Classification of Arcs in Small Desarguesian Projective Planes

Classificatie van Bogen in Kleine Desarguesiaanse Projectieve Vlakken

Heide Sticker

Proefschrift ingediend tot het behalen van de graad van
Doctor in de Wetenschappen: Wiskunde

Promotor:
Prof. dr. dr. Kris Coolsaet

June 2012

Faculteit Wetenschappen
Vakgroep Toegepaste Wiskunde en Informatica

Contents

1

Introduction

The main topic of this text is the determination of all complete $(k,2)$- and $(k,3)$-arcs in Desarguesian projective planes $\mathrm{PG}(2,q)$ up to equivalence.

Many attempts have been made to determine all complete $(k,2)$-arcs in $\mathrm{PG}(2,q)$ up to equivalence. For all but the smallest q this is infeasible without the use of a computer. Full classifications for $q \leq 23$ have been known for some time [15, 26]. In [10] and [12], we presented a full classification of the complete $(k,2)$-arcs in $\mathrm{PG}(2,23)$ and $\mathrm{PG}(2,25)$, resp. $\mathrm{PG}(2,27)$ and $\mathrm{PG}(2,29)$. As far as we know, we are the first to obtain a full classification in the cases, $q = 25$, 27 and 29. The spectra for $q = 25$ and $q = 27$, i.e. the values of k for which a complete arc exists, have been computed before by Marcugini et al. [34, 31]. They also found that in $\mathrm{PG}(2,29)$ no arc of size $k < 13$ exists. Chao and Kaneta found that the size $m'(2,q)$ of the second largest complete arcs in $\mathrm{PG}(2,q)$ is 21 for $q = 25$, 22 for $q = 27$ and 24 for $q = 29$ [7]. They also proved that no

arc of size $m'(2,q)-1$ exists for $q = 25$, 27 and 29. G. Kéri [26] has obtained a classification of all arcs of size $k \geq q-8$ for values of q up to 32, in the context of MDS codes. Our results agree with the partial results of [26].

People have also been working on determining all inequivalent complete $(k,3)$-arcs. For $q \leq 9$, the classification was already done by Marcugini et al. [30, 32]. They also found that the largest size of a complete arc is 21 in $\mathrm{PG}(2,11)$ and 23 in $\mathrm{PG}(2,13)$ and that the smallest size of a complete arc in $\mathrm{PG}(2,13)$ is 15 [29, 33]. For $q = 13$ they found the spectrum: there is a complete $(k,3)$-arc for each k, $15 \leq k \leq 23$ [33]. We extended this to a full classification of all complete $(k,3)$-arcs in $\mathrm{PG}(2,11)$ and $\mathrm{PG}(2,13)$ [13]. Our programs reproduce the results of Marcugini et al. More information on lower and upper bounds on the maximum size of (k,n)-arcs can be found in [2, 20].

Our methods can also be used to classify the full set of $(k,2)$-arcs and $(k,3)$-arcs, i.e., not necessarily only those that are complete, and in that case we think we are the first to obtain a full classification of the $(k,2)$-arcs for $q = 23, 25, 27, 29$. For $q = 11, 13$, we were the first to obtain a full classification of all inequivalent $(k,2)$- and $(k,3)$-arcs.

In Chapter 4, we present the algorithms that we used to find the complete $(k,2)$- and $(k,3)$-arcs in the projective plane $\mathrm{PG}(2,q)$. The algorithms are an application of isomorph-free generation using canonical augmentation, as introduced by B. Mckay [35]. We adapted this general technique to the particular case of generating arcs in projective planes.

The results of the algorithms are presented in Chapters 5, 6 and 7. In Chapter 5, the inequivalent complete arcs are listed according to the size of the arc and the type of its automorphism group. We have also enumerated the arcs that are not necessarily complete. For $(k,2)$-arcs, we also listed the arcs according to their size and to the type of algebraic curve into which they can be embedded. For $(k,3)$-arcs, we have also singled out the arcs that are *regular* in the sense that every point of the arc lies on the same number of trisecants to that arc.

We found some general constructions of arcs that also work for larger fields. The general constructions are described in Sections 6.1, 6.2 and 6.3 for $(k,2)$-

arcs, and in Sections 7.1, 7.2 and 7.3 for $(k,3)$-arcs. In the remaining part of Chapters 6 and 7, for each q we present the arcs corresponding to the general constructions and we give a geometric description of some arcs that have a large stabilizer group.

In the hope of finding a faster algorithm to tackle the case $q = 31$ for $(k,2)$-arcs, we developed a second algorithm which generates $(k,2)$-arcs starting from subsets of a conic. This algorithm is explained in Chapter 8. An implementation of this algorithm reproduces our previous results for $q \leq 25$. Unfortunately, it proved too slow for $q > 25$.

We have also worked on $(k,2)$-arcs having a large intersection with a conic (i.e., a large conical subset)[11]. An arc can intersect a conic in at most $(q+3)/2$ points when all points not on the conic are external to the conic. For arcs containing at least one internal point, the maximum size of a conical subset is $(q+1)/2$. In Chapter 3, we discuss the arcs with a conical subset of maximum size and 1 extra point (Section 3.7) and we give an explicit complete classification, up to PGL-equivalence, for the cases of 2 internal points, 2 external points and the combination of 1 internal and 1 external point (Section 3.3- 3.5). For the classification, we use the properties of the cyclic group of all norm 1 elements of the field $\mathbb{F}_{q^2}$. This has the advantage that the classification can be formulated without the use of groups, making it very straightforward (and efficient) to use in subsequent computer searches. We list the results of these searches in Section 3.8. In Section 3.6, we prove that for an arc with maximum size $(q+1)/2$ the number of points internal to $\mathcal{C}$ can be at most 4, and we give a complete classification of all arcs that attain this bound.

The subject of arcs is not only interesting in its purely geometrical setting. Arcs have applications in coding theory, where they can be interpreted as linear maximum distance separable codes (MDS codes). For instance, a linear $[k,d,k-d]_q$ code C such that its dual code $C^\perp$ has minimum distance equal to d is called NMDS. Every $[k,3,k-3]_q$ NMDS code is equivalent to a $(k,3)$-arc in $\mathrm{PG}(2,q)$ containing at least three collinear points. A $(k,3)$-arc is also the complement of a t-fold blocking set with $t = q-2$. $(k,2)$-arcs are related to superregular matrices (i.e., matrices with entries in $\mathbb{F}(q)$ where every minor is non-zero), to linearly independent sets of vectors in vector spaces over $\mathbb{F}_q$ and to optimal covering arrays.

2

Preliminaries

The primary purpose of this chapter is to establish some notations. Most of the properties described here belong to 'mathematical folklore' and shall be given without proof.

2.1 Finite Field

Let $\mathbb{F}_q$ denote the field of q elements. ($\mathbb{F}_q$ is also called the *Galois Field* of order q, notation $\mathbb{F}_q = \mathrm{GF}(q)$.) Note that q must always be an integral power p^h of a prime p. p is called the *characteristic* of the finite field. When q is prime, we can write $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$. When $q = p^h, h > 1$, we have $\mathbb{F}_q = \{0, 1, \alpha, \ldots, \alpha^{q-2}\}$ where α is the root of a primitive polynomial of degree h over $\mathbb{F}_p$. In Table 2.1, we present the primitive polynomials that will be used for the fields of order

a prime power in the rest of this text.

q	irreducible polynomial
8	$\alpha^3 + \alpha^2 + \alpha + 1 = 0$
9	$\alpha^2 + \alpha - 1 = 0$
16	$\alpha^4 + \alpha^3 + 1 = 0$
25	$\alpha^2 + \alpha + 2 = 0$
27	$\alpha^3 - \alpha^2 + 1 = 0$

Table 2.1: Primitive polynomials for the fields $\mathbb{F}_q$.

There exists a *primitive generating element* s in $\mathbb{F}_q$ such that

$$\mathbb{F}_q = \{0, 1, s, \ldots, s^{q-2} | s^{q-1} = 1\}.$$

When q is not prime, the root α is such an element. We note $\mathbb{F}_q^*$ for the set $\mathbb{F}_q \setminus \{0\}$. If $q = p^h$, then $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$. It is called the *prime subfield* of $\mathbb{F}_q$.

Let x be an element of $\mathbb{F}_q$. Then:

- $x^q = x$.
- The *norm* $N(x)$ of x is given by $N(x) = x \cdot x^p \cdot x^{p^2} \cdot \ldots \cdot x^{p^{h-1}}$.
- The *trace* $tr(x)$ of x is given by $tr(x) = x + x^p + x^{p^2} + \cdots + x^{p^{h-1}}$.

An *automorphism* π of $\mathbb{F}_q$ is a one-to-one mapping $\mathbb{F}_q \mapsto \mathbb{F}_q : x \mapsto x^\pi$ such that

$$(x + y)^\pi = x^\pi + y^\pi, \quad (xy)^\pi = x^\pi y^\pi$$

for all $x, y \in \mathbb{F}_q$. The map $x \mapsto x^p$ is an automorphism of $\mathbb{F}_q$, known as the *Frobenius automorphism*. The elements of $\mathbb{F}_q$ fixed by the Frobenius automorphism are precisely those lying in the prime subfield $\mathbb{F}_p$. Hence when q is prime, the Frobenius automorphism is the identity. The group of automorphisms of $\mathbb{F}_q$ is cyclic of order h and is generated by the Frobenius automorphism. (This means that every automorphism has the form $x \mapsto x^{p^i}$ for some value of i with $0 \leq i \leq h - 1$).

2.2 Projective Plane

Consider the *Desarguesian projective plane* $\mathrm{PG}(2,q)$[1] over the field $\mathbb{F}_q$. $\mathrm{PG}(2,q)$ contains q^2+q+1 points and q^2+q+1 lines. There are exactly $q+1$ points on each line and $q+1$ lines through each point.

The points and lines of $\mathrm{PG}(2,q)$ satisfy the axioms of a projective plane:

- every two distinct points are on a unique common line,
- every two distinct lines contain a unique common point,
- there are four distinct points, no three of which are on a common line,

Points and lines of $\mathrm{PG}(2,q)$ can be represented by coordinate triples. Let $X = (x,y,z) \in \mathbb{F}_q^3 \setminus \{(0,0,0)\}$. The point P with coordinates X shall be represented by $P(X) = P(x,y,z)$. Likewise, the line ℓ with coordinates $U^t = (k,l,m)^t$ shall be represented by $\ell(k,l,m)^t = \ell(U^t)$. We write $(x_1,y_1,z_1) \approx (x_2,y_2,z_2)$ for two triples that are equal up to a scalar factor. Two points $P(X)$ and $P(Y)$ are the same if and only if $X \approx Y$. Likewise, two lines $\ell(U^t)$ and $\ell(V^t)$ are the same if and only if $U \approx V$.

A point $P(x,y,z)$ is incident with a line $\ell(k,l,m)^t$ if and only if

$$XU^t = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} k \\ l \\ m \end{pmatrix} = kx + ly + mz = 0.$$

With every non-singular matrix $T = (t_{ij}) \in \mathbb{F}_q^{3\times 3}$ we associate a bijection mapping the point $P(X) = P(x,y,z)$ onto $P'(X') = P'(x',y',z')$ and the line $\ell(U^t) = \ell(k,l,m)^t$ onto $\ell'(U'^t) = \ell'(k',l',m')^t$ with $X' = XT$ and $U'^t = T^{-1}U^t$.

[1] Although the theory of n-dimensional projective spaces $\mathrm{PG}(n,q)$ is very similar, we shall restrict ourselves mainly to the case $n = 2$, the context of the remainder of this text.

In other words,

$$\begin{pmatrix} x' & y' & z' \end{pmatrix} = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} t_{00} & t_{01} & t_{02} \\ t_{10} & t_{11} & t_{12} \\ t_{20} & t_{21} & t_{22} \end{pmatrix}$$

$$\begin{pmatrix} k' \\ l' \\ m' \end{pmatrix} = \begin{pmatrix} t_{00} & t_{01} & t_{02} \\ t_{10} & t_{11} & t_{12} \\ t_{20} & t_{21} & t_{22} \end{pmatrix}^{-1} \begin{pmatrix} k \\ l \\ m \end{pmatrix}.$$

Such a bijection is called a *projectivity* or *projective linear transformation*. A projectivity preserves the incidence between points and lines: a point $P(X)$ lies on a line $\ell(U^t)$ if and only if the image $P'(X')$ of $P(X)$ lies on the image $\ell'(U'^t)$ of $\ell(U^t)$. Indeed, $X'U'^t = XTT^{-1}U^t = XU^t = 0$. As with coordinate triples, also the matrix T of a projectivity is only determined up to a scalar factor.

The group of all projectivities of $\mathrm{PG}(2,q)$ is the *projective general linear group* $\mathrm{PGL}(3,q)$ and has order $q^3(q^3-1)(q^2-1)$. A projectivity is uniquely determined by the four images of the vertices of a quadrangle. In other words, $\mathrm{PGL}(3,q)$ acts transitively on ordered quadrangles.

A *collineation* in $\mathrm{PG}(2,q)$ is a bijection mapping points to points and lines to lines, which preserves incidence. Clearly each projectivity is a collineation. However, in general not all collineations are projectivities. The Frobenius automorphism mapping the point $P(x,y,z)$ onto $P'(x^p,y^p,z^p)$ is a collineation, but not a projectivity. The fundamental theorem of projective geometry states that each collineation can be seen as a combination of a projectivity and a field automorphism. Let ψ be a collineation, then there exists a non-singular matrix T and a field automorphism σ, such that

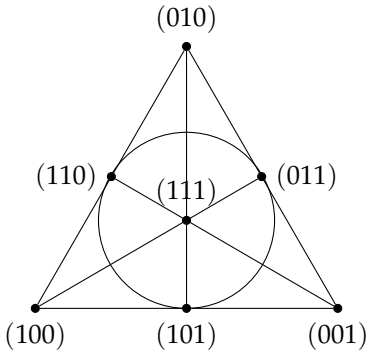
$$\psi : \begin{pmatrix} x & y & z \end{pmatrix} \mapsto \begin{pmatrix} x & y & z \end{pmatrix}^\sigma \begin{pmatrix} t_{00} & t_{01} & t_{02} \\ t_{10} & t_{11} & t_{12} \\ t_{20} & t_{21} & t_{22} \end{pmatrix}^\sigma$$

$$\psi : \begin{pmatrix} k \\ l \\ m \end{pmatrix} \mapsto \left(\begin{pmatrix} t_{00} & t_{01} & t_{02} \\ t_{10} & t_{11} & t_{12} \\ t_{20} & t_{21} & t_{22} \end{pmatrix}^{-1} \right)^\sigma \begin{pmatrix} k \\ l \\ m \end{pmatrix}^\sigma$$

The group of all collineations of $\mathrm{PG}(2,q)$ is the *collineation group* $\mathrm{P\Gamma L}(3,q)$ and has order $hq^3(q^3-1)(q^2-1)$. $\mathrm{PGL}(3,q)$ is a subgroup of $\mathrm{P\Gamma L}(3,q)$ and $[\mathrm{P\Gamma L}(3,q) : \mathrm{PGL}(3,q)] = h$. When q is prime, then $\mathrm{PGL}(3,q) = \mathrm{P\Gamma L}(3,q)$.

Two sets of points are called *equivalent* (or $\mathrm{P\Gamma L}$-equivalent) if there exists a collineation mapping one set to the other. Note that we consider the collineations of the full group $\mathrm{P\Gamma L}(3,q)$ in this definition. If there exists a projectivity mapping one set of points to another, i.e., a collineation of $\mathrm{PGL}(3,q)$, then the sets will be called PGL-equivalent. When q is a prime, both notions of equivalence coincide.

Example 2.1 The smallest projective plane is $\mathrm{PG}(2,2)$. It consists of 7 points and 7 lines. Each point is lying on 3 lines, each line contains 3 points. This plane is called the *Fano plane* and is depicted below.



□

2.3 Projective Line

Let $\mathrm{PG}(1,q)$ be the *projective line* over the field $\mathbb{F}_q$. $\mathrm{PG}(1,q)$ has exactly $q+1$ points and each point P is determined by a coordinate pair $X \in \mathbb{F}_q^2 \setminus \{(0,0)\}$,

again unique only up to a scalar factor. We will write both $P(x,y)$ and $P(X)$ for the point P with coordinates X. We shall usually normalise the coordinates of the points on the line as the set $\{(1,t)|t \in \mathbb{F}_q\} \cup \{(0,1)\}$. Mapping $t \in \mathbb{F}_q$ to $(1,t)$ and ∞ to $(0,1)$ defines a one-one relation between $\mathbb{F}_q \cup \{\infty\}$ and $\mathrm{PG}(1,q)$. We say that $t \in \mathbb{F}_q \cup \{\infty\}$ is the coordinate of a point on the projective line.

With every non-singular matrix $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a,b,c,d \in \mathbb{F}_q$ we asociate a bijection mapping the point $P(X) = P(x,y)$ onto $P'(X') = P'(x',y')$ with $X' = XT$. Such a bijection is called a *projectivity* or *projective linear transformation*. The group of projectivities can be represented by its action on $\mathbb{F}_q \cup \{\infty\}$: the transformation $t \mapsto (b+dt)/(a+ct)$ is associated to an element of $\mathrm{PGL}(2,q)$ in the following way:

$$\begin{pmatrix} 1 & t \end{pmatrix} \mapsto \begin{pmatrix} 1 & t \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2.1}$$

A projectivity in $\mathrm{PG}(1,q)$ is uniquely determined by the images of three different points.

The group of all projectivities of $\mathrm{PG}(1,q)$ is the *projective general linear group* $\mathrm{PGL}(2,q)$ and has order $q(q^2-1)$.

