a-1, -2(2a+1), \ldots, (2a+1)+r\}. \end{aligned}$$

We find

Theorem 7 *Let $a \in \{0, \ldots, r-1\}$. Let $f = \gcd(2a+1, q+1)$, $m = (q+1)/f$, $h = (f-1)/2$. Let $S = T \cup \{Q_0, Q_{2a+1}\}$, with $T \subset C$ and $|T| = (q+1)/2$. Then S is an arc of $\mathrm{PG}(2,q)$ if and only if $N(T)$ can be written as a disjoint union of the form*

$$N(T) = \Pi_k \cup Z'_{\pm 1} \cup \ldots \cup Z'_{\pm h},$$

with independent choices of sign, and $k \in \{0, \ldots, m/2\}$.

We shall identify these arcs by their signature $M(a; k; \epsilon_1, \ldots, \epsilon_h)$, where $\epsilon_k = \pm 1$ depends on the choice made for the half cycle $Z'_{\pm k}$.

As before, we shall now determine what isomorphisms exist between arcs of this type. Among the elements of G that fix Q_0 the reflections M_0 and M_r interchange Q_{2a+1} and Q_{-2a-1} and hence for every arc with a signature of the form $M(a;k;\epsilon_1,\ldots,\epsilon_h)$ there is an equivalent arc with a signature of the form $M(r-a-1;k;\epsilon_1,\ldots,\epsilon_h)$. In what follows we may therefore restrict ourselves to $a \in \{0,1,\ldots,\lfloor (r-1)/2 \rfloor\}$.

Theorem 8 *Let $q \geqslant 13$, let $a \in \{0,\ldots,r-1\}$, let $f = \gcd(2a+1, q+1)$ and $m = (q+1)/f$. Further, let H_a denote the subgroup of $\mathrm{PG}(3,q)$ that leaves the conic C invariant and fixes the pair $\{Q_0, Q_{2a+1}\}$. If m is even, then the elements of H_a are as follows :*

1. *When $m \neq 2$*

Element of H_a	*Image of Π_k*	*Image of Z'_k*	*Image of $M(a;k;\epsilon_1,\ldots,\epsilon_h)$*
M'_0 *(the identity)*	Π_k	Z'_k	$M(a;k;\epsilon_1,\ldots,\epsilon_h)$
M'_r	$\Pi_{m/2-k}$	Z'_k	$M(a;m/2-k;\epsilon_1,\ldots,\epsilon_h)$

2. *When $m = 2$*

Element of H_a	*Image of Π_k*	*Image of Z'_k*	*Image of $M(a;k;\epsilon_1,\ldots,\epsilon_h)$*
M'_0 *(the identity)*	Π_k	Z'_k	$M(a;k;\epsilon_1,\ldots,\epsilon_h)$
M'_r	Π_{1-k}	Z'_k	$M(a;1-k;\epsilon_1,\ldots,\epsilon_h)$
M_0	Π_k	Z'_{-k}	$M(a;k;-\epsilon_1,\ldots,-\epsilon_h)$
M_r	Π_{1-k}	Z'_{-k}	$M(a;1-k;-\epsilon_1,\ldots,-\epsilon_h)$

Proof : Note that the case $m = 2$ is equivalent to $2a+1 = r = f$. Also note that in general $r = (m/2)f$ and hence $Z'_{k+r} = Z'_k$

Since Q_0 is an external point of C, and Q_{2a+1} is an internal point, there are no elements of H_a that interchange Q_0 and Q_{2a+1}. The elements of G that fix Q_0 are M'_0, M'_r, M_0 and M_r. The first two always fix Q_{2a+1}, the latter only if $2a+1 = r$.

The rotation M'_r maps Π_k onto the set

$$\begin{aligned} &\{r, r-2a-1, r-2(2a+1), \ldots, r-(k-1)(2a+1)\} \cup \{r+(k+1)(2a+1), \ldots, 0\} \\ &= \{0, \ldots, -(m/2-k-1)(2a+1)\} \cup \{(m/2-k+1)(2a+1), \ldots, r\} \end{aligned}$$

and this is the half path $\Pi_{m/2-k}$. When $m = 2$ the half paths are the singletons $\Pi_0 = \{r\}$ and $\Pi_1 = \{0\}$. These are left invariant by M_0 and interchanged by M_r. ∎

Although this theorem is valid for all $a \in \{0,\ldots,r-1\}$, we only need it when $0 \leqslant a \leqslant \lfloor (r-1)/2 \rfloor$, as explained earlier.