As before, the group $\mathrm{P\Gamma L}(2,q)$ can be extended to the full group of all collineations $\mathrm{P\Gamma L}(2,q)$ by combining projectivities with field automorphisms.

2.4 Conic

A *conic* $\mathcal{C}$ is a set of $q+1$ points of $\mathrm{PG}(2,q)$ whose coordinates (x,y,z) are the zeroes of an absolutely irreducible quadratic form

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + dxy + eyz + fzx,$$

with $a,b,c,d,e,f \in \mathbb{F}_q$. When q is odd, every conic $\mathcal{C}$ can be represented as a symmetric matrix A: a point $P(x,y,z)$ lies on $\mathcal{C}$ if and only if $XAX^t = 0$, i.e.

if and only if

$$XAX^t = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} a & d/2 & f/2 \\ d/2 & b & e/2 \\ f/2 & d/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

Consider a projectivity $T \in \mathrm{PGL}(3,q)$. Let $\mathcal{C}$ denote the conic represented by the matrix A. Then the image $\mathcal{C}'$ of $\mathcal{C}$ by T is represented by the matrix $A' = T^{-1}A(T^{-1})^t$. Indeed,

$$\begin{aligned} X'A'X'^t &= (XT)(T^{-1}A(T^{-1})^t)(XT)^t \\ &= XTT^{-1}A(T^{-1})^tT^tX^t \\ &= XAX^t \\ &= 0. \end{aligned}$$

One can always find a projectivity T that maps the conic $\mathcal{C}$ onto the conic wih equation

$$y^2 = xz.$$

We will call this conic the *standard conic*. It follows that all conics in $\mathrm{PG}(2,q)$ are equivalent.

When q is even, we cannot represent the conic by the use of a symmetric matrix, but we can still map each conic onto the standard conic. Hence also for even q, all conics are equivalent.

In this text $\mathcal{C}$ will usually refer to the standard conic, unless explicitely noted otherwise. When q is odd, the matrix representation of this conic is

$$XCX^t = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

We usually represent the points of the standard conic by the following coordinates: $(0,0,1)$ and $(1,t,t^2)$ with $t \in \mathbb{F}_q$. Mapping $t \in \mathbb{F}_q$ to $(1,t,t^2)$ and ∞ to $(0,0,1)$ defines a one-one relation between $\mathbb{F}_q \cup \{\infty\}$ and $\mathcal{C}$. This yields a natural bijection between the conic and the projective line. It can be used to show that the subgroup of $\mathrm{PGL}(3,q)$ that stabilizes $\mathcal{C}$ (the projective group $\mathrm{PGO}(3,q)$ of order $q(q^2-1)$) is isomorphic to the group $\mathrm{PGL}(2,q)$. Indeed,

consider a general element $t \mapsto (b+dt)/(a+ct)$ of $\mathrm{PGL}(2,q)$. Applied to the point $(1,t,t^2)$ of $\mathcal{C}$, this yields

$$\begin{aligned}(1\ t\ t^2) &\mapsto \left(1\ \tfrac{b+dt}{a+ct}\ (\tfrac{b+dt}{a+ct})^2\right)\\ &\approx \left((a+ct)^2\ (a+ct)(b+dt)\ (b+dt)^2\right)\\ &= (1\ t\ t^2)\begin{pmatrix} a^2 & ab & b^2\\ 2ac & ad+bc & 2bd\\ c^2 & cd & d^2\end{pmatrix}.\end{aligned}$$

This can be extended to all points (x,y,z) of $\mathrm{PG}(2,q)$:

$$(x\ y\ z) \mapsto (x\ y\ z)\begin{pmatrix} a^2 & ab & b^2\\ 2ac & ad+bc & 2bd\\ c^2 & cd & d^2\end{pmatrix}. \tag{2.2}$$

A point $P(x,y,z)$ which does not lie on the conic $\mathcal{C}$ is called *external* to $\mathcal{C}$ (resp. *internal* to $\mathcal{C}$) if and only if y^2-xz is a non-zero square (resp. a non-square) in $\mathbb{F}_q$. Three different points of the same conic are never collinear. We call a line intersecting the conic in 0 (resp. 1 or 2) points an external line (resp. tangent or secant). The intersection of a tangent ℓ and the conic $\mathcal{C}$ is called the tangent point of ℓ. When q is odd, there are exactly two tangents and $(q-1)/2$ secants through an external point of C. The tangent points of the two tangents through an external point p will be called the tangent points of p. An internal point does not lie on any tangent of $\mathcal{C}$ and hence lies on $(q+1)/2$ secants.

When q is even, there are no internal points and the $q+1$ tangents to a conic are concurrent. The point of intersection is called the *nucleus* and for the standard conic this is the point with coordinates $(0,1,0)$.

A *polarity* π is a bijection mapping points to lines and lines to points, which inverts incidence and such that π^2 is the identity. The image of a line is called the *pole* of the line, that of a point is called the *polar line* of the point. When q is odd, the matrix A of a conic $\mathcal{C}$ is the matrix of a polarity. The polar line of a point $P(X)$ has coordinates AX^t. The pole of a line $\ell(U)$ has coordinates $(A^{-1}U)^t$. When $\mathcal{C}$ is the standard conic, the polar line of a point $P(x,y,z)$ has coordinates $CX^t = (z,-2y,x)^t$, the pole of a line $\ell(k,l,m)^t$ has coordinates $(C^{-1}U)^t = (m,-l/2,k)$. The polarity of a conic $\mathcal{C}$ maps each point of $\mathcal{C}$ on the

tangent to $\mathcal{C}$ through that point. Also, each tangent to $\mathcal{C}$ is mapped onto its tangent point. Internal points are mapped onto external lines, external points are mapped onto secants and vice versa. The polar secant of an external point is the line connecting the two tangent points of this external point.

It is well known that when $q \geq 4$, there is a unique conic through each set of 5 points in which no three points are collinear. Also, two conics intersect in at most 4 points.

2.5 Cubic curve

A *cubic curve* $\mathcal{F}$ is a set of points of $\mathrm{PG}(2,q)$ whose coordinates (x,y,z) are the zeroes of an absolutely irreducible cubic form

$$F(x,y,z) = a_1x^3 + a_2y^3 + a_3z^3 + a_4x^2y + a_5x^2z + a_6xy^2 + a_7y^2z + a_8xz^2 + a_9yz^2 + a_{10}xyz,$$

with $a_1,\ldots,a_{10} \in \mathbb{F}_q$.

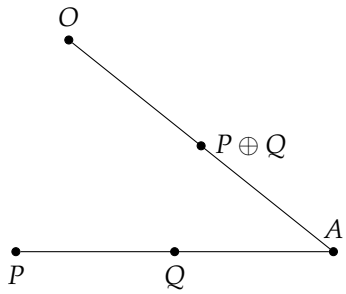
An *inflexion point* of a cubic curve $\mathcal{F}$ is a point of $\mathcal{F}$ at which the tangent has three-point contact. For odd q, the *Hessian* of the curve $\mathcal{F}$ is the curve $\mathcal{H}$ with equation $H(x,y,z) = 0$, with

$$H(x,y,z) = \begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial x \partial z} & \frac{\partial^2 F}{\partial y \partial z} & \frac{\partial^2 F}{\partial z^2} \end{vmatrix}.$$

The inflexion points are the points $P(x,y,z)$ of $\mathcal{F}$ satisfying $H(x,y,z) = 0$ and $\frac{\partial F}{\partial x}(x,y,z)\frac{\partial F}{\partial y}(x,y,z)\frac{\partial F}{\partial z}(x,y,z) \neq 0$.

A *singular point* $P(x,y,z)$ is a point of $\mathcal{F}$ for which $\frac{\partial F}{\partial x}(x,y,z) = \frac{\partial F}{\partial y}(x,y,z) = \frac{\partial F}{\partial z}(x,y,z) = 0$.

Cubic curves have the interesting property that a group operation can be introduced on the curve. The non-singular points of an absolutely irreducible plane cubic curve $\mathcal{F}$ form an abelian group $G_{\mathcal{F}}$ as follows: let P, Q be non-singular points of $\mathcal{F}$ and let A be the third point on the line PQ that also lies on the cubic $\mathcal{F}$. Take a non-singular point $O \in \mathcal{F}$ as identity point. Then $P \oplus Q$ is the third cubic point on the line OA, with A the third point on the line PQ.



If $P = Q$, then $P \oplus P = 2P$ is the third cubic point on the line OA, with A the other point on the line that is tangent to $\mathcal{F}$ in the point P. If PQ is tangent to $\mathcal{F}$ in the point P with $P \neq Q$, then $P \oplus Q$ is the third cubic point on the line OP. If $A = O$, then $P \oplus Q = O'$, the second point on the tangent through O. If the line OA is tangent to $\mathcal{F}$ in A then $P \oplus Q = A$.

In general, three points P, Q and R are collinear if and only if $P \oplus Q \oplus R = O'$. If the identity O is an inflexion, then $O' = O$ and three points P, Q and R are collinear if and only if $P \oplus Q \oplus R = O$. Also $2P \oplus Q = O$ if Q is the other point that lies on the tangent through P. For an inflexion point S we have $3S = 0$.

2.6 Arcs

A (k, n)-*arc* S of $\mathrm{PG}(2, q)$ is defined to be a set of k points of the plane such that at least one line of the plane meets S in n points but no line meets S in more than n points.

For $n = 2$, it is easily seen that k cannot be larger than $q + 2$. For every even q examples of $(q + 2)$ arcs are known. When q is odd, it can be proved that $(q + 2)$-arcs do not exist. However, every conic is a $(q + 1)$-arc, and a well-known theorem of Segre proves that also the converse is true when q is odd. A $(k, 2)$-arc is called *complete* if and only if it is not contained in a $(k + 1, 2)$-arc. By definition, a line of $\mathrm{PG}(2, q)$ intersects a k-arc in either 0, 1 or 2 points, in which case it is called an *external line*, a *unisecant* or a *bisecant*, respectively. A $(k, 2)$-arc is complete if and only if every point of the plane lies on at least one bisecant of the arc. (The unisecants of a conic are its tangents, the bisecants its secants.) By the above, when q is odd, a $(q + 1)$-arc always exists and is complete. It can be proved however that a q-arc always is contained in a conic and hence never is complete [19]. For $q > 13$, it can be proved that a $(q - 1)$-arc is incomplete, except possibly for q, $37 \leq q \leq 89$ [19]. For q, $13 < q < 31$, full classifications are known and no complete $(q - 1)$-arc occurs. In [26], Kéri showed that for $q = 31$ the second largest size of a complete arc is 22, hence also in $\mathrm{PG}(2, 31)$ each $(q - 1)$-arc is incomplete. For $q \leq 13$, a complete $(q - 1)$-arc exists for $q = 7, 9, 11, 13$ (see Chapter 6).

For $n = 3$ and $q \geq 4$, it can be proved that $k \leq 2q + 1$. It is well known that an absolutely irreducible cubic curve always is a $(k, 3)$-arc. A $(k, 3)$-arc is called *complete* if and only if it is not contained in a $(k + 1, 3)$-arc. By definition, a line of $\mathrm{PG}(2, q)$ intersects a $(k, 3)$-arc in either 0, 1, 2 or 3 points, in which case it is called an *external line*, a *unisecant*, a *bisecant* or a *trisecant*, respectively. A $(k, 3)$-arc is complete if and only if every point of the plane lies on at least one trisecant of the arc. We will often silently drop the requirement that at least one line must contain 3 points, especially in Chapter 4 where the algorithms are discussed. In other words, we will sometimes regard a $(k, 2)$-arc as a special case of a $(k, 3)$-arc. Of course, for complete $(k, 3)$-arcs this is not an issue because a $(k, 2)$-arc can never be a complete $(k, 3)$-arc.

In this text, the term "arcs" will always refer to $(k, 2)$- or $(k, 3)$-arcs. It will always be clear from the context which of the two is meant. In some cases, it can refer to either when describing some general aspects.

Let S be any $(k, 2)$-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.

For further information on the geometrical properties of $(k,2)$- and $(k,3)$-arcs we refer to [19].

2.7 Information on groups

Notations

Let V denote a finite set and let G denote a group with a right action on V. Let $s \in V$, $g \in G$. We usually write s^g for the image of s through the action of g and hence $s^{gh} = (s^g)^h$. Also, for $g, h \in G$, we write $g^h = h^{-1}gh$.

Sometimes it is more convenient to write $\sigma(x)$ with $x \in V$, $\sigma \in G$. In this case we have $(\sigma_1\sigma_2)(x) = \sigma_2(\sigma_1(x))$. Note the reversal of the order.

If $S \subseteq V$, we write $S^g \stackrel{\text{def}}{=} \{s^g \mid s \in S\}$ for the image of S through the action of g and $G_S \stackrel{\text{def}}{=} \{g \in G \mid S^g = S\}$ for the set stabilizer of S. If $H \leq G$, i.e., if H is a subgroup of G, then $s^H \stackrel{\text{def}}{=} \{s^h \mid h \in H\}$ denotes the orbit of s through H, and similarly, the orbit of S is denoted by S^H.

The symmetric group on four elements

It is well known that $\mathrm{PGL}(3,q)$ acts sharply transitively on ordered quadrangles in $\mathrm{PG}(2,q)$. Hence any permutation of the 4 vertices of a quadrangle can be extended uniquely to a projectivity. Therefore, with every choice of quadrangle there corresponds an embedding of the symmetric group S_4 on 4 elements in $\mathrm{PGL}(3,q)$. In particular, two choices of quadrangles lead to nice representations of S_4 in $\mathrm{PGL}(3,q)$.

First, consider the following quadrangle:

$$(1,1,1), (-1,1,1), (1,-1,1), (1,1,-1).$$

With this representation the group elements consist of two types of transformations: the permutations of the three coordinates and the transformations changing the sign of one or more of the coordinates. The subgroup A_4 (the alternating group on 4 elements) of S_4 then consists of the permutations of the three coordinates of order 3 and changing the sign of exactly one coordinate. Note that this representation only holds for q odd.

For a second representation, we look at $\mathrm{PG}(2,q)$ as the plane with equation $x+y+z+u=0$ in the three-dimensional projective space $\mathrm{PG}(3,q)$ and we choose the following quadrangle:

$$(1,1,1,-3),(1,1,-3,1),(1,-3,1,1),(-3,1,1,1).$$

With this representation the group consists of all permutations of the four coordinates. The subgroup A_4 then contains all even permutations of the four coordinates.

Note that both representations of S_4 are equivalent.

3

Arcs with large conical subsets

In this chapter we classify the $(k,2)$-arcs in PG$(2,q)$, q odd, which consist of $(q+3)/2$ points of a conic $\mathcal{C}$ and two points not on the conic but external to $\mathcal{C}$, or $(q+1)/2$ points of $\mathcal{C}$ and two additional points, at least one of which is an internal point of $\mathcal{C}$. We prove that for arcs of the latter type, the number of points internal to $\mathcal{C}$ 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. The results are listed in Section 3.8. In this chapter q is odd and "arcs" will always refer to $(k,2)$-arcs. Most of this chapter has been published in [11].

3.1 Introduction

As mentioned in Section 2.6, when q is odd an arc can be of size at most $q+1$ and in that case it always coincides with the set of points of some conic $\mathcal{C}$ (and is complete). It is natural to ask what the second biggest size for a complete arc in $\mathrm{PG}(2,q)$ is.

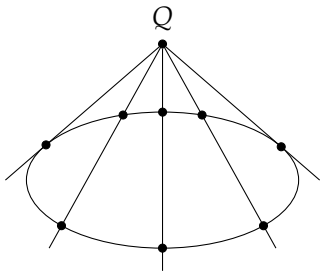
Removing some points from a conic $\mathcal{C}$ yields an arc, but this arc is obviously not complete. However, removing a sufficient number of points (at least $(q-1)/2$, as will be shown later) it may be possible to extend the set thus obtained to an arc by adding a point that does not belong to $\mathcal{C}$. 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 chapter. For many values of q, arcs of this type are among the largest ones known.

Fix an arc S and a conical subset T of S. The elements of $U \stackrel{\text{def}}{=} S \setminus T$ will be called *supplementary* points and the number $e = |U|$ of supplementary points will be called the *excess* of the arc. In this chapter, we shall always assume that $e \geq 1$, i.e., that S is not fully contained in a conic.

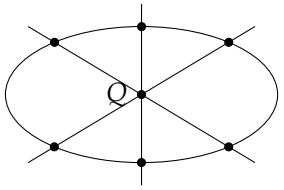
Arcs of this type fall into two categories, depending on whether at least one of the supplementary points is internal or not.

Theorem 3.1 *Let q be odd and let S be an arc which is not a conic, then the maximum size of a conical subset T of S is $\frac{q+3}{2}$. If $|T| = \frac{q+3}{2}$, then all points of $U = S \setminus T$ are external points of the conic. If U contains at least one internal point of C, then $|T| \leq \frac{q+1}{2}$.*

Proof : When $Q \in U$ 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 $|T| \leq (q+3)/2$.



Likewise, when Q is an internal point, the $(q+1)/2$ secants imply that $|T| \leq (q+1)/2$ (there are no tangents through Q in this case).



■

We call conical subsets which attain these bounds *large*. 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 $\mathcal{C}$.
- An arc S of *type E* has a conical subset of size $(q+3)/2$ where all supplementary points are *external* points of $\mathcal{C}$.
- 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 $\mathcal{C}$ and some are *external* points.

Only a few arcs are known with large conical subsets and with an excess greater than 2. We establish a simple theoretical framework for an extensive

computer search for arcs of that type. In Sections 3.3, 3.4 and 3.5 we provide a complete (computer-free) classification of all such arcs with excess 2, up to projective equivalence. 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 3.8.

Arcs of this type have also been studied by Pellegrino [37, 38], Korchmáros and Sonnino [24, 25] and Davydov, Faina, Marcugini and Pambianco [14]. In particular, our methods are similar to those of Korchmáros and Sonnino [25], 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 $\mathbb{F}_{q^2}$. 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.

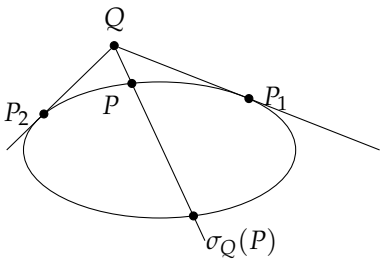
3.2 Notation and preliminary definitions

Before we proceed, we shall first establish some notations and list some elementary results. Similar notation and properties are used in [37, 38].

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

As in Section 2.4, for the points on $\mathcal{C}$ we shall mostly use coordinates $(1, t, t^2)$, $t \in \mathbb{F}_q \cup \{\infty\}$.

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



Let Q and P respectively have coordinates (a, b, c) and $(1, t, t^2)$ and let the third point on the line PQ have coordinates $(1, u, u^2)$, then

$$0 = \begin{vmatrix} 1 & t & t^2 \\ 1 & u & u^2 \\ a & b & c \end{vmatrix} = (t-u)(-atu + b(t+u) - c)$$

and hence $u(b - at) = c - bt$. It follows that σ_Q maps t to $u = (c - bt)/(b - at)$, or equivalently, that σ_Q acts like the element of $\mathrm{PGL}(2, q)$ represented by the following matrix:

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

This involution can be extended to the entire plane as in (2.2).

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 $\mathcal{C}$. The lines fixed by σ_Q are the $q + 1$ lines through Q and the polar line of Q.

It is easily proved that 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 $\mathcal{C}$.

Q is an external point to $\mathcal{C}$ if and only if $b^2 - ac$ is a (non-zero) square of $\mathbb{F}_q$. In that case the two points of $\mathcal{C}$ 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 $\mathbb{F}_q$ and let $L = \mathbb{F}_q[\sqrt{\beta}]$ denote the quadratic extension field of $\mathbb{F}_q$. We write $\bar{x} = x^q$ for the conjugate of $x \in L$. 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 $i \in \mathbb{Z}_{q^2-1}$ define $c_i, s_i \in \mathbb{F}_q$ to be the 'real' and 'imaginary' part of α^i, i.e., $\alpha^i \stackrel{\text{def}}{=} c_i + s_i\sqrt{\beta}$. The conjugate of α^i satisfies $\bar{\alpha}^i = c_i - s_i\sqrt{\beta}$ and

$$c_i = \frac{\alpha^i + \bar{\alpha}^i}{2}, \quad s_i = \frac{\alpha^i - \bar{\alpha}^i}{2\sqrt{\beta}}$$

From $\alpha^0 = 1$ and $\alpha^{i+j} = \alpha^i \cdot \alpha^j$, we derive

$$c_0 = 1, \quad s_0 = 0, \quad c_{i+j} = c_i c_j + s_i s_j \beta, \quad s_{i+j} = c_i s_j + s_i c_j. \tag{3.1}$$

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' $t_i \in \mathbb{F}_q \cup \{\infty\}$:

$$t_i \stackrel{\text{def}}{=} s_i/c_i = \frac{1}{\sqrt{\beta}} \frac{\alpha^i - \bar{\alpha}^i}{\alpha^i + \bar{\alpha}^i}.$$

Let $\phi \stackrel{\text{def}}{=} \alpha/\bar{\alpha} = \alpha^{1-q}$. Note[1] that $N(\phi) = \phi^{q+1} = \alpha^{1-q^2} = 1$ and $\phi^{\frac{q+1}{2}} = -1$. Every element of L^* of norm 1 can be written as ϕ^i for some exponent i which is unique mod $q + 1$. We may now express t_i directly in terms of ϕ as follows:

$$t_i = \begin{cases} \dfrac{1}{\sqrt{\beta}} \dfrac{\phi^i - 1}{\phi^i + 1}, & \text{when } \phi^i \neq -1, \\ \infty, & \text{when } \phi^i = -1. \end{cases} \tag{3.2}$$

We have the following properties:

[1] In this chapter, $N(x) = N\left[L : \mathbb{F}_q\right](x) = x\bar{x} = x^{q+1}$ for $x \in L$.

Lemma 3.2

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

Also, $t_i = t_j$ if and only if $i \equiv j \pmod{q+1}$.

Proof : Recall that $r = (q+1)/2$ and $\phi^r = -1$.

It is easily seen that $t_0 = t_{q+1} = 0$, $t_r = \infty$ and $t_{-i} = -t_i$, using (3.2) and the properties of ϕ.

For t_{i+r}, we find

$$t_{i+r} = \frac{1}{\sqrt{\beta}} \frac{\phi^i \phi^r - 1}{\phi^i \phi^r + 1} = \frac{1}{\sqrt{\beta}} \frac{-\phi^i - 1}{-\phi^i + 1} = \frac{\sqrt{\beta}}{\beta} \frac{\phi^i + 1}{\phi^i - 1} = \frac{1}{t_i \beta}.$$

Note that when $\phi^i = 1$, then $t_i = 0$ and $t_{i+r} = \infty = t_r$.

Using (3.1), we find

$$t_{i+j} = \frac{s_{i+j}}{c_{i+j}} = \frac{c_i s_j + s_i c_j}{c_i c_j + s_i s_j \beta} = \frac{\frac{c_i s_j + s_i c_j}{c_i c_j}}{\frac{c_i c_j + s_i s_j \beta}{c_i c_j}} = \frac{\frac{s_j}{c_j} + \frac{s_i}{c_i}}{1 + \frac{s_i s_j \beta}{c_i c_j}} = \frac{t_i + t_j}{1 + t_i t_j \beta}$$

This also implies $t_{i+(q+1)} = t_i$. We have $t_i = t_j$ if and only if

$$\frac{\phi^i - 1}{\phi^i + 1} = \frac{\phi^j - 1}{\phi^j + 1}$$
$$\phi^{i+1} + \phi^i - \phi^j - 1 = \phi^{i+1} + \phi^j - \phi^i - 1$$
$$\phi^i = \phi^j,$$

i.e. if and only if $i \equiv j \pmod{q+1}$ ∎

The index i of t_i can be treated as an element of $\mathbb{Z}_{q+1}$. The sequence $t_0, t_1, \ldots, t_q$ contains every element of $\mathbb{F}_q \cup \{\infty\}$ exactly once.

Let ℓ be an external line of $\mathcal{C}$. 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 $(\beta, 1/t_i, 1) \approx (s_i\beta, c_i, s_i)$ for $i \neq 0$ and 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 $\mathbb{Z}_{q+1}$. The point Q_i is an external (resp. internal) point of $\mathcal{C}$ if and only if $c_i^2 - s_i^2\beta$ is a square (resp. non-square). This value is the norm of α^i $N(\alpha^i) = N(\alpha)^i$, hence Q_i is external (resp. internal) if its orbital index i is even (resp. odd).

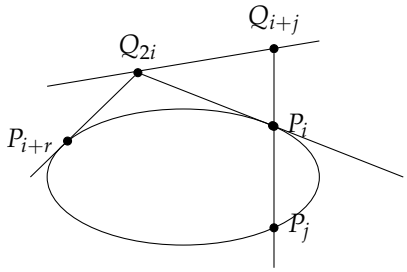
In a similar way, we number the points of the conic $\mathcal{C}$ as $P_0, P_1, \ldots, P_q$ where P_i has coordinates $(1, t_i, t_i^2)$, for $i \neq r$ and P_r has coordinates $(0, 0, 1)$. Again, the index i of P_i will be called its *orbital index*, and again it can be treated as an element of $\mathbb{Z}_{q+1}$.

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

Lemma 3.3 *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 $\mathcal{C}$ if and only if $k \equiv 2i \pmod{q+1}$.*

Proof :



P_i, P_j, Q_k are collinear if and only if P_j is the image of P_i under the action of σ_{Q_k} and vice versa. The action of σ_{Q_k} on P_i is

$$\begin{aligned}
\begin{pmatrix} 1 & t_i \end{pmatrix} \begin{pmatrix} c_k & s_k \\ -s_k\beta & -c_k \end{pmatrix} &= \begin{pmatrix} c_k - s_k\beta s_i/c_i & s_k - c_k s_i/c_i \end{pmatrix} \\
&\approx \begin{pmatrix} 1 - s_k s_i \beta/c_k c_i & s_k/c_k - s_i/c_i \end{pmatrix} \\
&= \begin{pmatrix} 1 - t_k t_i \beta & t_k - t_i \end{pmatrix} \\
&\approx \begin{pmatrix} 1 & \frac{t_k - t_i}{1 - t_k t_i \beta} \end{pmatrix} \\
&= \begin{pmatrix} 1 & t_{k-i} \end{pmatrix},
\end{aligned}$$

so P_j is the image of P_i under σ_{Q_k} if and only if $k - i \equiv j \pmod{q+1}$ or $k = i + j \pmod{q+1}$.

P_iQ_k is a tangent to $\mathcal{C}$ if and only if the image of P_i under the action of σ_{Q_k} is again P_i which is only the case if $k - i \equiv i \pmod{q+1}$ or $k = 2i \pmod{q+1}$.
■

Lemma 3.4 *The subgroup H of $\mathrm{PGL}(3,q)$ that leaves both the conic $\mathcal{C}$ and its external line ℓ invariant, is a dihedral group of order $2(q+1)$ whose elements correspond to matrices of the following type*[2]*:*

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

Proof : The group H consists of all matrices of the form (2.2) that leave the line ℓ invariant, i.e., such that

$$\begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad+bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -\beta \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ -\beta \end{pmatrix},$$

[2]Also for matrices, "$\approx$" denotes equality up to a scalar factor.

or equivalently

$$ac = bd\beta, \quad -\beta(a^2 - b^2\beta) = (c^2 - d^2\beta).$$

From this we obtain $(c + a\sqrt{\beta})^2 = (b\beta + d\sqrt{\beta})^2$ and hence $c + a\sqrt{\beta} = \pm(b\beta + d\sqrt{\beta})$. As $a, b, c, d \in \mathbb{F}_q$ but $\sqrt{\beta} \notin \mathbb{F}_q$, we find the solutions $c = b\beta$, $a = d$ and $c = -b\beta$, $a = -d$. In terms of matrices of $\mathrm{PGL}(2, q)$ and $\mathrm{PGL}(3, q)$ the results are the following:

$$\begin{pmatrix} a & b \\ \pm b\beta & \pm a \end{pmatrix}, \begin{pmatrix} a^2 & ab & b^2 \\ \pm 2ab\beta & \pm a^2 + b^2\beta) & \pm 2ab \\ b^2\beta^2 & ab\beta & a^2 \end{pmatrix},$$

which are exactly the matrices M_i and M'_i when replacing b/a by t_i. ∎

We have

$$M'_0 = 1, \quad M'_i = {M'_1}^i, \quad M'_i = M_0 M_i,$$
$$M'_{i+j} = M'_i M'_j \quad M_{i+j} = M_i M_0 M_j.$$

(Again indices can be treated as belonging to $\mathbb{Z}_{q+1}$.) 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 H 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 $(-\beta, 0, 1)$.

Lemma 3.5 *The action of the reflections and rotations on $\mathcal{C}$ and ℓ is given by*

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

Proof : Note that $t_{2i} = 2t_i/(1 + t_i^2\beta)$ and

$$t_{2i-1} = \frac{t_{2i} - t_j}{1 - t_{2i}t_j\beta} = \frac{2t_i - t_j(1 + t_i^2\beta)}{1 + t_i^2\beta - 2t_i t_j\beta}.$$

We have

$$P_j M_i = \begin{pmatrix} 1 - t_i t_j \beta & t_i - t_j \end{pmatrix} = \begin{pmatrix} 1 & t_{i-j} \end{pmatrix} = P_{i-j}$$

and

$$\begin{aligned} Q_j M_i &= \begin{pmatrix} \beta & 1/t_j & 1 \end{pmatrix} \begin{pmatrix} 1 & t_i & t_i^2 \\ -2t_i\beta & -1 - t_i^2\beta & -2t_i \\ t_i^2\beta^2 & t_i\beta & 1 \end{pmatrix} \\ &= \begin{pmatrix} \beta(1 - 2t_i/t_j + t_i^2\beta) & t_i\beta - (1 + t_i^2\beta)/t_j + t_i\beta & t_i^2\beta - 2t_i/t_j + 1 \end{pmatrix} \\ &\approx \begin{pmatrix} \beta(t_j - 2t_i + t_i^2 t_j\beta) & t_i t_j\beta - 1 - t_i^2\beta + t_i t_j\beta & t_i^2 t_j\beta - 2t_i + t_j \end{pmatrix} \\ &\approx \begin{pmatrix} \beta & \frac{2t_i t_j\beta - 1 - t_i^2\beta}{t_i^2 t_j\beta - 2t_i + t_j} & 1 \end{pmatrix} \\ &= \begin{pmatrix} \beta & 1/t_{2i-j} & 1 \end{pmatrix} \\ &= Q_{2i-j}. \end{aligned}$$

Toghether with $M_i' = M_0 M_i$, this implies

$$P_j M_i' = P_j M_0 M_i = P_{-j} M_i = P_{i+j}$$

and

$$Q_j M_i' = Q_j M_0 M_i = Q_{-j} M_i = Q_{2i+j}$$

■

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 H 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 H_k of Q_k in H has order 4 and consists of M_0' (the identity), M_r', M_k and M_{k+r}. H_k fixes Q_k and Q_{k+r} and interchanges Q_i and Q_{2k-i} for $i \neq k, k+r$.

We now introduce some definitions that will be useful in the rest of this chapter.

Let $\mathcal{C}$ 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 $\Gamma(\mathcal{C}, U)$ as follows:

- Vertices are the elements of $\mathbb{Z}_{q+1}$,
- 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 $\Gamma(\mathcal{C}, U)$ is at most $|U|$.

Let S be an arc with corresponding conical subset $T = \mathcal{C} \cap S$. Write $U = S \setminus T$. Denote by $N(T)$ the set of orbital indices of vertices of T, i.e., the unique subset of $\mathbb{Z}_{q+1}$ 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 $\Gamma(\mathcal{C}, U)$, vertices of $N(T)$ can never be adjacent. In other words, $N(T)$ is an *independent set* of $\Gamma(\mathcal{C}, U)$.

3.3 Arcs of type I with excess two

Let S denote 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 $\mathcal{C}$.

As was explained in the introduction, each secant line through one of the supplementary points intersects $\mathcal{C}$ 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 $\mathcal{C}$. Because the supplementary points are internal, the line cannot be a tangent to $\mathcal{C}$ either and hence it must be an external line.

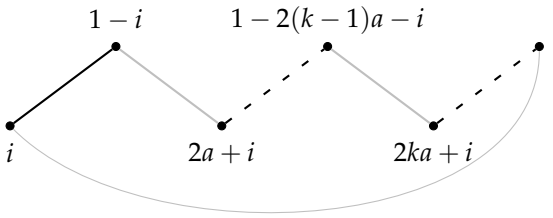
Without loss of generality we may assume this line to be the line ℓ with equation $x = \beta z$ (as in the previous section). All internal points on ℓ lie in a single orbit of H, and therefore we may take the first of the supplementary points to be Q_1. The second supplementary point must have an odd 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 $\Gamma = \Gamma(\mathcal{C}, U) = \Gamma(\mathcal{C}, \{Q_1, Q_{2a+1}\})$. The edges of Γ are of the form $\{j, 1-j\}$ and $\{j, 2a+1-j\}$ (by Lemma 3.3) and therefore Γ must be

a regular graph of order $q+1$ and of degree 2, i.e., a union of pairwise disjoint 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 $i \equiv (2na)+i \pmod{q+1}$, or length $2n+1$ with $i \equiv 1-(2na)-i \pmod{q+1}$. 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 first case applies and n is equal to the order of $2a \pmod{q+1}$, i.e., n is the smallest positive integer such that $na \equiv 0 \pmod{r}$. Note that n is independent of the choice of i and therefore all cycles have the same size. This proves the following result.

Lemma 3.6 *If S is an arc of type I with supplementary points Q_1 and Q_{2a+1}, then $\Gamma(\mathcal{C}, U)$ 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 $Z_k \stackrel{\text{def}}{=}$

$k + 2a\mathbb{Z}_{q+1} = k + 2d\mathbb{Z}_{q+1}$. (Because a is a multiple of d, each multiple of $2a$ is also a multiple of $2d$.) 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 3.7 *Let $a \in \{1, \ldots, r-1\}$. Let $d = \gcd(a, r)$. Let $S = T \cup \{Q_1, Q_{2a+1}\}$, with $T \subset \mathcal{C}$ 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 the union of pairwise disjoint sets, of the form*

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

with independent choices of sign.

Every arc listed in Theorem 3.7 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 $Z_k^{\pm}$.