Corollary 7 *Let $q \geqslant 13$. Let H_S denote the subgroup of $\mathrm{PGL}(3,q)$ that leaves invariant the arc S with signature $M(a;k;\epsilon_1,\ldots,\epsilon_h)$. If m is even and $m \neq 2$, then*

- *$H_S = \{M'_0, M'_r\}$ if and only if $k = m/4$*

- $H_S = \{M_0'\}$ *otherwise.*

Lemma 8 *Let $M_q(a)$ denote the number of projectively inequivalent arcs S with a signature of the form $M(a;k;\epsilon_1,\ldots,\epsilon_h)$, where $2h+1 = \gcd(2a+1, q+1)$. Then*

$$M_q(a) = \begin{cases} 2^{h-1}, & \text{when } h = (q-1)/4, \\ (\lfloor \frac{q+1}{2(2h+1)} \rfloor + 1)2^h, & \text{when } h < (q-1)/4, \end{cases} \tag{7}$$

Proof : For a given k there are 2^h arcs of the requested signature. There are $m/2+1$ possible values of k.

When $m/2$ is odd, we therefore have $M_q(a) = \frac{1}{2}(m/2+1)2^h$. When $m/2$ is even, $m \neq 2$, we have $M_q(a) = 2^h + \frac{1}{2}(m/2)2^h = \frac{1}{2}(m/2+2)2^h$. In both cases this can be written as $(\lfloor m/4 \rfloor + 1)2^h$.

When $m = 2$ we have $M_q(a) = \frac{1}{4}(m/2+1)2^h = 2^{h-1}$. ∎

Theorem 9 *Let $q \geqslant 13$. The number M_q of projectively inequivalent arcs S in $\mathrm{PG}(2,q)$ of size $|S| = (q+5)/2$, with a conical subset $T = S \cap C$ of size $|T| = (q+1)/2$ such that $S \setminus T$ consists of an internal and an external point of C, is given by*

$$\sum_h{}' \lceil \frac{1}{2}\phi\left(\frac{q+1}{2h+1}\right) \rceil M_q(h)$$

where the sum is restricted to all proper odd divisors $2h+1$ of $q+1$ such that $(q+1)/(2h+1)$ is even, and where ϕ denotes Eulers totient function, and $M_q(h)$ is as in Lemma 8.

Proof : Note that the value of $M_q(a)$ only depends on h. Hence for all a such that $\gcd(2a+1, q+1) = 2h+1 = f$ we have the same value. There are exactly $\phi((q+1)/f)$ such values of $2a+1$ in the range $1,\ldots,q$. But of these values we only need to consider half, except in the case $f = r$ in which all of them need to be considered. ∎

6 Arcs of type I with excess 3 or 4

In this section we shall prove that an arc of type I cannot have an excess larger than 4 and we shall explicitely describe the arcs that reach this bound. The techniques we use are related to those of Korchmáros and Sonnino [3] who prove a similar result for arcs of type E (but with restrictions on the values of q).

Note that an arc of type I with excess 4 does not need to be complete. It is theoretically possible that further points can be added that are external to the conic C. However, an exhaustive computer search for values up to $q = 503$ did not produce such an example.

Consider an arc S of type I with conical subset $T = C \cap S$ as before. We shall use the following criterion to determine whether S is an arc.

Lemma 9 *Let T be a subset of a conic C of size $|T| = (q+1)/2$. Let U be a set of internal points of C. Then $S = T \cup U$ is an arc if and only if*

- *no three points of U are collinear.*
- *every line joining two points of U is an external line of C,*
- *$\sigma_Q(T) = C \setminus T$ for all points Q of U,*

with σ_Q as defined in Section 2.

Proof : We divide the triples of points of S into the following four categories :

1. Triples of points of U. The first hypothesis of this lemma is satisfied if and only if no such triple is collinear.

2. Triples of points of T. These can never be collinear, as T lies on a conic.

3. Triples consisting of two points $Q, Q' \in U$ and one point of T. Clearly, if QQ' is an external line it does not intersect C and hence this triple cannot be collinear. Conversely, as was already explained in the introduction, if QQ' is a secant line, at least one of its points must belong to T, yielding a collinear triple of this type. (QQ' can not be a tangent to C, because Q, Q' are internal.)