Example 3.1 Consider the Galois Field $\mathbb{F}_{19}$. Then $q + 1 = 20$, $r = 10$ and we find the following table for the values of a, n and d:

a	n	d
1,3,7,9	10	1
2,4,6	5	2
5,8	2	5

For $a = 6$, we have two cycles

$$1, 0, 13, 8, 5, 16, 17, 4, 9, 12, 1$$

$$2, 19, 14, 7, 6, 15, 18, 3, 10, 11, 2$$

with

$$Z_1^+ = \{1,13,5,17,9\} \quad Z_1^- = Z_0 = \{0,8,16,4,12\}$$
$$Z_2^+ = \{2,14,6,18,10\} \quad Z_2^- = Z_{19}\{19,7,15,3,11\}$$

Hence, there are four arcs S of type I of size 12 with $S \setminus T = \{Q_1, Q_{13}\}$. These are the arcs with signatures $I(6,+,+)$, $I(6,+,-)$, $I(6,-,+)$ and $I(6,-,-)$. Note that some of these arcs are equivalent. For instance, the mapping $M_{17} = M_{a+r+1}$ maps the first arc onto the last arc and the second onto the third arc.

Also, the points Q_{13} and $Q_9 = Q_{-11}$ are interchanged by M_1 and M_{11}. Hence, each arc of type $I(6;\epsilon_1,\cdots,\epsilon_d)$ is equivalent to an arc with a signature of the form $I(4;\epsilon_1',\cdots,\epsilon_d')$. □

Of course, as mentioned in the above example, 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 $\mathcal{C}$ as fixed. However, for a given arc S there could be several conical subsets that are large. Fortunately, we have the following

Lemma 3.8 *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*

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

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

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

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

Corollary 3.9 *If $q \geq 13$, 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 $e \leq 2$. Then by Lemma 3.8, any other conical subset must have excess $e' \geq (q+5)/2 - e - 4 \geq 9 - 2 - 4 = 3$. ∎

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

With this assumption, S determines $\mathcal{C}$ uniquely. Any isomorphism between any of the arcs listed in Theorem 3.7 must therefore leave $\mathcal{C}$ 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 H as defined in Lemma 3.4.

From Section 3.2 we know that the elements of H that fix Q_1 are the following :

$$\begin{array}{lcccccc} M_0' \text{ (the identity)} & : & P_j & \mapsto & P_j, & Q_j & \mapsto & Q_j, \\ M_r' & : & P_j & \mapsto & P_{j+r}, & Q_j & \mapsto & Q_j, \\ M_1 & : & P_j & \mapsto & P_{1-j}, & Q_j & \mapsto & Q_{2-j}, \\ M_{r+1} & : & P_j & \mapsto & P_{r+1-j}, & Q_j & \mapsto & Q_{2-j}. \end{array} \tag{3.3}$$

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 as $a \in \mathbb{Z}_r^*$). To enumerate all arcs up to isomorphism, it is therefore sufficient to consider only those a that satisfy $1 \leq a \leq r/2$.

We now consider the case where a is fixed.

Theorem 3.10 *Let $q \geq 13$, $a \in \{1,\ldots,r-1\}$ $d = \gcd(a,r)$ and $n = r/d$. Further, let H_a denote the subgroup of $\mathrm{PG}(3,q)$ that leaves the conic $\mathcal{C}$ 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' *(identity)*	$Z_k^{\pm}$	$I(a;\epsilon_1,\ldots,\epsilon_d)$	
M_r'	$Z_k^{\pm}$	$I(a;\epsilon_1,\ldots,\epsilon_d)$	*for n even,*
	$Z_{d+k}^{\pm} = Z_{d+1-k}^{\mp}$	$I(a;-\epsilon_d,\ldots,-\epsilon_1)$	*for n odd.*
M_{a+1}	$Z_{1-k}^{\pm} = Z_k^{\mp}$	$I(a;-\epsilon_1,\ldots,-\epsilon_d)$	*for a/d even,*
	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$	*for a/d odd.*
M_{a+r+1}	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$	*for n even, a/d odd,*
	$Z_{d+1-k}^{\pm}$	$I(a;\epsilon_d,\ldots,\epsilon_1)$	*for n odd, a/d even,*
	$Z_{1-k}^{\pm} = Z_k^{\mp}$	$I(a;-\epsilon_1,\ldots,-\epsilon_d)$	*for n odd, a/d 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 H. Any element of H_a must either fix the points Q_1 and Q_{2a+1} or interchange them.

From (3.3) we easily derive that the identity and M'_r will fix both points, and so will M_1 and M_{r+1} provided that $(2a+1) \equiv 2-(2a+1) \pmod{q+1}$, i.e., when $4a \equiv 0 \pmod{q+1}$, i.e., $a = r/2$.

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

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

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 $4a \equiv 0 \pmod{q+1}$, 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 $Z_k = k + 2d\mathbb{Z}_{q+1}$ is mapped to $k+i+2d\mathbb{Z}_{q+1} = Z_{k+i}$. Similarly, the reflection M_i maps k to $i-k$ and hence $Z_k = k + 2d\mathbb{Z}_{q+1}$ to $i-k-2d\mathbb{Z}_{q+1} = Z_{i-k}$.

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 $a \leq r/2$, as explained earlier.)

Example 3.2 For $q = 19$, $H_6 = \{M'_0, M'_{10}, M_7, M_{17}\}$. The cycles are fixed by M'_0. M'_{10} maps each cycle onto its opposite cycle. M_7 and M_{17} interchange $Z_1^{\pm}$ with $Z_2^{\pm}$. □

The group H_a in Theorem 3.10 contains precisely the projective equivalences that exist among the arcs listed in Theorem 3.7, 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 3.11 *Let $q \geq 13$. 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.*

Example 3.3 For $q = 19$, the arcs with signatures $I(6,+,+)$ and $I(6,-,-)$ have $\{M_0', M_7\}$ as stabilizer group. The arcs with signatures $I(6,+,-)$ and $I(6,-,+)$ have $\{M_0', M_{10}'\}$ as stabilizer group. □

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 3.12 *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*

$$I_q(a) = \begin{cases} 2^{d-2} + 2^{\lfloor \frac{d-2}{2} \rfloor}, & \text{when } \frac{q+1}{2d} \text{ is odd or } \frac{q+1}{2d} = 2, \\ 2^{d-1} + 2^{\lfloor \frac{d-1}{2} \rfloor}, & \text{when } \frac{q+1}{2d} \text{ is even and } \frac{q+1}{2d} \neq 2. \end{cases} \tag{3.4}$$

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 3.10 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 3.11.

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 3.11 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

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

■

Example 3.4 $I_{19}(6) = 2$. □

Theorem 3.13 *Let $q \geq 13$. The number I_q of projectively inequivalent arcs S in $\mathrm{PG}(2,q)$ of size $|S| = (q+5)/2$, with a conical subset $T = S \cap \mathcal{C}$ of size $|T| = (q+1)/2$ such that the elements of $S \setminus T$ are internal points of $\mathcal{C}$, 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 3.12.

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, $1 \leq a < r$ such that $d = \gcd(a,r)$ is equal to $\phi(r/d) = \phi(n)$. If we restrict ourselves to $a \leq r/2$ 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. ■

Example 3.5 For $q = 19$, the proper divisors d of $(q+1)/2$ are 1, 2 and 5 with corresponding values $\phi(r/d) = 4$, 4 and 1. With

$$I_{19}(1) = 2^0 + 2^0 = 2$$
$$I_{19}(2) = 2^0 + 2^0 = 2$$
$$I_{19}(5) = 2^3 + 2^1 = 10$$

we find

$$I_{19} = \frac{1}{2} \cdot 4 \cdot 2 + \frac{1}{2} \cdot 4 \cdot 2 + \lceil \frac{1}{2} \cdot 1 \rceil \cdot 10 = 18.$$

□

3.4 Arcs of type E with excess two

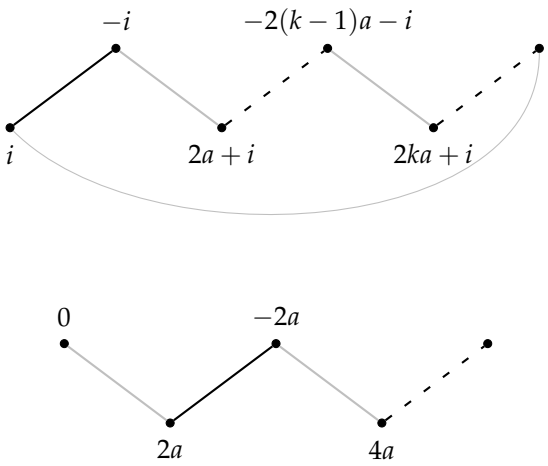
The arcs of type E are in many aspects very similar to those of type I in the previous section. We shall therefore mainly focus on the differences between both cases.

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 one of the supplementary points is Q_0 as all external points on ℓ lie in a single orbit of H. Let the other supplementary point be Q_{2a} for some $a \in \mathbb{Z}_r, a \neq 0$. The tangent points for Q_0 are P_0 and P_r, and those of Q_{2a} are P_a and P_{a+r} (by Lemma 3.3).

Consider the graph $\Gamma = \Gamma(\mathcal{C}, U) = \Gamma(\mathcal{C}, \{Q_0, Q_{2a}\})$. 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 (possibly zero) cycles. We may enumerate the vertices of the cycle or path that contains i as follows:

$$\ldots, i, -i, 2a+i, -2a-i, 4a+i, -4a-i, \ldots \tag{3.5}$$



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 (3.5) 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 (3.5) denotes a cycle, and not a path. The cycle either has length $2n$ with $i \equiv 2na+i \pmod{q+1}$, or length $2n+1$ with $i \equiv -2na-i \pmod{q+1}$. 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 $\pm i \pmod{d}$.

Also, if (3.5) 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 d. The following lemma provides further information on the composition of these paths.

Lemma 3.14 *The two paths that are components of Γ each contain n vertices.*

The end points 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 end points. 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 $(2k'-1)a = 0 \pmod{q+1}$ or $(2k'-1)2a = 0 \pmod{q+1}$ 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 $(2k''-1)2a = 2r = 0 \pmod{q+1}$ 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 $(a - i) + (a - j) = 0$. So adjacent points are mapped onto adjacent points. Hence, this map 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 end points). ∎

This provides us with the analogue of Lemma 3.6 :

Lemma 3.15 *If S is an arc of type E with supplementary points Q_0 and Q_{2a}, then $\Gamma(\mathcal{C}, S \setminus \mathcal{C})$ 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 3.3, we introduce the half cycles $Z_k \stackrel{\text{def}}{=} k + 2a\mathbb{Z}_{q+1} = k + 2d\mathbb{Z}_{q+1}$. 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 3.16 *Let $a \in \{1, \ldots, r - 1\}$. Let $d = \gcd(a, r)$, $n = r/d$. Let $S = T \cup \{Q_0, Q_{2a}\}$, with $T \subset \mathcal{C}$ 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 the union of pairwise disjoint sets, 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 [14] corresponds to the special case $n = 3$ of this result.)

Corollary 3.17 *When $q+1$ is a power of 2 there are no arcs of type E with excess larger than 1.*

Proof : Indeed, n divides r and hence also $q+1$, so n is even if $q+1$ is a power of 2. ∎

We shall identify the arcs in Theorem 3.16 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 $Z_{\pm k}$.

Example 3.6 For $q = 19$ and $a = 6$ ($n = 5$ and $a/d = 3$ are odd), we have two paths and one cycle:

$$0, 12, 8, 4, 16$$
$$10, 2, 18, 14, 6$$
$$1, 19, 13, 7, 5, 15, 17, 3, 9, 11, 1$$

with

$$\Pi = \{0, 8, 16\} \qquad \Pi' = \{10, 18, 6\}$$
$$Z_1 = \{1, 13, 5, 17, 9\} \quad Z_{-1}\{19, 7, 15, 3, 11\}$$

Hence, there are two arcs S of type E of size 13 with $S \setminus T = \{Q_1, Q_{12}\}$. These are the arcs with signatures $E(6, +)$ and $E(6, -)$. Note that they are equivalent. □

As before, we shall now determine what isomorphisms exist between arcs of this type. Lemma 3.8 in this case has the following

Corollary 3.18 *If $q \geq 11$, 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.*

Proof : Assume S has a conical subset T with excess $e \leq 2$. Then by Lemma 3.8, any other conical subset must have excess $e' \geq (q+7)/2 - e - 4 \geq 9 - 2 - 4 = 3$. ∎

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

From Section 3.2 we obtain the elements of H that fix Q_0 :

$$\begin{array}{lcccccc} M_0' \text{ (the identity)} & : & P_j & \mapsto & P_j, & Q_j & \mapsto & Q_j, \\ M_r' & : & P_j & \mapsto & P_{j+r}, & Q_j & \mapsto & Q_j, \\ M_0 & : & P_j & \mapsto & P_{-j}, & Q_j & \mapsto & Q_{-j}, \\ M_r & : & P_j & \mapsto & P_{r-j}, & Q_j & \mapsto & Q_{-j}. \end{array} \tag{3.6}$$

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.

Example 3.7 For $q = 19$, the points Q_{12} and $Q_8 = Q_{-12}$ are interchanged by M_0 and M_{10}. □

Theorem 3.19 *Let $q \geq 11$, $a \in \{1, \ldots, r-1\}$ $d = \gcd(a,r)$ and $n = r/d$. Further, let H_a denote the subgroup of $\mathrm{PG}(3,q)$ that leaves the conic $\mathcal{C}$ 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 (3.6) 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 3.14 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 $M_{a+r} = M_a M'_r$. ∎

Example 3.8 For $q = 19$, $H_6 = \{M'_0, M'_{10}, M_6, M_{16}\}$. The paths are fixed by M'_0 and M_{16} and interchanged by the other two. The half cycles are fixed by M'_0 and M_6 and interchanged by the other two mappings. □

Corollary 3.20 *Let $q \geq 11$. 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 $H_S = \{M_0', M_r', M_a, M_{a+r}\} = H_a$.

Example 3.9 For $q = 19$ and $a = 6$, both arcs $E(6,+)$ and $E(6,-)$ have $\{M_0', M_6\}$ as stabilizer group. □

Lemma 3.21 *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*

$$E_q(a) = \begin{cases} 1, & \text{when } d = 1, \\ 2^{d-3} + 2^{\lfloor \frac{d-3}{2} \rfloor}, & \text{when } d > 1. \end{cases} \tag{3.7}$$

Proof : As in the proof of Lemma 3.12, 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

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

■

Example 3.10 $E_{19}(6) = 1$. □

And using an argument similar to that of Section 3.3, this yields

Theorem 3.22 *Let $q \geq 11$. The number E_q of projectively inequivalent arcs S in $\mathrm{PG}(2,q)$ of size $|S| = (q+7)/2$, with a conical subset $T = S \cap \mathcal{C}$ of size $|T| = (q+3)/2$ such that the elements of $S \setminus T$ are external points of $\mathcal{C}$, 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 3.21.

Proof: The total number of inequivalent arcs is given by $\sum_{a=1}^{r} E_q(a)$. Note that $E_q(a)$ does not directly depend on a, but only on $d = \gcd(a,r)$. The number of integers a, $1 \leq a < r$ such that $d = \gcd(a,r)$ is equal to $\phi(r/d) = \phi(n)$. If we restrict ourselves to those a with a/d odd, we obtain $\phi(n)/2$ values. ■

Example 3.11 For $q = 19$, the proper divisors d of $(q+1)/2$ are 1, 2 and 5. Only for $d = 2$ we have that $(q+1)/2d$ is odd and then $\phi(r/d) = \phi(5) = 4$ With

$$E_{19}(2) = 2^{-1} + 2^{\lceil \frac{-1}{2} \rceil} = 1$$

we find

$$E_{19} = \frac{1}{2} \cdot 4 \cdot 1 = 2.$$

□

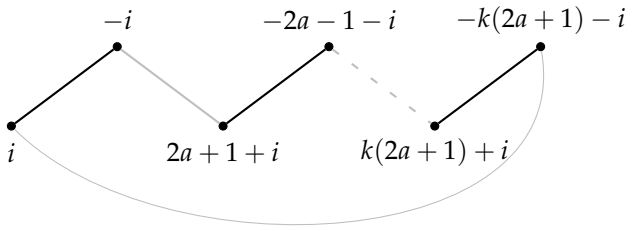
3.5 Arcs of type M with excess two

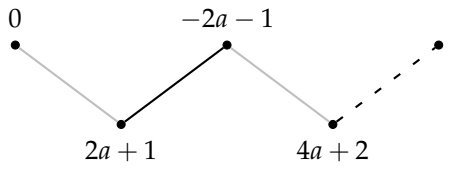
Again, in many respects the arcs of type M are similar to those of type I and type E from the previous sections, and therefore again we will focus mainly on the differences.

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 $a \in \mathbb{Z}_r$. Every vertex of the graph $\Gamma = \Gamma(\mathcal{C}, S \setminus \mathcal{C})$ 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 $\pm i$ mod $2a+1$, and using similar arguments as in the previous section, we may conclude

Lemma 3.23 *If S is an arc of type M with supplementary points Q_0 and Q_{2a+1}, then $\Gamma(\mathcal{C}, S \setminus \mathcal{C})$ 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., $f = \gcd(2a+1, q+1)$.*

Proof : A cycle has either length $2m$ with $i \equiv m(2a+1) \pmod{q+1}$ or length $2m+1$ with $i \equiv -m(2a+1) - i \pmod{q+1}$. The latter case is again 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, each cycle has length $2m$ and m is equal to the order of $2a+1 \pmod{q+1}$, i.e. m is the smallest positive integer such that $m(2a+1) \equiv 0 \pmod{q+1}$. Note that m is independent of i and therefore all cycles have the same size.

The path has endpoints 0 and r. Hence, the point r must be a multiple of (2a+1), say $r \equiv (2a+1)k \pmod{q+1}$ for some k. k can alwyas be chosen to satisfy $0 < k < m$. We have $2(2a+1)k \equiv 2r \equiv 0 \pmod{q+1}$ and hence $2k$ must be a multiple of the order of $(2a+1) \pmod{q+1}$, which is m. Because $0 < k < m$, this is only possible when $m = 2k$, hence m must be even. Note that the path contains all vertices that are multiple of $2a+1$ and hence has size m.

As each cycle has length $2m$ and the path has size m, there are $\frac{q+1-m}{2m} = \frac{f-1}{2}$ cycles. ∎

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

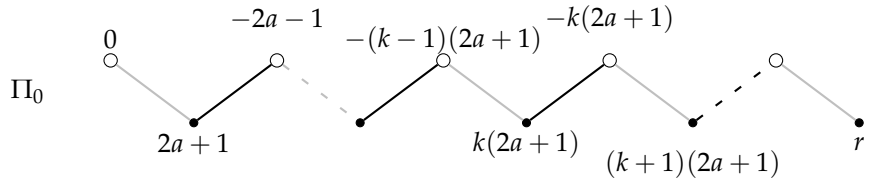
It also follows that $N(T)$ is a union of half cycles $Z'_k \stackrel{\text{def}}{=} k + (2a+1)\mathbb{Z}_{q+1} = k + f\mathbb{Z}_{q+1}$ and one *half path*, i.e., an independent set of size $m/2$ in the path that joins 0 and r.

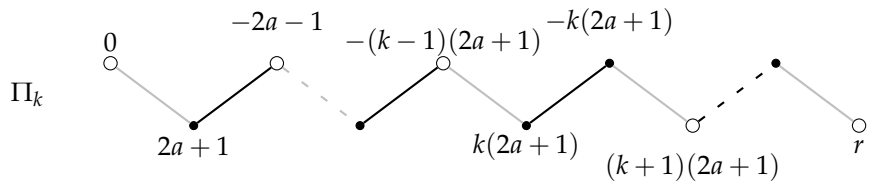
There are exactly $m/2+1$ half paths, which we will denote by Π_k with $k = 0, \ldots, m/2$. We have

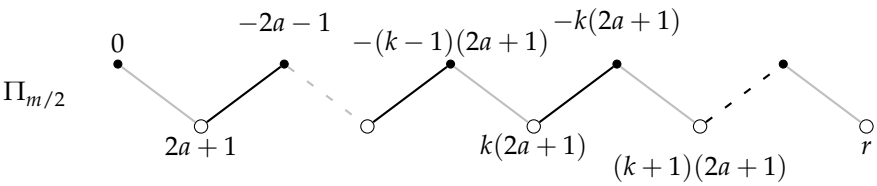
$$\Pi_k \stackrel{\text{def}}{=} \{0, -2a-1, -2(2a+1), \ldots, -(k-1)(2a+1)\} \cup \{(k+1)(2a+1), \ldots, r\},$$

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 3.24 *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 $T \subset \mathcal{C}$ 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 the union of pairwise disjoint sets, 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 $Z'_{\pm k}$.

Example 3.12 Again consider the Galois Field $\mathbb{F}_{19}$. We find the following table for the values of a, m and f:

a	m	f
1,3,4,5,6,8,9	20	1
2,7	4	5

For $a = 2$, we have one path and two cycles:

$$0, 5, 15, 10$$

$$1, 4, 16, 9, 11, 14, 6, 19, 1$$

$$2, 18, 7, 13, 12, 8, 17, 3, 2$$

with

$$\Pi_0 = \{5, 10\}, \quad \Pi_1 = \{0, 10\}, \quad \Pi_2 = \{0, 15\}$$

$$Z'_1 = \{1, 16, 11, 6\} \quad Z'_{-1} = Z_{19} = \{4, 9, 14, 19\}$$
$$Z'_2 = \{2, 7, 12, 17, \} \quad Z_{-2} = Z_{18}\{18, 13, 8, 3\}$$

Hence, there are twelve arcs S of type M of size 12 with $S \setminus T = \{Q_0, Q_5\}$. These are the arcs with signatures

$$M(2,0,+,+) \quad M(2,0,+,-) \quad M(2,0,-,+) \quad M(2,0,-,-)$$
$$M(2,1,+,+) \quad M(2,1,+,-) \quad M(2,1,-,+) \quad M(2,1,-,-)$$
$$M(2,2,+,+) \quad M(2,2,+,-) \quad M(2,2,-,+) \quad M(2,2,-,-).$$

Note that some of these arcs are equivalent. □

As before, we shall now determine what isomorphisms exist between arcs of this type. Among the elements of H 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 $a \in \{0,1,\ldots,\lfloor (r-1)/2 \rfloor\}$.

Example 3.13 For $q = 19$, the points Q_5 and $Q_{-5} = Q_{15}$ are interchanged by M_0 and M_{10}. □

Theorem 3.25 *Let $q \geq 13$, 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 $\mathcal{C}$ 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 $\mathcal{C}$, 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 H 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

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

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 $0 \le a \le \lfloor (r-1)/2 \rfloor$, as explained earlier.

Example 3.14 For $q = 19$, $H_2 = \{M'_0, M'_{10}\}$. □

Corollary 3.26 *Let $q \ge 13$. 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 $m \ne 2$, then*

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

Example 3.15 For $q = 19$, the arcs with signatures $M(2,0,\pm,\pm)$ and $M(2,2,\pm,\pm)$ have $\{M'_0\}$ as stabilizer group. The arc with signatures $M(2,1,\pm,\pm)$ has $\{M'_0, M'_{10}\}$ as stabilizer group. □

Lemma 3.27 *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*

$$M_q(a) = \begin{cases} 2^{h-1}, & \text{when } h = (q-1)/4, \\ (\lfloor \frac{q+1}{4(2h+1)} \rfloor + 1)2^h, & \text{when } h < (q-1)/4, \end{cases} \tag{3.8}$$

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

Example 3.16 $M_{19}(2) = 8$. □

Theorem 3.28 *Let $q \geq 13$. The number M_q of projectively inequivalent arcs S in $\mathrm{PG}(2,q)$ of size $|S| = (q+5)/2$, with a conical subset $T = S \cap \mathcal{C}$ of size $|T| = (q+1)/2$ such that $S \setminus T$ consists of an internal and an external point of $\mathcal{C}$, 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 3.27.

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. But then $\phi((q+1)/(2h+1)) = \phi(2) = 1$ and hence $\lceil \frac{1}{2}\phi(n) \rceil = 1$. ∎

Example 3.17 For $q = 19$, the proper odd divisors $2h+1$ of $q+1$ are 1 and 5 and $(q+1)/(2h+1)$ is even in both cases. The corresponding values $\phi((q+1)/(2h+1))$ are $\phi(20) = 8$ and $\phi(4) = 2$. With

$$M_{19}(0) = (5+1)2^0 = 6$$
$$M_{19}(2) = (1+1)2^2 = 8$$

we find

$$M_{19} = \frac{1}{2} \cdot 8 \cdot 6 + \frac{1}{2} \cdot 2 \cdot 8 = 24 + 8 = 32.$$

□

3.6 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 [24] 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 $\mathcal{C}$. 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 $T = \mathcal{C} \cap S$ as before. We shall use the following criterion to determine whether S is an arc.

Lemma 3.29 *Let T be a subset of a conic $\mathcal{C}$ of size $|T| = (q+1)/2$. Let U be a set of internal points of $\mathcal{C}$. 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 $\mathcal{C}$,*
- *$\sigma_Q(T) = C \setminus T$ for all points Q of U,*

with σ_Q as defined in Section 3.2.

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 $\mathcal{C}$ 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 $\mathcal{C}$, 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 $\mathcal{C}$, 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 3.30 *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 3.10 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} is the line $[1,-2/t_{2a+1},\beta]$ and intersects ℓ in Q_{2a+1+r}. Because Q_{2a+1+r} lies on the polar line of Q_{2a+1} and on the polar line of R, the polar line of Q_{2a+1+r} is the line RQ_{2a+1}. $RQ_{2a+1}$is an external line if and only if its pole Q_{2a+1+r} is an internal point which is the case if and only if r is even.

Similarly, also RQ_1 is an external line if and only if r is even.

From Lemma 3.29 the claim follows. ∎

Define $\hat{\Delta}_T$ to be the group of all projectivities 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 3.31 *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 $|T| = (q+1)/2 \equiv 1/2 \pmod{p}$, 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 [6, Theorem 2] for example. The subgroups of $\mathrm{PGL}(2,q)$ that satisfy Lemma 3.31 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 3.32 *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 3.33 *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 3.30*

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, instead of the standard conic, we shall use $X^2 + Y^2 + Z^2 = 0$ as the equation of $\mathcal{C}$ 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 $\mathcal{C}$.) 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. $(x, y, z) \mapsto (y, x, -z)$ is an example of such an involution. The corresponding point Q of this involution is the intersection point of the $(q + 1)/2$ lines PP' through the points $P(a, b, c)$ and $P(b, a, -c)$, $a, b, c \in \mathbb{F}_q$. These lines have equation $-c(a + b)X + c(a + b)Y + (a^2 + b^2)Z = 0$, their intersection point Q is the point with coordinates$(1, 1, 0)$.

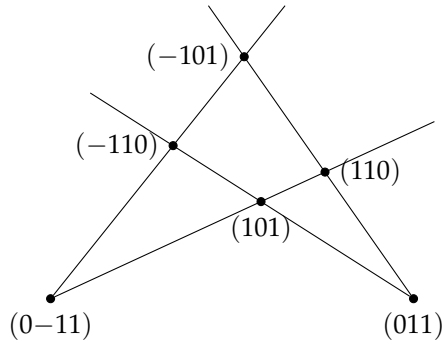
The other points corresponding to the involutions are the the images of Q through S_4, i.e. $(\pm 1, \pm 1, 0)$, $(0, \pm 1, \pm 1)$ and $(\pm 1, 0, \pm 1)$. (Note that changing the sign of both non-zero coordinates does not change the point itself.)

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

$$\begin{array}{lcllcl} Q & = & (1,-1,0), & \sigma_Q(x,y,z) & = & (y,x,z) \\ Q' & = & (1,1,0), & \sigma_{Q'}(x,y,z) & = & (y,x,-z) \\ Q'' & = & (1,0,-1), & \sigma_{Q''}(x,y,z) & = & (z,y,x) \\ Q''' & = & (1,0,1), & \sigma_{Q'''}(x,y,z) & = & (z,-y,x) \end{array} \tag{3.9}$$

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

In view of Lemma 3.29 we will investigate the conditions for a candidate point to be an internal point of $\mathcal{C}$, and for a line joining two candidate points to be external to $\mathcal{C}$.

Lemma 3.34 *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* $\mathcal{C}$ *with equation* $X^2+Y^2+Z^2=0$ *if and only if* $q\equiv 5$ *or* $7 \pmod 8$.

The line with equation $X=0$ *(and similarly* $Y=0$ *or* $Z=0$*) is an external line of* $\mathcal{C}$ *if and only if* $q\equiv 3 \pmod 4$.

A line with an equation of the form $Z=\pm X\pm Y$ *is an external line of* $\mathcal{C}$ *if and only if* $q\equiv 5 \pmod 6$.

Proof : Consider a point Q with coordinates $(1,\pm1,0)$. (The other cases will be left to the reader.) This point is internal to $\mathcal{C}$ if and only if its polar line is external to $\mathcal{C}$. 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 $\mathbb{F}_q$, 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 $\mathbb{F}_q$. 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 $\mathbb{F}_q$.

When p is a prime, -2 is a square modulo p if and only if $p\equiv 1$ or $3 \pmod 8$. When $q=p^h$ with h even, every element of the prime field is a square, but then also $q\equiv 1 \pmod 8$. When h is odd, -2 is a square in $\mathbb{F}_q$ if and only if it is a square modulo p, but in that case also $q\equiv p \pmod 8$. Hence, for general odd q, -2 is a square in $\mathbb{F}_q$ if and only if $q\equiv 1$ or $3 \pmod 8$. As a consequence, the point Q is internal if and only if $q\equiv 5$ or $7 \pmod 8$.

Similarly, -1 is a square if and only if $q\equiv 1 \pmod 4$ and -3 is a square if and only if $q\equiv 1 \pmod 6$ or $q\equiv 0 \pmod 3$. ∎

Lemma 3.35 *Let* $q\equiv -1 \pmod{24}$. *Then* S_4 *acts semiregularly on* $\mathcal{C}$ *(i.e., every orbit has size* 24*).*

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

1. σ is an involution of $S_4 \setminus A_4$. Then $\sigma = \sigma_Q$ for one of the 'candidate points' Q discussed above. By Lemma 3.34 Q must be an internal point and then σ_Q cannot have fixed points on $\mathcal{C}$.

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

3. σ has order 3. Take $\sigma(x, y, z) = (y, z, x)$. A fixed point of σ 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 $\mathbb{F}_q$.

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

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

Lemma 3.36 *Let $q \equiv -1 \pmod{24}$. Let $d = (q+1)/24$. Let $O_1, \ldots, O_d$ denote the orbits of S_4 on $\mathcal{C}$. For $i = 1, \ldots, d$ write $O_i = O_i^+ \cup O_i^-$, where $O_i^\pm$ are orbits of A_4 on $\mathcal{C}$.*

Then

$$S \stackrel{\text{def}}{=} O_1^\pm \cup \cdots \cup O_d^\pm \cup \{Q, Q', Q'', Q'''\}, \tag{3.10}$$

for any choices of signs, is an arc of type I and excess 4 (with Q, Q', Q'', Q''' as defined in (3.9)).

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

Theorem 3.37 *An arc in* $\mathrm{PG}(2,q)$ *of type I can have at most excess 4. If the excess is 4 then* $q \equiv -1 \pmod{24}$ *and the arc is as described in Lemma 3.36.*

Theorem 3.38 *Let* $q \equiv -1 \pmod{24}$. *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 3.36 all arcs of this type are equivalent to one of the form (3.10), 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 $\mathcal{C}$ 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 $\mathcal{C}$ invariant:

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

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 $S^- = (\mathcal{C} \setminus T) \cup U$ 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. ∎

3.7 Arcs with excess one

In this section we regard the arcs of type I and E with excess one (type M has excess at least two).

First, consider the arcs of type E with excess one.

Lemma 3.39 *The subgroup H of $\mathrm{PGL}(2,q)$ that leaves both the conic $\mathcal{C}$ and an external point invariant, is isomorphic to the dihedral group of order $2(q-1)$ consisting of the following elements:*

$$\begin{cases} N_k : t \mapsto kt, \\ N'_k : t \mapsto k/t, \end{cases} \tag{3.11}$$

with $k \in \mathbb{F}_q^*$ and $t \in \mathbb{F}_q \cup \{\infty\}$.

Proof : We may without loss of generality assume that the external point is $Q_0(0,1,0)$. Its tangent points are $P_0(1,0,0)$ and $P_r(0,0,1)$.

The group that stabilizes the conic $\mathcal{C}$ and the point Q_0 is equal to the group that stabilizes the conic and the polar line P_0P_r of Q_0. Hence, H consists of all matrices of the form (2.2) that stabilize the points P_0 and P_r or interchanges

them. In the first case, we find $c = 0$ and $b = 0$ and hence the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & d/a & 0 \\ 0 & 0 & d^2/a^2 \end{pmatrix}$$

In the second case we find $a = 0$ and $d = 0$ and hence the matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & c/b & 0 \\ c^2/b^2 & 0 & 0 \end{pmatrix}.$$

These are exactly the mappings of (3.11), but here in terms of matrices. ∎

Because an arc of type E with excess one contains exactly one conic point on each of its $(q-1)/2$ secants through the external point, there are $2^{(q-1)/2}$ different arcs of type E with the same supplementary point. Among these arcs some are equivalent. This equivalence depends on the choice of the points on the secants. The stabilizer group of such an arc always is a subgroup of the dihedral group of order $2(q-1)$. Because the number of possible subgroups is large, we did not attempt to classify them.

Arcs among these with a lot of symmetry are those with the stabilizer group isomorphic to the dihedral group of order $q-1$ consisting of those elements N_k, N'_k for which k is a square in $\mathbb{F}_q^*$. An example of such an arc is the arc consisting of Q_0, P_0, P_r and the points with coordinates $(1, t, t^2)$ with t a square in $\mathbb{F}_q^*$.

Secondly, consider the arcs of type I with excess one.

Lemma 3.40 *The subgroup H of $\mathrm{PGL}(2,q)$ that leaves both the conic $\mathcal{C}$ and an internal point invariant, is isomorphic to the dihedral group of order $2(q+1)$ consisting of the following elements:*

$$\begin{cases} M_i : P_j \mapsto P_{i-j}, \\ M'_i : P_j \mapsto P_{j+i}, \end{cases} \tag{3.12}$$

with $i \in \mathbb{Z}_{q+1}$.

Proof : The group that stabilizes the conic $\mathcal{C}$ and an internal point is equal to the group that stabilizes the conic and the corresponding polar line, which is external. Hence, we can apply Lemma 3.4. ∎

For similar reasons as for arcs of type E, there are $2^{(q+1)/2}$ different arcs of type I with the same supplementary point and again, some of them are equivalent.

When $(q+1)/2$ is odd, arcs with a lot of symmetry are those with stabilizer group isomorphic to a dihedral group of order $q+1$ consisting of the elements M_i, M_i' with i even. An example of such an arc is the arc consisting of the internal point R with coordinates $(-\beta, 0, 1)$ and the points P_j, with j even.

The arcs of type E with excess one are also discussed in [39], those of type I are discussed in [23].

3.8 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 3.2 and 3.3 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 3.13, 3.22 and 3.28, while N_i denotes the number of (inequivalent) *incomplete* arcs with excess two, as found by computer.

By Corollaries 3.9 and 3.18, 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.

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

Table 3.1: Number of inequivalent complete arcs of type E in PG$(2, q)$ of excess at least three.