4. Triples consisting of one point $Q \in U$ and two points $P, P' \in T$. By definition of σ_Q, P, P', Q are collinear if and only if $\sigma(P) = P'$. As a consequence, no collinear triple of this type exists if and only if $\sigma_Q(T)$ and T are disjoint, for all $Q \in U$. Since T contains exactly half of the points of C, this is equivalent to the third hypothesis of this lemma. ∎

We use this lemma to show that there are plenty of arcs of type I with excess 3.

Theorem 10 *Let $a \in \{1, \ldots, r-1\}$. Let $d = \gcd(a, r)$, $n = r/d$. Consider the arc S with signature $I(a; \epsilon_1, \ldots, \epsilon_d)$. Let R be the pole of ℓ, i.e., the internal point with coordinates $(-\beta : 0 : 1)$.*

Then $S \cup \{R\}$ is an arc if and only if $4|q+1$, n is odd and $\epsilon_1 = \epsilon_d$, $\epsilon_2 = \epsilon_{d-1}$, ...

Proof : The conical subset T of S is the set

$$T = Z_1^{\epsilon_1} \cup \cdots \cup Z_d^{\epsilon_d},$$

and then

$$C \setminus T = Z_1^{-\epsilon_1} \cup \cdots \cup Z_d^{-\epsilon_d}.$$

By Theorem 2 it follows that $\sigma_R(T) = M'_r(T) = C \setminus T$ if and only if n is odd and $\epsilon_1 = \epsilon_d$, $\epsilon_2 = \epsilon_{d-1}$, ...

The polar line of Q_{2a+1} intersects ℓ in Q_{2a+1+r}. This is an internal point if and only if r is even, and hence RQ_{2a+1} is an external line if and only if r is even. Similarly, also RQ_1 is an external line if and only if r is even.

From Lemma 9 the claim follows. ∎

Define $\hat{\Delta}_T$ to be the group of all projective transformations that either fix both sets T and $C \setminus T$, or interchange them. $\hat{\Delta}_T$ fixes the conic C and hence is a subgroup of $\mathrm{PGL}(2, q)$. Define Δ_T to be the subgroup of $\hat{\Delta}_T$ that fixes T (and hence also $C \setminus T$).

The group $\hat{\Delta}_T$ is never trivial. Indeed, for every supplementary point Q the involution σ_Q interchanges T and $C \setminus T$ and hence belongs to $\hat{\Delta}_T$. It also follows that Δ_T is a proper subgroup of $\hat{\Delta}_T$, of index 2.

Lemma 10 *Δ_T does not contain any element of order p (where p is the characteristic of the field).*

Proof : Suppose $\rho \in \Delta_T$ has order p. Then orbits of ρ on C have size p or 1. T must be a union of orbits of ρ and since $|T| = (q+1)/2 = 1/2 \pmod p$, ρ must have at least $(p+1)/2$ fixed points in T, and similarly, in $C \setminus T$. Hence ρ must have at least $p+1$ fixed points on C. Hence $\rho = 1$ since the identity is the only element of $\mathrm{PGL}(2,q)$ that fixes more than two points. ∎

To obtain a list of candidates for $\hat{\Delta}_T$ we may use the classification of subgroups of $\mathrm{PGL}(2,q)$, as given in [1, Theorem 2] for example. The subgroups of $\mathrm{PGL}(2,q)$ that satisfy Lemma 10 are isomorphic to one of the following :

1. A cyclic group C_d where d divides $q-1$ or $q+1$,
2. A dihedral group D_{2d} where d divides $q-1$ or $q+1$,
3. The alternating group A_4,
4. The symmetric group S_4,
5. The alternating group A_5.

The alternating groups can be ruled out immediately as candidates for $\hat{\Delta}_T$, because they have no subgroups of index 2.

The first two cases are dealt with in the following lemmas.

Lemma 11 *If $\hat{\Delta}_T$ is cyclic, then the excess of S can be at most 1.*

Proof : A cyclic group contains at most one element of order 2, hence $\hat{\Delta}_T$ contains at most one element that may function as σ_Q with Q an internal point of C. (Note that σ_Q determines Q uniquely.) ∎

Lemma 12 *If $\hat{\Delta}_T$ is a dihedral group, then the excess of S can be at most 3. In case of equality S is as described in Theorem 10*

Proof : A dihedral group can be generated by two of its involutions. These two involutions can always be written as σ_Q, $\sigma_{Q'}$ with $Q, Q' \notin C$, $Q \neq Q'$. Both involutions fix the line QQ' and hence $\hat{\Delta}_T$ also fixes this line. Every other involution of $\hat{\Delta}_T$ must therefore be of the form σ_R where either R is the pole of QQ' or else lies on the line QQ'.