In Table 3.1 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 [25], and although we managed to investigate larger values of q, we did not find any new examples.

In Table 3.4 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 3.6. The arcs in the last two columns are of type M.

Finally in Table 3.5 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 3.4, as obviously (containing two internal points) these arcs can also be constructed from an arc of type I and excess two.

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
131	2148567242	1043	524860	0	132248	0

Table 3.2: Number of inequivalent large arcs of types I, E and M in PG$(2, q)$, $q \leq 131$.

q	type I		type E		type M	
	N_a	N_i	N_a	N_i	N_a	N_i
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 3.3: Number of inequivalent large arcs of types I, E and M in PG$(2, q)$, $131 < q < 256$.

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

q	1 int. pt, 2 ext. pts	2 int. pts, 1 ext. pt	2 int. pts, 2 ext. pts	1 int. pt, 3 ext. pt	1 int. pt, 7 ext. 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 3.5: Number of inequivalent complete arcs of type M in $\mathrm{PG}(2,q)$ of excess at least three.

4

Generation of $(k,2)$- and $(k,3)$-arcs

In this chapter we describe the algorithms that are used to find a full classification (up to equivalence) of all complete $(k,2)$-arcs and $(k,3)$-arcs in PG$(2,q)$. The algorithms used are an application of isomorph-free backtracking using canonical augmentation which we have adapted to the case of subset generation in projective planes. The results of the algorithms are described in Chapters 5, 6 and 7.

4.1 Isomorph-free generation

The natural way to generate all complete arcs of a given (finite) projective plane is to use a backtracking algorithm which recursively generates every $(k+1)$-arc S' from a k-arc S such that $S \subseteq S'$. At each step in the recursion

a point s is taken which does not belong to S and S' is set equal to $S \cup \{s\}$. Typically, to avoid generating every arc more than once, the points of the projective plane are numbered in a certain way, and a point s is added to S only if it has a sequence number larger than that of any point of S. Also s is only added when it does not lie on a bisecant of S, and if for a given S no such s can be found, S is checked for completeness.

In most applications we do not seek to generate every single complete arc, but only one arc for each equivalence class, i.e., one representative of each orbit of $G = \mathrm{P\Gamma L}(3,K)$ (or $\mathrm{PGL}(3,K)$). It is well known that filtering out equivalent arcs at the end of the standard generation process, or even after all arcs of a given size have been generated, is simply too costly in time and memory. In our programs we have instead used a technique for isomorph-free generation called *canonical augmentation* which was developed by B. McKay [35]. For further details we refer the reader to that paper, or to [21, Section 4.2.3] which gives a comprehensive description of these methods in the setting of codes and designs.

4.1.1 Canonical augmentation

Let V denote a finite set of size $|V| = n$ and let G denote a group with a right action on V. In our case V is the set of points of $\mathrm{PG}(2,q)$ and G is $\mathrm{PGL}(3,q)$ or $\mathrm{P\Gamma L}(3,q)$, but the algorithms below work in a more general setting.

If H is a subgroup of G, then the partition of V into orbits of H is denoted by $H\backslash\backslash V$. We define the *base size* of an orbit S^H to be the size $|S|$ of one (and hence of all) of its representatives.

An orbit $\mathcal{O}' = S'^G$ is said to *augment* an orbit $\mathcal{O}$ if and only if S' can be written as $S' = S \cup \{s\}$ with $s \notin S$ and $S \in \mathcal{O}$. In other words, $\mathcal{O}'$ augments $\mathcal{O}$ if a representative of $\mathcal{O}'$ (and hence every representative) can be obtained from a representative of $\mathcal{O}$ by adding a single element of V. In that case the base size of $\mathcal{O}'$ will be one larger than the base size of $\mathcal{O}$.

Algorithms 1 and 2 which we shall describe below can be used to generate,

up to equivalence, all subsets S that satisfy a certain property $\mathsf{P}(S)$, where P is a set predicate with the following characteristics:

1. P is *group invariant*: $\mathsf{P}(S)$ if and only if $\mathsf{P}(S^g)$, for every $S \subseteq V$ and $g \in G$;
2. P is *hereditary*: if $\mathsf{P}(S)$ then $\mathsf{P}(S')$ for every subset S' of S.

Because P is group invariant, we may also regard P as a predicate on set orbits. In other words, if $\mathcal{O} \in G\backslash\backslash 2^V$ (2^V is the set of all subsets of V), then we write $\mathsf{P}(\mathcal{O})$ if and only if $\mathsf{P}(S)$ holds for some $S \in \mathcal{O}$ (and then for all $S \in \mathcal{O}$).

Algorithms 1 and 2 take as input a set of orbits $\mathcal{A}_{\text{in}} \subseteq G\backslash\backslash 2^V$ that satisfy P. They generate as output a set $\mathcal{A}_{\text{out}} \subseteq G\backslash\backslash 2^V$ of orbits that augment elements of $\mathcal{A}_{\text{in}}$. In the following section, we prove that if we initialize $\mathcal{A}_{\text{in}}$ to contain all orbits of a fixed base size k that satisfy P, we will end up with te set $\mathcal{A}_{\text{out}}$ of all orbits of base size $k+1$ that satisfy P. Hence, to generate *all* orbits that satisfy P, we start with $\mathcal{A}_{\text{in}} = \{\emptyset\}$ and iterate the algorithm to generate all orbits of subsequent base sizes. In this way we finally obtain all orbits that satisfy P.

In practice it is not always necessary to start from the empty set and to avoid having to store the sets $\mathcal{A}_{\text{out}}$ at each stage it is better to convert the breadth-first search which we describe here to an equivalent depth-first search. Also, instead of working with orbits directly, we represent each orbit by a single representative.

The algorithms make use of a special function $F : 2^V \to 2^V$ which needs to be chosen carefully (and whose choice depends on the particular problem). We shall however postpone the precise definition of F to Section 4.2.3. For now we only list the properties F is required to satisfy to make the algorithms work.

1. For all S, $S \subseteq V$, $S \neq \emptyset$, we have $F(S) \in G_S\backslash\backslash S$,
2. For all $S \subseteq V$, $g \in G$, we have $F(S^g) = F(S)^g$.

Note that $G_{S^g} \backslash\backslash S^g = (G_S \backslash\backslash S)^g$, and hence both requirements do not contradict each other. Also, it follows immediately that $F(S)^h = F(S)$ for all $h \in G_S$.

Informally, F singles out a *special orbit* of G_S in S, for every S.

4.1.2 The algorithms

Algorithm 1 provides a first method for isomorph-free generation of sets using the technique of canonical augmentation. Lemmas 4.1 and 4.2 below show

Algorithm 1 Isomorph-free generation

Input: $\mathcal{A}_{\text{in}} \subseteq G \backslash\backslash 2^V$
Output: $\mathcal{A}_{\text{out}} \subseteq G \backslash\backslash 2^V$
1: $\mathcal{A}_{\text{out}} = \emptyset$
2: **for all** $\mathcal{O} \in \mathcal{A}_{\text{in}}$ **do**
3: Choose $S \in \mathcal{O}$ ❶
4: **for all** $O \in G_S \backslash\backslash (V \setminus S)$ **do**
5: Choose $s \in O$ ❷
6: $S' \leftarrow S \cup \{s\}$
7: **if** $\mathsf{P}(S')$ and $s \in F(S')$ **then**
8: Add S'^G to $\mathcal{A}_{\text{out}}$ ❸
9: **end if**
10: **end for**
11: **end for**

that the resulting set $\mathcal{A}_{\text{out}}$ is independent of the choices of orbit representatives made at statements ❶ and ❷, and hence that the algorithm is well-defined.

Lemma 4.1 *The result of Algorithm 1 is independent of the choice of the representative s of the orbit O at statement ❷.*

Proof : Assume we choose $\bar{s} \in O$ instead of s. Then $\bar{s} = s^h$ for some $h \in G_S$ and

hence on line 6 we obtain $\overline{S'} = S \cup \{\bar{s}\}$ instead of S'. We have $\overline{S'} = S \cup \{\bar{s}\} = S^h \cup \{s^h\} = (S \cup \{s\})^h = S'^h$, and hence $\mathsf{P}(\overline{S'})$ holds if and only if $\mathsf{P}(S')$ does. Likewise, $s \in F(S')$ if and only if $\bar{s} = s^h \in F(S')^h = F(S'^h) = F(\overline{S'})$. It follows that statement ❸ will be executed for $\overline{S'}$ if and only if it would be executed for S', and because $\overline{S'}^G = S'^{hG} = S'^G$, in both cases exactly the same element is added to $\mathcal{A}_{\text{out}}$. ∎

Lemma 4.2 *The result of Algorithm 1 is independent of the choice of the representative S of the orbit $\mathcal{O}$ at statement ❶.*

Proof : Assume we choose $\bar{S} \in \mathcal{O}$ instead of S. Then $\bar{S} = S^g$ for some $g \in G$. The set of orbits O traversed by the loop on line 4 is now $G_{\bar{S}} \backslash\backslash (V \setminus \bar{S}) = G_{S^g} \backslash\backslash (V \setminus S^g) = G_S^g \backslash\backslash (V \setminus S)^g = (G_S \backslash\backslash (V \setminus S))^g$.

Hence, for every O which we encounter for the original choice of S, we now obtain a new element $\bar{O} = O^g$. The element chosen on line 5 can now be written as $\bar{s} = s^g \in \bar{O}$, and on line 6, S' is replaced by $\overline{S'} = S^g \cup \{s^g\} = S'^g$. As in the proof of Lemma 4.1 we have $\mathsf{P}(S')$ if and only if $\mathsf{P}(\overline{S'})$ and $s \in F(S')$ if and only if $\bar{s} \in F(\overline{S'})$. It again follows that statement ❸ will be executed for $\overline{S'}$ if and only if it would be executed for S' with the original choice of S. And again $\overline{S'}^G = S'^{gG} = S'^G$. ∎

We are now ready to prove that Algorithm 1 indeed does what we expect of it.

Theorem 4.3 *Let $k \in \{1, \ldots, |V| - 1\}$. If $\mathcal{A}_{\text{in}}$ is initialized to the set of all orbits $\mathcal{O}$ of base size k such that $\mathsf{P}(\mathcal{O})$, then Algorithm 1 terminates with $\mathcal{A}_{\text{out}}$ equal to the set of all orbits $\mathcal{O}'$ of base size $k+1$ such that $\mathsf{P}(\mathcal{O}')$.*

Moreover, statement ❸ of Algorithm 1 is executed at most once for every such $\mathcal{O}'$.

Proof : We need to prove that statement ❸ of Algorithm 1 is executed exactly

once for every orbit $\mathcal{O}' = S'^G$ that satisfies $\mathsf{P}(\mathcal{O}')$ and such that $|S'| = k+1$.

Let $\mathcal{O}'$ denote an orbit of this type, and let $T' \in \mathcal{O}'$. From $\mathsf{P}(\mathcal{O}')$ it follows that $\mathsf{P}(T')$ (by definition). Let $t \in F(T')$ and define $T = T' \setminus \{t\}$. Note that $|T| = k$ and because P is hereditary, that $\mathsf{P}(T)$. Hence $T^G \in \mathcal{A}_{\text{in}}$ and therefore $\mathcal{O} = T^G$ is one of the orbits that will be considered by the loop of line 2.

By Lemma 4.2 we may without loss of generality choose $S = T$ in statement ❶. When $O = t^{G_T}$ (which is certainly considered by the loop at line 4, as $t \in V \setminus T$) we may without loss of generality choose $s = t$ in statement ❷, by Lemma 4.1. In this case $S' = T'$, $\mathsf{P}(S')$ is satisfied and also $s \in F(S')$, and therefore $S'^G = T'^G = \mathcal{O}'$ is added to $\mathcal{A}_{\text{out}}$ in statement ❸. Hence, statement ❸ is called at least once for each of the orbits $\mathcal{O}'$ of the requested type.

Now assume that statement ❸ is called for $\mathcal{O}'$ in two different occasions, say for $\mathcal{O}' = {S'_1}^G$ and for $\mathcal{O}' = {S'_2}^G$. Because S'_1 and S'_2 are representatives of the same orbit, there exists $g \in G$ such that $S'_1 = {S'_2}^g$. Lines 6 and 7 of the algorithm imply that

$$\begin{aligned} S'_1 &= S_1 \cup \{s_1\} \quad \text{for some } s_1 \in F(S'_1), \\ S'_2 &= S_2 \cup \{s_2\} \quad \text{for some } s_2 \in F(S'_2). \end{aligned}$$

Now $F(S'_1) = F({S'_2}^g) = F(S'_2)^g$ and therefore both s_1 and s_2^g belong to $F(S'_1)$, an orbit of $G_{S'_1}$. Hence, there exists $h \in G_{S'_1}$ such that $s_1^h = s_2^g$.

We have

$$S_1^h = {S'_1}^h \setminus \{s_1^h\} = S'_1 \setminus \{s_2^g\} = {S'_2}^g \setminus \{s_2^g\} = S_2^g,$$

and therefore S_1 and S_2 belong to the same orbit $\mathcal{O}$ of G.

Because line 2 of the algorithm only visits each orbit of G at most once, and line 3 chooses exactly one representative of that orbit, it follows that $S_1 = S_2$. This also implies that $S_1^h = S_2^g = S_1^g$, and hence $hg^{-1} \in G_{S_1}$. Now, $s_2 = s_1^{hg^{-1}}$, and therefore s_1 and s_2 belong to the same orbit O of G_{S_1}. Because line 4 of the algorithm only visits each orbit of G_S on $(V \setminus S)$ at most once, and line 5 chooses exactly one representative of that orbit, we may now derive that $s_1 = s_2$ and therefore $S'_1 = S'_2$. ∎

It is crucial to the efficiency of the algorithm that statement ❸ will be executed *at most* once for every such orbit $\mathcal{O}'$. It allows us to implement $\mathcal{A}_{\text{out}}$ as a list instead of a set, in other words, that elements can simply be added to the end of $\mathcal{A}_{\text{out}}$ without the need to check for duplicates.

Without this property, adding elements to $\mathcal{A}_{\text{out}}$ would be a costly operation, not only because $\mathcal{A}_{\text{out}}$ is very large, but also because checking for equality of elements is quite expensive. Indeed, because an orbit is represented by one of its representatives, testing whether two orbits are equal amounts to deciding whether two elements are in the same orbit and this is difficult to do fast, especially because the elements in this case are sets of points.

The fact that we represent an orbit by one of its elements exposes a weak point of Algorithm 1: the inner loop of the algorithm visits every orbit O exactly once, which again implies that we need to determine whether two elements belong to the same orbit. Fortunately in this case elements are points and not entire sets. However, the group for which we need to compute the orbits is the stablizer group G_S, which is different for every iteration of the outer loop, and is non-trivial to compute.

For this reason, it is sometimes more convenient to use Algorithm 2 which is a simple variant of the first algorithm. Algorithm 2 tries to augment the set S with every possible $s \in V \setminus S$, and not with just one s for each orbit of G_S. Instead of adding the resulting orbits S'^G immediately to $\mathcal{A}_{\text{out}}$ they are gathered into a set $\mathcal{B}$, which is then added every time to $\mathcal{A}_{\text{out}}$ in its entirety. This time $\mathcal{B}$ is a true set and not a simple list: contrary to Algorithm 1 it may now happen that the same orbit is added more than once to $\mathcal{B}$ in statement ❹. Hence, avoiding the computation of G_S comes at the cost of an extra check for duplicates in a set of sets of points $\mathcal{B}$, albeit a small one.

We now prove that the algorithm is well-defined.

Lemma 4.4 *The result of Algorithm 2 is independent of the choice of the representative S of the orbit $\mathcal{O}$ at statement ❹.*

Algorithm 2 Isomorph-free generation without the need to compute G_S

Input: $\mathcal{A}_{\text{in}} \subseteq G\backslash\backslash 2^V$
Output: $\mathcal{A}_{\text{out}} \subseteq G\backslash\backslash 2^V$
1: $\mathcal{A}_{\text{out}} = \emptyset$
2: **for all** $\mathcal{O} \in \mathcal{A}_{\text{in}}$ **do**
3: Choose $S \in \mathcal{O}$ ❹
4: $\mathcal{B} = \emptyset$
5: **for all** $s \in V \setminus S$ **do**
6: $S' \leftarrow S \cup \{s\}$
7: **if** $\mathsf{P}(S')$ and $s \in F(S')$ **then**
8: Add S'^G to $\mathcal{B}$ ❺
9: **end if**
10: **end for**
11: Add all elements of $\mathcal{B}$ to $\mathcal{A}_{\text{out}}$ ❻
12: **end for**

Proof : Assume we choose $\overline{S} \in \mathcal{O}$ instead of S. Then $\overline{S} = S^g$ for some $g \in G$. We obtain $(V \setminus \overline{S}) = (V \setminus S)^g$, so the algorithm runs through each $\bar{s} \in (V \setminus \overline{S})$ instead of each $s \in (V \setminus S)$. However, for each $\bar{s}$ there exists a $s \in (V \setminus S)$ such that $\bar{s} = s^g$. On line 6, the element S' is replaced by $\overline{S'} = \overline{S} \cup \{\bar{s}\} = S^g \cup \{s^g\} = s'^g$. We have $\mathsf{P}(S')$ if and only if $\mathsf{P}(\overline{S'})$ and $s \in F(S')$ if and only if $\bar{s} \in F(\overline{S'})$. It follows that statement ❻ will be executed for $\overline{S'}$ if and only if it would be executed for S' with the original choice of S, and because $\overline{S'}^G = S'^{gG} = S'^G$, in both cases exactly the same element is added to $\mathcal{B}$. ∎

Theorem 4.5 *Let $k \in \{1, \ldots, |V|-1\}$. If $\mathcal{A}_{\text{in}}$ is initialized to the set of all orbits $\mathcal{O}$ of base size k such that $\mathsf{P}(\mathcal{O})$, then Algorithm 2 terminates with $\mathcal{A}_{\text{out}}$ equal to the set of all orbits $\mathcal{O}'$ of base size $k+1$ such that $\mathsf{P}(\mathcal{O}')$.*

Proof : We need to prove that statement ❺ of Algorithm 2 is executed at least once for every orbit $\mathcal{O}' = S'^G$ that satisfies $\mathsf{P}(\mathcal{O})$ and such that $|S'| = k+1$.