Because QQ' can contain at most two supplementary points of S, the excess of S cannot be larger than three and in that case the pole of QQ' must be one of the supplementary points. ∎

This leaves only the case where $\hat{\Delta}_T$ is isomorphic to S_4 (and then Δ_T is isomorphic to A_4). All instances of the subgroup S_4 of $\mathrm{PGL}(2,q)$ are conjugate, so without loss of generality we may choose a fixed representation.

For the remainder of this section we choose $X^2+Y^2+Z^2=0$ as the equation of C and S_4 the subgroup of all transformations of the form $(x:y:z)\mapsto(\pm x:\pm y:\pm z)$ optionally combined with any permutation of the coordinates. (Obviously, this group leaves the value of $X^2+Y^2+Z^2$ invariant and hence fixes C.) The subgroup A_4 then corresponds to a combination of one or more sign changes and an *even* permutation of the coordinates.

The set $S_4 \setminus A_4$ contains exactly six involutions, hence there are six candidates for σ_Q and hence at most six supplementary points Q. These involutions consist of a single transposition of two coordinates, optionally combined with a sign change of the third coordinate. (For example, $(x:y:z)\mapsto(y:x:-z)$.) The corresponding points Q have coordinates of the form $(\pm1:\pm1:0)$, $(0:\pm1:\pm1)$ or $(\pm1:0:\pm1)$. (Note that changing the sign of both non-zero coordinates does not change the point itself.)

There are seven lines that contain at least two of these candidate points. Each of the four lines with an equation of the form $Z=\pm X\pm Y$ contains three of these points:

$Z=X-Y$	$Z=Y-X$	$Z=X+Y$	$Z=-X-Y$
$(1:1:0)$	$(1:1:0)$	$(1:0:1)$	$(1:-1:0)$
$(0:-1:1)$	$(-1:0:1)$	$(-1:1:0)$	$(0:1:-1)$
$(1:0:1)$	$(0:1:1)$	$(0:1:1)$	$(1:0:-1)$

The other three lines have equations $X=0, Y=0, Z=0$ and each contain two candidate points.

It is easily seen that the largest subset of candidate points such that no three are collinear has size 4. Without loss of generality we may choose this set to be $U=\{Q,Q',Q'',Q'''\}$, with

$$\begin{array}{rclrcl} Q &=& (1:-1:0), & \sigma_Q(x:y:z) &=& (y:x:z) \\ Q' &=& (1:1:0), & \sigma_{Q'}(x:y:z) &=& (y:x:-z) \\ Q'' &=& (1:0:-1), & \sigma_{Q''}(x:y:z) &=& (z:y:x) \\ Q''' &=& (1:0:1), & \sigma_{Q'''}(x:y:z) &=& (z:-y:x) \end{array} \tag{8}$$

Note that three of these involutions already generate the whole group S_4.

In view of Lemma 9 we will investigate the conditions for a candidate point to be an internal point of C, and for a line joining two candidate points to be external to C.

Lemma 13 *Consider the plane* $\mathrm{PG}(2,q)$ *with q odd. A point with coordinates of the form* $(\pm1:\pm1:0)$, $(0:\pm1:\pm1)$ *or* $(\pm1:0:\pm1)$ *is an internal point of the conic C with equation $X^2+Y^2+Z^2=0$ if and only if $q=5$ or $7 \pmod 8$. The line with equation $X=0$ (and similarly $Y=0$ or $Z=0$) is an external line of C if and only if $q=3 \pmod 4$. A line with an equation of the form $Z=\pm X\pm Y$ is an external line of C if and only if $q=5 \pmod 6$.*

Proof : Consider the point Q with coordinates $(1,\pm1,0)$. (The other cases will be left to the reader.) The polar line of this point has equation $X\pm Y=0$, i.e., $Y=\mp X$. The

intersection points of this line with the conic satisfy $2X^2 + Z^2 = 0$. Hence there will be two intersections or zero, according to whether -2 is a square in GF(q), or not.

The intersection of $X = 0$ with the conic yields $Y^2 + Z^2 = 0$ and has solutions if and only if -1 is a square in GF(q). The intersection of $Z = \pm X \pm Y$ with the conic yields $X^2 + Y^2 + (X \pm Y)^2 = 0$, and hence $X^2 \pm XY + Y^2 = 0$, which has solutions if and only if -3 is a square in GF(q).

When p is a prime, -2 is a square modulo p if and only if $p = 1$ or $3 \pmod 8$. When $q = p^h$ with h even, every element of the prime field is a square, but then also $q = 1 \pmod 8$. When h is odd, -2 is a square in GF(q) if and only if it is a square modulo p, but in that case also $q = p \pmod 8$.

Similarly, -1 is a square if and only if $q = 1 \pmod 4$ and -3 is a square if and only if $q = 1 \pmod 6$. ∎

Lemma 14 *Let $q = -1 \pmod{24}$. Then S_4 acts semiregularly on C (i.e., every orbit has size 24).*

Proof : To prove semiregularity we shall prove that no element of S_4 stabilizes a point of C. For this it is sufficient to prove this for one element g of each conjugacy class of S_4. We have the following cases:

1. g is an involution of $S_4 \setminus A_4$. Then $g = \sigma_Q$ for one of the 'candidate points' Q discussed above. By Lemma 13 Q must be an internal point and then σ_Q cannot have fixed points on C.

2. g is an involution of A_4. Without loss of generality we may take g to be the map $(x : y : z) \mapsto (x : y : -z)$. A fixed point of g therefore either has $x = y = 0$ or $z = 0$. A fixed point that belongs to C must therefore satisfy $x^2 + y^2 = 0$, which is not possible, as -1 is not a square in GF(q).

3. g has order 3. Take $g(x : y : z) = (y : z : x)$. A fixed point of g must satisfy

$$\begin{vmatrix} x & y \\ y & z \end{vmatrix} = \begin{vmatrix} y & z \\ z & x \end{vmatrix} = \begin{vmatrix} z & x \\ x & y \end{vmatrix} = 0.$$

Together with $x^2 + y^2 + z^2 = 0$, this yields $x^2 + xy + y^2 = 0$ and this has no solution because -3 is not a square in GF(q).

4. g has order 4. If g fixes a point, then so does g^2, an involution that was already treated before. ∎

Combining the various lemmas in this section we obtain the following result.

Lemma 15 *Let $q = -1 \pmod{24}$. Let $d = (q+1)/24$. Let $O_1, \ldots, O_d$ denote the orbits of S_4 on C. For $i = 1, \ldots, d$ write $O_i = O_i^+ \cup O_i^-$, where $O_i^\pm$ are orbits of A_4 on C.*

Then

$$S \stackrel{\text{def}}{=} O_1^\pm \cup \cdots \cup O_d^\pm \cup \{Q, Q', Q'', Q'''\}, \tag{9}$$

for any choices of signs, is an arc of type I and excess 4 (with Q, Q', Q'', Q''' as defined in (8)).

The information we obtained so far is sufficient to state the following result.

Theorem 11 *An arc in* $\mathrm{PG}(2,q)$ *of type I can have at most excess 4. If the excess is 4 then* $q = -1 \pmod{24}$ *and the arc is as described in Lemma 15.*

Theorem 12 *Let* $q = -1 \pmod{24}$. *Let* $d = (q+1)/24$. *The number of projectively inequivalent arcs in* $\mathrm{PG}(2,q)$ *of type I with excess* 4 *is* 2^{d-1}. *The automorphism group of each arc is of type* 2^2.

Proof : By Lemma 15 all arcs of this type are equivalent to one of the form (9), with d choices of sign. Hence, there are 2^d arcs of this form. We shall prove that each arc S of this form is isomorphic to exactly one other arc S^- of this form, and hence that the number of inequivalent arcs is 2^{d-1}.