Let $\mathcal{O}'$ denote an orbit of this type, and let $T' \in \mathcal{O}'$. From $\mathsf{P}(\mathcal{O}')$ it follows

that $\mathsf{P}(T')$ (by definition). Let $t \in F(T')$ and define $T = T' \setminus \{t\}$. Note that $|T| = k$ and because P is hereditary, that $\mathsf{P}(T)$. Hence $T^G \in \mathcal{A}_{\text{in}}$ and therefore $\mathcal{O} = T^G$ is one of the orbits that will be considered by the loop of line 2.

By Lemma 4.4 we may without loss of generality choose $S = T$ in statement ❹. As $t \in (V \setminus S)$, $T' = T \cup \{t\}$ will be considered in line 6 and will be added to $\mathcal{B}$ in ❺. Hence, statement ❺ is called at least once for each of the orbits $\mathcal{O}'$ of the requested type. ∎

Lemma 4.6 *In Algorithm 2, every orbit S'^G is added to at most one $\mathcal{B}$ in step ❺ and hence is added to $\mathcal{A}_{\text{out}}$ at most once.*

Proof : Assume the algorithm tries to add $S_1'^G$ to a set $\mathcal{B}_1$ and $S_2'^G$ to a set $\mathcal{B}_2$ in step ❺, with $S_1'^G = S_2'^G$. There exists a $g \in G$ such that $S_1' = S_2'^g$. From lines 6 and 7 of the algorithm it follows that

$$\begin{array}{rlll} S_1' = & S_1 \cup \{s_1\} & \text{for some} & s_1 \in F(S_1') \\ S_2' = & S_2 \cup \{s_2\} & \text{for some} & s_2 \in F(S_2') \end{array}$$

Also $F(S_1') = F(S_2'^g) = F(S_2')^g$ which implies that both s_1 and s_2^g belong to $F(S_1')$, an orbit of $G_{S_1'}$. Hence, there exists $h \in G_{S_1'}$ such that $s_1^h = s_2^g$. We have

$$S_1^h = S_1'^h \setminus \{s_1^h\} = S_1' \setminus \{s_2^g\} = S_2'^g \setminus \{s_2^g\} = S_2^g,$$

and therefore S_1 and S_2 belong to the same orbit $\mathcal{O}$ of G. This leaves us two cases, either $S_1 = S_2$ or $S_1 \neq S_2$. If $S_1 \neq S_2$, then lines 2 and 3 of the algorithm imply that only one of these sets is considered during generation, and hence either $S_1'^G$ is added to $\mathcal{B}_1$ or $S_2'^G$ is added to $\mathcal{B}_2$. If $S_1 = S_2$ then S_1' and S_2' are added to the same set $\mathcal{B}$. ∎

We have programmed both algorithms in the case of k-arcs. For smaller q, we have run them both as an additional validity check.

In Section 4.4.3, we explain some additional speed improvements that turn out to be useful in practice.

4.2 Isomorph-free generation for $(k,3)$-arcs

In this section, for $\mathsf{P}(S)$ we consider the predicate "S is a $(k,2)$-arc or a $(k,3)$-arc of $\mathrm{PG}(2,q)$" (often simply referred to as "arcs" in this section). Recall that we often silently drop the requirement that at least one line must contain 3 points in a $(k,3)$-arc. This means that we sometimes regard a $(k,2)$-arc as a special case of a $(k,3)$- arc. Of course, for complete $(k,3)$-arcs this is not an issue because a $(k,2)$-arc can never be a complete $(k,3)$-arc.

The predicate is group invariant and hereditary as required for the algorithm. Indeed, for every subset $T \subset S$ it holds that if S is an arc, then so is T. Also S^g with $g \in G$ is an arc if and only if S is an arc.

Note that "being a *complete* arc" is not a hereditary property and can therefore not be used as predicate P. Instead we generate *all* arcs (up to equivalence) and discard the incomplete arcs at the end.

4.2.1 Invariants

We were able to obtain significant speed improvements to the basic algorithms of Section 4.1 by making use of certain invariants of the arcs being generated.

Let S be a $(k,3)$-arc, let ℓ be a line of the plane, let p be a point of the plane. Denote the number of points of S on ℓ by $d_S(\ell)$, the number of bisecants of S through p by $b_S(p)$ and the number of trisecants of S through p by $t_S(p)$. Note that $d_S(\ell)$, $b_S(p)$ and $t_S(p)$ are invariant for the group G in the sense that $d_S(l) = d_{S^g}(l^g)$, $b_S(p) = b_{S^g}(p^g)$ and $t_S(p) = t_{S^g}(p^g)$ for all $g \in G$. Hence it follows that $d_S(\ell)$, $b_S(p)$ and $t_S(p)$ are also invariant for the group G_S.

For every line ℓ of the plane we define the following *line invariant*:

$$I_S(\ell) \stackrel{\text{def}}{=} h_1(d_S(\ell)) + \sum_{p \in \ell \setminus S} (h_2(b_S(p)) + h_3(t_S(p))) \tag{4.1}$$

where h_1, h_2, h_3 denote simple hash functions (cf. Section 4.4.5). Again I_S

satisfies $I_{S^g}(\ell^g) = I_S(\ell)$ for every $g \in G$. Note that I_S can be computed very efficiently if we keep track during the course of the algorithms of the values of $d_S(\ell)$, $b_S(p)$ and $t_S(p)$ for all lines and points of the plane.

For every point p of the plane we define a *point invariant*:

$$I_S(p) \stackrel{\text{def}}{=} \sum_{\ell, p \in \ell} h(I_S(\ell)), \tag{4.2}$$

where h denotes a simple hash function (cf. Section 4.4.5). Here we also have $I_{S^g}(p^g) = I_S(p)$ for every $g \in G$. The computation of the point invariant values for all points in the arc S is not very efficient, but we do not need to compute them for every generated arc S. In many cases $t_S(p)$ is itself already a sufficiently strong invariant for our purposes and $I_S(p)$ is only used when this turns out not to be the case.

The functions t_S and I_S each induce a partition on S which we will denote by $t_S \backslash\backslash S$, resp. $I_S \backslash\backslash S$. Two points p, p' belong to the same part $U \in t_S \backslash\backslash S$ ($I_S \backslash\backslash S$) if and only if $t_S(p) = t_S(p')$ ($I_S(p) = I_S(p')$), and in that case we shall write $t_S(U) \stackrel{\text{def}}{=} t_S(p)$ ($I_S(U) \stackrel{\text{def}}{=} I_S(p)$). We will call elements of these partitions *t-quasi-orbits* and *I-quasi-orbits* of S.

Note that $U \in t_S \backslash\backslash S$ satisfies $U^g = U$ for every $g \in G_S$ and therefore any t-quasi-orbit U is a union of orbits of G_S on S. The same holds for all I-quasi-orbits. In particular, every singleton t- or I-quasi-orbit $\{p\}$ must be a true orbit of G_S. In other words, $G_S \backslash\backslash S$ is a refinement of $t_S \backslash\backslash S$ and of $I_S \backslash\backslash S$. The sets U are called quasi-orbits because we hope the invariants to be sufficiently strong such that the sets are true orbits in most of the cases.

4.2.2 Canonical form

While the invariants t_S and I_S play a crucial role in the canonical augmentation algorithm, there are (rare) occasions where they are not sufficient to ensure isomorph-free generation. In those cases we need to use a so called *canonical form* $\text{can}(S)$ of the generated set S. A canonical form is a map $\text{can} : 2^V \mapsto 2^V$ such that

- $\mathrm{can}(S) \in S^G$
- $\mathrm{can}(S) = \mathrm{can}(T)$ if and only if $S^G = T^G$.

In other words, $\mathrm{can}(\cdot)$ chooses one particular representative in every orbit of $G\backslash\backslash 2^V$. We simply call $\mathrm{can}(S)$ the canonical form of S. Fortunately, the data we gather to compute the invariants can also be put to good use when constructing such a canonical form. We want to construct a canonical form for S in which certain known points have minimal point invariant values.

Let J_S denote one of the point invariants (I_S or t_S) of the previous section. To describe the canonical form which was used in our algorithms, we introduce the following ordering on the quasi-orbits of S: let $U, U' \in J_S\backslash\backslash S$, then $U < U'$ if and only if $|U| < |U'|$ or $|U| = |U'|$ and $J_S(U) < J_S(U')$. In other words, we order the quasi-orbits first according to size and then according to point invariant value. This ordering has the interesting property that it is group invariant in the following sense: if $U < U'$ in $J_S\backslash\backslash S$, then $U^g < U'^g$ in $J_{S^g}\backslash\backslash S^g$.

It is very easy to see that the two points p_1 and p_2 with minimal invariants, i.e., satisfying $J_S(p_1) \leq J_S(p_2) \leq J_S(p)$ for all $p \in S - \{p_1, p_2\}$, can always be mapped by a projectivity to two chosen points, say the points e_1, e_2 with coordinates $(1,0,0)$ and $(0,1,0)$. We would like to extend this principle to four points, but there are some complications.

The first complication already arises for the point p_3 with third smallest invariant. We have two possibilities: if p_1, p_2, p_3 are not collinear, then p_3 can be mapped to $e_3(0,0,1)$, otherwise it can be mapped to $f_3(1,1,0)$.

We can however be sure that if the third point cannot be mapped to $e_3(0,0,1)$ then the fourth point can (otherwise there would be four points on the same line). More generally, among the five points with smallest invariants, we will always be able to find four that form a quadrangle. The fourth point of the quadrangle can then be mapped to $e_4(1,1,1)$. Whence the following definition :

Let J_S denote an invariant (in our case $J_S = I_S$ or t_S). Then an arc S will be called *J-quasi-canonical* if and only if the following conditions are satisfied :

- $e_1, e_2, e_3, e_4 \in S$,
- $J_S(e_1) \leq J_S(e_2) \leq J_S(e_3) \leq J_S(e_4)$
- There exist at most one point $p \in S - \{e_1, e_2, e_3, e_4\}$ such that $J_S(p) < J_S(e_4)$.
- If such p exists, it lies on at least one of the lines $e_i e_j$, or equivalently, $\{e_1, e_2, e_3, e_4, p\}$ is not a $(5,2)$-arc.
- If such p lies on exactly one line $e_i e_j$, then $J_S(p) \geq J_S(e_i)$ and $J_S(p) \geq J_S(e_j)$.

Proposition 4.7 *Let S be a $(k,3)$-arc of $\mathrm{PG}(2,q)$ with $|S| \geq 5$. Then S^G contains at least one J-quasi-canonical element.*

Proof : We can always find a set $P = \{p_1, \ldots, p_5\} \subseteq S$ of 5 points of S that satisfy the condition $J_S(p_1) \leq J_S(p_2) \leq \cdots \leq J_S(p_5)$. (Take p_1 to be one of the points of S for which J_S is minimal, take p_2 to be one of the points of $S - \{p_1\}$ for which J_S is minimal, ...)

Now define the point p_* as follows :

- If no three points among $p_1, \ldots, p_5$ are collinear, then $p_* \stackrel{\text{def}}{=} p_5$.
- If P contains exactly one collinear triple, say $p_i p_j p_k$ with $i < j < k$, then $p_* \stackrel{\text{def}}{=} p_k$.
- If P contains two collinear triples, then p_* is the point these triples have in common.

Define $P' = P - \{p_*\}$. By the choice of p_*, P' contains no collinear triples. Write $P' = \{p_i, p_j, p_k, p_\ell\}$ with $i < j < k < \ell$. Now, there exists a (unique) projectivity g that maps p_i to e_1, p_j to e_2, p_k to e_3 and p_ℓ to e_4.

We leave it to the reader to verify that S^g is J-quasi-canonical. ∎

The proof of this proposition is constructive and can easily be extended to an algorithm which finds *all* J-quasi-canonical elements of S^G.

Fix an ordering on the points of the plane and extend this to a lexical ordering of subsets of points of equal size. We are finally in a position to define the *canonical form* of a $(k,3)$-arc. Let S denote a $(k,3)$-arc with $k \geq 5$.

1. If the t-quasi-orbit partition of S contains at least one singleton, then define $\mathrm{can}(S)$ to be the smallest of all t-quasi-canonical arcs in S^G with respect to this lexical ordering.
2. Otherwise, define $\mathrm{can}(S)$ to be the smallest of all I-quasi-canonical arcs in S^G with respect to this lexical ordering.

Although the definition of the canonical form is rather involved, in practice it can be computed quite efficiently, especially when all relevant invariant values are known beforehand.

There are two places in our algorithms where the canonical form can be useful. First, it is used to construct the function F (Section 4.2.3). Second, it can be used to decide whether two arcs belong to the same orbit of G (Section 4.2.4).

4.2.3 The function F

We use the point invariants and the canonical form to construct the function F which we have used in Algorithms 1 and 2.

For $(k,3)$-arcs we define F as follows:

1. If the t-quasi-orbit partition of S contains at least one singleton, then we define $F(S)$ to be the singleton $\{p\}$ for which $t_S(p)$ is minimal.
2. Otherwise, if the I-quasi-orbit partition of S contains at least one singleton, then we define $F(S)$ to be the singleton $\{p\}$ for which $I_S(p)$ is minimal.

3. Otherwise $F(S) \stackrel{\text{def}}{=} e_1^{hG_S}$ where $h \in G$ is such that $S = \text{can}(S)^h$ and e_1 is as in Section 4.2.2. In simple terms: F selects that orbit of G_S whose representative corresponds to e_1 in the canonical form of S.

Note that the definition of the function F is independent of the choice of h. Indeed, suppose $S = (\text{can}(S))^h = (\text{can}(S))^{h'}$ with $h, h' \in G$. Then $\text{can}(S) = S^{h^{-1}} = S^{h'^{-1}}$, so $S^{h^{-1}h'} = S$. This implies $h^{-1}h' \in G_S$ and hence $h^{-1}h'G_S = G_S$. So $hG_S = h'G_S$.

The following proposition shows that F satisfies the necessary properties to be safely applied in Algorithms 1 and 2 (cf. Section 4.1.1):

Proposition 4.8 *Let $F(S)$ be defined as above. Then*

1. *For all S, $S \subseteq V$, $S \neq \emptyset$, $F(S)$ is an orbit of G_S on S;*
2. *For all $S \subseteq V$, $g \in G$, we have $F(S^g) = F(S)^g$.*

Proof : 1. In the first and second case of the definition $F(S)$ is a singleton quasi-orbit of S and hence a true orbit of G_S on S. Otherwise, $F(S)$ is of the form $e_1^{hG_S}$ which is a G_S-orbit of e_1^h. And because $e_1 \in \text{can}(S)$, we have $e_1^h \in (\text{can}(S))^h = S$.

2. Let J_S denote one of the invariants t_S or I_S. Because the J-quasi-orbit partition for S^g is the image by g of the J-quasi-orbit partition of S, either both will contain singletons or neither. Hence $F(S)$ and $F(S^g)$ either both satisfy the conditions of the first (or second) part of the definition, or neither do.

In the first case we have $J_{S^g}(p^g) = J_S(p)$ for all singleton quasi-orbits $\{p\}$ of S, and hence if $\{p\}$ is the singleton for which J_S is minimal, then $\{p'\} = \{p^g\}$ will be the singleton for which J_{S^g} is minimal, with the same value. Hence $F(S^g) = F(S)^g$ in that case.

Otherwise S^g and S are in the same G-orbit, and hence have the same canon-

ical form $\text{can}(S) = \text{can}(S^g)$. If $S = (\text{can}(S))^h$, then $S^g = (\text{can}(S))^{hg}$ and therefore $F(S^g) = e_1^{hgG_{Sg}} = e_1^{hG_Sg} = F(S)^g$. ∎

Computing $F(S)$ is fast in most cases. Indeed, the majority of (partial) arcs encountered in the course of the algorithm have a trivial automorphism group and therefore all orbits have size 1. Moreover, if the automorphism group is non-trivial, it is often small enough to contain at least a few orbits of size 1. When orbits have size 1, we expect (some of) the quasi-orbits also to have size 1, and indeed in practice this often turns out to be the case. As a consequence, we hardly ever need to compute the canonical form of S in order to determine whether $s \in F(S')$ (line 7 of the algorithms).

Also note that we only use the point invariant $I_S(p)$ if there is no unique value among all values $t_S(p)$ for all $p \in S$. For instance, for $q = 11$ this only happens in 41% of the cases, for $q = 13$ in 38% of the cases .

4.2.4 Orbit membership

In statement ❺ of Algorithm 2 we need to decide whether two arcs (say S' and T') belong to the same orbit of G. This is a non-trivial task. Fortunately, we can use the point invariant values that already have been computed as a preliminary test: two non-isomorphic sets always have different invariant values. Therefore, we store the J-point invariant values of the points p of the arc S', resp. T' in a sorted list $L_{S'}$, resp. $L_{T'}$ according to the ordering defined in Section 4.2.2. If the lists $L_{S'}$ and $L_{T'}$ are different, then S' and T' cannot belong to the same orbit (this turns out to happen in most of the cases). If the lists are equal however, we compute $\text{can}(S)'$ and $\text{can}(T)'$ and compare them for equality (they are equal if and only if $S'^G = T'^G$).