We first determine the automorphism group of S. Any automorphism of S must fix the conic C and the set $U = \{Q, Q', Q'', Q'''\}$. The stabilizer of U in $\mathrm{PGL}(3,q)$ is a symmetric group of degree 4, acting on U by permuting the 4 points. (This group is not to be confused with the group $S_4 = \hat{\Delta}_T$.) Of these 24 permutations, only the following also leave C invariant:

$$\begin{array}{lrcl}
\text{the identity} & (x:y:z) & \mapsto & (x:y:z) \\
(Q\ Q')(Q''\ Q''') & (x:y:z) & \mapsto & (x:-y:-z) \\
(Q\ Q'')(Q'\ Q''') & (x:y:z) & \mapsto & (x:z:y) \\
(Q\ Q''')(Q'\ Q'') & (x:y:z) & \mapsto & (x:-z:-y) \\
 & & & \\
(Q\ Q') & (x:y:z) & \mapsto & (x:-y:z) \\
(Q''\ Q''') & (x:y:z) & \mapsto & (x:y:-z) \\
(Q\ Q'''\ Q'\ Q'') & (x:y:z) & \mapsto & (x:z:-y) \\
(Q\ Q''\ Q'\ Q''') & (x:y:z) & \mapsto & (x:-z:y)
\end{array}$$

They form a subgroup of type D_8 of S_4 (the dihedral group of order 8). Also $D_4 = D_8 \cap A_4$ is isomorphic to the Klein group 2^2 (consisting of the first four elements listed above).

Now, any element of $S_4 \setminus A_4$ (and therefore also any element of $D_8 \setminus D_4$) interchanges the orbits O_i^+ and O_i^-, for all i, and hence maps S to the arc $S^- = (C \setminus T) \cup U$ in which each orbit $O_i^\pm$ is replaced by the orbit $O_i^\mp$. On the other hand, any element of A_4 (and therefore any element of D_4) leaves every $O_i^\pm$ invariant and hence fixes S. It follows that the automorphism group of S is D_4, and that S^- is the only other arc of the same form that is equivalent to S. ∎

7 Computer results

As was already mentioned in the introduction, one of our motivations for the theoretical treatment of the previous sections is to provide a basic setting for a computer program to search for arcs with excess larger than two: we use the theorems of the previous sections to quickly generate all large arcs with excess two up to equivalence, and then use an exhaustive search to try to extend each of these arcs with further supplementary points.

In Tables 4 and 5 we list the numbers of inequivalent arcs of types I, E and M with excess two, for field orders smaller than 256. In these tables N_a denotes the number of *all* inequivalent arcs with excess two, as computed from the formulae in Theorems 3, 6 and 9, while N_i denotes the number of (inequivalent) *incomplete* arcs with excess two, as found by computer.

By Corollaries 1 and 5, we do not list values for q smaller than 13 (for type I and M) or 11 (for type E). Note that some of the numbers N_a are already quite large, even for reasonably small values of q. As our program for finding arcs with larger excess needs to investigate each arc of excess 2 separately, this puts a limit on the values of q for which we could still find results in a reasonable time. If for this reason no further results could be obtained we have left the N_i-column blank for the corresponding value of q.

In Table 1 we list the number of inequivalent *complete* arcs of excess at least 3 that can be obtained by extending an arc of type E of excess two. These arcs are necessarily of type E themselves, because in this case the conic section is too large to allow supplementary points that are internal. Our results agree with those of [4], and although we managed to investigate larger values of q, we did not find any new examples.

In Table 2 we list the number of inequivalent complete arcs of excess larger than two that are extensions of an arc of excess two of type I. The first two columns are the arcs of type I that were discussed in Section 6. The arcs in the last two columns are of type M.

Finally in Table 3 we list the arcs of excess at least three that can be obtained from an arc of type M of excess two (and hence are themselves of type M too). The second and third columns are copies of the last two columns of Table 2, as obviously (containing two internal points) these arcs can also be constructed from an arc of type I and excess two.

q	3 external pts	4 external pts
13		1
17		1
19	1	
27	3	
43	1	
59	1	

Table 1: Number of inequivalent complete arcs of type E in $\mathrm{PG}(2, q)$ of excess at least three.

q	3 internal pts,	4 internal pts,	2 internal pts, 1 external pt	2 internal pts, 2 external pts
13			1	
19	2			
23	3	1		1
27	3			
43	5			
47	10	2		
59	28			
67	8			
71	42	4		
79	16			
83	82			
103	12			
107	277			
131	1052			
139	261			

Table 2: Number of inequivalent complete arcs in $\mathrm{PG}(2,q)$ that can be obtained by extending a large arc of type I and excess 2 with at least one point.

References

[1] P.J. Cameron, G.R. Omidi, B. Tayfeh-Rezaie, *3-Designs from* $\mathrm{PGL}(2,q)$, Electron. J. Combin. **13** (2006), #R50.

[2] A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *On sizes of complete caps in projective spaces* $\mathrm{PG}(n,q)$ *and arcs in planes* $\mathrm{PG}(2,q)$, J. Geom. **94** (2009), pp. 31-58

[3] G. Korchmáros and A. Sonnino, *Complete arcs arising from conics*, Discrete Math. **267** (2003), pp. 181–187

[4] G. Korchmáros and A. Sonnino, *On arcs sharing the maximum number of points with ovals in cyclic affine planes of odd order*, J. Combin. Des. **18** (2010), pp. 25-47

[5] G. Pellegrino, *Sur les k-arcs complets des plans de Galois d'ordre impair*, Ann. Discrete Math. **18** (1983), pp. 667–694

[6] G. Pellegrino, *Archi completi, contenenti* $(q+1)/2$ *punti di una conica, nei piani di Galois di ordine dispari*, Rend. Circ. Mat. Palermo (2) **62** (1993), pp. 273–308.

q	1 internal pt, 2 external pts	2 internal pts, 1 external pt	2 internal pts, 2 external pts	1 internal pt, 3 external pt	1 internal pt, 7 external pts
13	6	1			
17	11			1	
19	5			1	
23			1		
25	10				
27					1
29	9				
31	1				
37	10				
41	13				
49	14				
53	20				
61	15				
73	18				
81	20				
89	102				
97	33				
101	152				
109	62				
113	283				
121	23				
125	1115				

Table 3: Number of inequivalent complete arcs of type M in $\mathrm{PG}(2, q)$ of excess at least three.

q	type I		type E		type M	
	N_a	N_i	N_a	N_i	N_a	N_i
11			1	0		
13	3	1	3	1	16	7
17	6	0	5	2	27	14
19	18	3	2	1	32	11
23	39	7	3	0	40	1
25	6	0	6	0	74	10
27	48	4	3	3	64	1
29	20	0	14	0	116	14
31	96	0	0	0	72	1
37	9	0	9	0	346	10
41	51	0	32	0	618	20
43	548	6	5	1	184	0
47	1200	20	36	0	144	0
49	30	0	22	0	2202	18
53	154	0	87	0	4284	31
59	8616	47	160	2	464	0
61	15	0	15	0	16624	15
67	32928	9	8	0	800	0
71	67207	78	537	0	380	0
73	18	0	18	0	131414	18
79	263416	24	72	0	416	0
81	20	0	20	0	524708	20
83	529134	149	2116	0	2472	0
89	8582	0	4342	0	2097904	192
97	129	0	81	0	8389229	45
101	32936	0	16544	0	16778288	288
103	16785550	14	18	0	1032	0
107	33624706	533	32935	0	17136	0
109	1126	0	594	0	67109736	104
113	131373	0	65828	0	134219454	548
121	30	0	30	0	536871842	23
125	525352	0	262962	0	1073744892	1115
127	1073807856	0	0	0	1056	0

Table 4: Number of inequivalent large arcs of types I, E and M in $\mathrm{PG}(2, q)$, $q \leqslant 127$.

q	type I		type E		type M	
	N_a	N_i	N_a	N_i	N_a	N_i
131	2148567242	1043	524860	0	132248	0
137	2098231	0	1049644	0	8589939722	
139	8590009516	81	4580	0	263392	0
149	8407258	0	4204736	0	68719486844	
151	68720001653		27	0	4476	0
157	39	0	39	0	274877908504	
163	549756338256		20	0	2098832	0
167	1099580854798		33560130	0	7760	0
169	65904	0	33104	0	2199023258752	
173	134225990	0	67117112	0	4398046545524	
179	8796363720868		134292172	0	8391616	0
181	6492	0	3324	0	17592186047176	
191	70369834769136		536887296	0	2112	0
193	48	0	48	0	140737488357680	
197	2147518740	0	1073775818	0	281474976844528	
199	281475010795762		262686	0	26968	0
211	2251799847239784		26	0	134220536	0
223	18014398777992520		24768	0	3312	0
227	36028865873183538		34359869548		536877816	0
229	4196506	0	2099310	0	72057594037943304	
233	137439222744		68719742540		144115188076908684	
239	288230652112857584		137443412112		5600	0
241	2695	0	1415	0	576460752303427803	
243	576460752840294520		30	0	2147487368	0
251	2305844109801372844		549756443182		4294979568	0

Table 5: Number of inequivalent large arcs of types I, E and M in PG$(2, q)$, $127 < q < 256$.