When line 8 is reached during the algorithm, the computation of $F(S')$ has already been done in line 7. Hence, at this point we already know whether the t-quasi orbit partion of S' contains a singleton or not. The arc T' to which S' is compared, was already part of the set $\mathcal{B}$, so for this set $F(T')$ was also already determined. If one of the sets S' or T' contains a singleton t-quasi orbit, then for this set the I-point invariant values were not determined yet,

and then we take $J = t$. If none of the sets contains a singleton, the values $I_{S'}(p)$ and $I_{T'}(p)$ have been computed in line 7, so then we take $J = I$.

4.3 Isomorph-free generation for $(k,2)$-arcs

In Section 4.3 we described the algorithm for the generation of $(k,3)$-arcs. The generation of $(k,2)$-arcs can be done in a very similar way. The major part of the algorithm is the same except for some changes (mostly simplifications) that will be explained in this section.

For $\mathsf{P}(S)$ we now consider the predicate "S is a $(k,2)$-arc of $\mathrm{PG}(2,q)$".

We no longer have the values $t_S(p)$ for points p in S as trisecants do not exist for $(k,2)$-arcs. Therefore we reduce (4.1) to

$$I_S(\ell) \stackrel{\text{def}}{=} \sum_{p \in \ell \setminus S} h_2(b_S(p)), \tag{4.3}$$

in which we have also dropped the value $d_S(\ell)$ because it can be derived from the values $b_S(p)$.

For $(k,3)$-arcs b_S (b_S and t_S are linear dependent) was itself already a sufficiently strong point invariant for our purposes and $I_S(p)$ was only used when this turned out not to be the case. For $(k,2)$-arcs, each point p in the arc has the same value $b_S(p) = k-1$. Therefore, the t-point invariant is of no use in this case and hence we only use the I-point invariant values.

Also, the definition of quasi-canonical arcs turns out to be easier: four points of the arc with minimal invariants, i.e. $I(p_1) \leq I(p_2) \leq I(p_3) \leq I(p_4) \leq I(p)$ for all $p \in S - \{p_1, p_2, p_3, p_4\}$, can always be mapped to the four points e_1, e_2, e_3, e_4 by a projectivity. Hence, a $(k,2)$- arc S will be called *quasi-canonical* if and only if $e_1, e_2, e_3, e_4 \in S$ and $I_S(e_1) \leq I_S(e_2) \leq I_S(e_3) \leq I_S(e_4)$. We have the following proposition:

Proposition 4.9 *Let S be an arc of $\mathrm{PG}(2,q)$ with $|S| \geq 4$. Then S^G contains at least one quasi-canonical element.*

The *canonical form* of a $(k,2)$-arc S with $k \geq 4$ can now be defined as the lexically smallest of all quasi-canonical elements of S^G.

In the definition of the function F, the first item can be dropped which again makes the definition more simple.

4.4 Additional remarks

We end this chapter with some additional information on the actual implementation of the generation algorithms.

4.4.1 Initial Configurations

In Section 4.1.1 we explained that it is not always necessary to start the generation from the empty set. In the case of $(k,2)$-arcs we start with the unique orbit of $(4,2)$-arcs in $\mathrm{PG}(2,q)$ and we take the set $\{(1,0,0),(0,1,0),(0,0,1),(1,1,1)\}$ as representative for this orbit. For $(k,3)$-arcs we need one additional orbit, the unique orbit of sets of size 4 in which at least 3 points are collinear. A representative of this set is $\{(1,0,0),(0,1,0),(1,1,0),(1,1,1)\}$.

4.4.2 Computation of invariants

During the course of the algorithms we keep track of several quantities instead of recomputing them every time we need them. For example, for each line we store whether it is an external line, a unisecant, a bisecant (or a trisecant) of

the current arc S. Whenever we augment S to $S' = S \cup \{s\}$, we only need to update this information for the lines through s, which can be done in time $O(q)$. Likewise, for every point p we keep track of the current number $b_S(p)$ of bisecants through that point. For $(k,3)$-arcs we also store the number $t_S(p)$ of trisecants. When S is augmented to S', and a line ℓ is promoted from unisecant to bisecant (or from bisecant to trisecant), we simply add one to this value $b_S(p)$ (or $t_S(p)$) for each point on ℓ. The values of $b_S(p)$ (or $t_S(p)$) also help us in determining which points can be added to the current arc for it to remain an arc: we only consider those points s that satsify $b_S(p) = 0$ (or $t_S(p) = 0$).

The values of the point and line invariants I_S are computed anew every time we need them. However, we only need to compute $I_S(p)$ for points $p \in S$, and as a consequence, we also do not need to compute $I_S(\ell)$ when ℓ is an external line of S. In the case of $(k,3)$-arcs, we even only compute $I_S(p)$ for points $p \in S$ if there was no singleton t-quasi orbit. If a singleton t-quasi orbit was found, we do not compute $I_S(\ell)$ for any line of the plane.

Programs that use canonical augmentation usually benefit from an optimization technique that consists of avoiding the computation of canonical forms as much as possible. In our case profiling statistics show that for larger q indeed little running time is still spent in constructing canonical forms. Instead most of the effort goes into calculating point and line invariants.

It might be possible to further decrease the number of canonical forms which need to be computed by using 'better' invariants, i.e., invariants for which the quasi-orbits more closely resemble the true stabilizer orbits. One way to obtain such invariants would be as follows: define a new line invariant $I'_S(\ell) \stackrel{\text{def}}{=} \sum_{p \in \ell} h'(I_S(p))$, and from this, a new point invariant $I'_S(p) \stackrel{\text{def}}{=} \sum_{\ell, p \in \ell} h''(I'_S(\ell))$ using some simple hash functions h' and h''. This strategy can even be repeated several times to obtain further invariants I''_S, I'''_S, ...

However, each step in this process takes $O(q^3)$ of computation time (with the simplifying assumption that we need the invariant values for all points and all lines). Because the determination of invariant values is already the major bottleneck of the program, using these new invariants would probably slow

down the generation process rather than speed it up.

4.4.3 Some small improvements

In Section 4.1 we presented two variants of the same algorithm. One variant makes use of the set stabilizer of the partial arc which we obtain, the other does not, but requires further checks to make sure that no two isomorphic arcs are ever generated. In the first algorithm, the set stabilizer of the arc has to be recomputed for every iteration, a non-trivial task.

However, in some cases too much work is done. Indeed, whenever G_S is trivial, and the point s has a unique value of $I_S(s)$, then also $G_{S'}$ must be trivial (with $S' = S \cup \{s\}$), and therefore there is no need to compute $G_{S'}$ explicitly. Also, when a sufficient number of points of S have a value of I_S that is unique (four points for $(k,2)$-arcs, five for $(k,3)$-arcs), this again implies that G_S is trivial (when $G = \mathrm{PGL}(3,q)$).

Because we compute the values of I_S in the course of the algorithm anyway, these extra checks allow us to make some simple shortcuts. Note that a trivial stabilizer group implies trivial orbits, making it easy to ensure that we select not more than one point for each orbit, a crucial step in the algorithm. As mentioned before, it turns out that almost all arcs that are encountered have a trivial automorphism group.

In our program we use a combination of Algorithm 1 and 2. Whenever an arc S' of size k has a trivial stabilizer group, we use Algorithm 1 to find the arcs of size $k+1$ containing S'. If however S' has a non-trivial stabilizer group, we use Algorithm 2 in the following level of the generation.

This idea is essentially a toned down version of a similar technique Brinkmann and McKay used for generating posets up to isomorphism [5].

4.4.4 Computational group methods

In the algorithm descriptions above we have left out any details about the computational group methods involved. Where most authors favour the use of permutation group techniques for problems like these, we have instead chosen to represent elements of $\mathrm{PGL}(3,q)$ as 3×3 matrices, and subgroups of $\mathrm{PGL}(3,q)$ as lists of such elements.

There were several reasons for this decision. Matrices use little storage space and provide an easy way to compute the unique projectivity that maps one 4-arc to another. Also the subgroups involved tend to be small. As has already been indicated before, the algorithms turn out to spend only a small part of their time doing group operations, and hence the particular choice of group representations is probably irrelevant for this type of problem.

One drawback of the matrix representation is that it does not allow elements of $\mathrm{P\Gamma L}(3,q) \setminus \mathrm{PGL}(3,q)$ to be represented easily.

However, we did extended our programs to use PΓL-equivalence. If the stabilizer group G_S of the arc S in $\mathrm{PGL}(3,q)$ is the same as the stabilizer group Γ_S of S in $\mathrm{P\Gamma L}(3,q)$, then an orbit of $\mathrm{P\Gamma L}(3,q)$ is the union of multiple orbits of $\mathrm{PGL}(3,q)$ if q is a prime power. This means that fewer arcs need to be considered during the course of the algorithm when using PΓL-equivalence, making the program significantly faster. We ran both versions of the programs, and the fact that for each k they resulted in the same number of PGL-equivalent arcs is an aditional indication that our pograms work correctly.

4.4.5 Further implementation details

Field elements

We use the numbers $0, 1, \ldots, q-1$ to represent the q elements of a finite field $\mathbb{F}_q$. Field operations are implemented by table lookup. This is fast and works for prime and prime power fields alike. If α is a generating element of $\mathbb{F}_q$,

then α^i is represented by $i+1$ (and 0 by 0).

Numbering of points and lines

In our programs we have numbered the points (and lines) of the plane in the following way: first, we normalize the coordinates of a point (line) such that the first non-zero coordinate always is equal to 1. Then we number the points (lines) according to a lexical ordering of the normalized coordinate triples. Hence, the point with coordinates $(0,0,1)$ has number 0, a point with coordinates $(0,1,a)$ has number $a+1$, and a point with coordinates $(1,a,b)$ has number $(a+1)q+b+1$.

Hash functions

In Section 4.2.1, for every line ℓ we would like to store a multiset containing the values $b_S(p)$ and $t_S(p)$ for every non-arc point on ℓ. Such a multiset is an invariant for the line. Multisets however are difficult to work with. Therefore, we try to attach an integer to each multiset in such a way that different sets correspond to different integers as much as possible. Taking just the sum of the elements of the multiset (i.e. $h(x) = x$) is not a good idea because then many different sets will turn out to correspond to the same integer. Instead, we translate the values $b_S(p)$ and $t_S(p)$ to larger integers using hash functions in order to spread out the sums. For the invariant $I_S(\ell)$ we also take into account the value of $d_S(\ell)$ in order to spread out the sums even more. The point invariants $I_S(p)$ are computed in a similar way.

In Section 4.3, the hash function $h_2(b_S(p))$ is equal to $2^{b_S(p)}$. When using bit shift operations, this can be computed very efficiently if we keep track of the values $b_S(p)$ during the course of the algorithm. Indeed, the values $b_S(p)$ always change with ± 1 which corresponds to a simple bit shift in $2^{b_S(p)}$.

4.4.6 Parallelization

We have written our programs in such a way that we can split the generation of arcs over several processors. The splitting program asks for the parameters *depth* k, *modulus* m and *step* i. Then for the arcs of size $k+1$ and larger only part of the arcs are generated. The modulus determines the number of parts into which the generation is split. The step determines which part of the generation is done. This is done in the following way: we generate all arcs up to size k. If the arc S of size k has number n in the generation of all arcs of size k, then the arcs $S' = S \cup \{s\}$ of size $k+1$ are only generated if $n \equiv i \pmod{m}$.

4.5 Consistency check

We have also run a consistency check based on the principle of 'double counting', somewhat similar to the method used by Östergård and Pottonen in their generation of perfect binary one-error-correcting codes [36].

Let A_k denote the number of pairs (S, p) where S is an arc of size k and p is a point of S. We shall count A_k in two different ways. Clearly, A_k is k times the total number of arcs of size k. By the orbit-stabilizer theorem, we have

$$A_k = k \sum_{S \in \mathcal{S}_k} \frac{|G|}{|G_S|},$$

where $\mathcal{S}_k$ contains one representative for each equivalence class of arcs of size k.

We can also compute A_k in a different way, by counting all pairs (T, p) where $S = T \cup \{p\}$. This yields

$$A_k = \sum_{T \in \mathcal{S}_{k-1}} n(T) \frac{|G|}{|G_T|},$$

where $n(T)$ denotes the number of points of the plane that can be added to T to create a new arc. Both formulas should yield the same result.

In order to compute the values of these formulas, we need to know the size of the stablizer group G_S and the number $n(S)$ for each arc S generated by our program. These are not so difficult to compute.

We ran the test for all $q \leq 27$ for $(k,2)$-arcs and for all $q \leq 11$ for $(k,3)$- arcs. Both formulas did indeed yield the same results. For $q = 29$ ($(k,2)$-arcs) and $q = 13$ ($(k,3)$-arcs) we did not run the test because this would have taken too long.

5

Results

Using the algorithms from Chapter 4 we have been able to compute a full classification of the projectively distinct complete $(k, 2)$-arcs in $\mathrm{PG}(2, q)$ for all $q \leq 29$ and of the projectively distinct complete $(k, 3)$-arcs for all $q \leq 13$. In this chapter, we have summarised the results in tables.

Most well-known constructions produce arcs that have an interesting (and often large) automorphism group. For this reason we have computed the automorphism groups of all complete arcs (see Section 5.1 and 5.4). We have studied some of the arcs with the larger automorphism groups in more detail, in order to describe them in a more elegant way than by just listing the coordinates of their points.

Sometimes general families of arcs can be described as special subsets of cubic curves or pairs of conics. Therefore, we have also computed for each $(k, 2)$-arc

the type of algebraic curve of lowest degree into which it can be embedded (see Section 5.2) and we have used this table to pick out some arcs to have a closer look at. For $(k,3)$ arcs, we have investigated some arcs lying for the greater part on a cubic curve.

In Chapter 6 and resp. 7, we discuss the results of the algorithm. We there give geometric descripions of the arcs whose stabilizer groups are underlined in the tables of Section 5.1, resp. 5.4.

5.1 The complete $(k,2)$-arcs of $\mathrm{PG}(2,q)$, $q \leq 29$

For each of the complete $(k,2)$-arcs we have determined the subgroups G_S of $\mathrm{PGL}(3,q)$ and Γ_S of $\mathrm{P\Gamma L}(3,q)$ that stabilize the set S of points of the arc. Note that $G_S = \Gamma_S$ when q is prime. The results are summarised in the tables below.

In these tables k denotes the size of the arcs in the corresponding column, and N_k the number of inequivalent complete arcs of size k.

For each k we specify a list of possible stabilizer groups G_S and Γ_S and the corresponding number of k-arcs that have an automorphism group of that type. (We use the 'Atlas'-notation for the groups [9].) The numbers listed refer to PΓL-inequivalent arcs and not to PGL-inequivalent arcs.

When $q = p^h$ with $h > 1$, there are three cases:

1. If $G_S = \Gamma_S$, then $[\Gamma_S : G_S] = 1$ and the orbit of S through Γ is the union of h disjoint orbits of G corresponding to the arcs S, $S^\sigma, \ldots$ and $S^{\sigma^{h-1}}$. These h arcs are therefore PΓL-equivalent but PGL-inequivalent. Hence the number of PGL-inequivalent k-arcs with a group of that type is h times the number listed.
2. If $[\Gamma_S : G_S] = h$, then $S^G = S^\Gamma$ (and hence S, $S^\sigma, \ldots S^{\sigma^{h-1}}$ are PGL-equivalent). In that case the number of inequivalent arcs of the given type is the same whether we regard $\mathrm{PGL}(3,q)$ or $\mathrm{P\Gamma L}(3,q)$ as the group defining equivalence.

3. If $G_S \neq \Gamma_S$ and $[\Gamma_S : G_S] \neq h$, then $[\Gamma_S : G_S]$ divides h. The orbit of S through Γ is the union of $h/[\Gamma_S : G_S]$ disjoint orbits of G. In this text, this only occurs when $q = 16$: then $[\Gamma_S : G_S] = 2$ and the number of PGL-inequivalent arcs is two times the number listed.

In Chapter 6 we give geometric descriptions of the arcs whose automorphism groups are underlined in the tables.

Our programs, which were written in Java, were run on an Ubuntu Linux desktop system with a dual core AMD Athlon 64 X2 4400+ processor (for $q \leq 25$), on a Debian Linux system with two quad core Intel Xeon X5355 2.66GHz processors (for $q = 27$) and on a cluster of Debian Linux systems with 56 quad core Intel Xeon X3220 2.40GHz processors (for $q = 29$).

Using only a single core, the cases $q \leq 19$ take less then 1 hour, the case $q = 23$ takes approximately one day of CPU time, the case $q = 25$ takes about ten days, the case $q = 27$ takes approximately 33 days of CPU time and the case $q = 29$ takes approximately 1870 days (five years) of CPU time. To store the results (in compressed form) we need about 130GByte of disk space.

PG(2,5)	
$k = 6$	
$N_k = 1$	
G_S	#
PGL$(2,5)$	1

PG(2,7)			
$k = 6$		$k = 8$	
$N_k = 2$		$N_k = 1$	
G_S	#	G_S	#
A_4	1	PGL$(2,7)$	1
$4\colon 3^2$	1		

PG(2,8)					
$k = 6$			$k = 10$		
$N_k = 1$			$N_k = 1$		
Γ_S	G_S	#	Γ_S	G_S	#
$\underline{S_4}$	$\underline{S_4}$	1	$\underline{\text{P}\Gamma\text{L}(2,8)}$	$\underline{\text{PGL}(2,8)}$	1

PG(2,9)											
$k = 6$ $N_k = 1$			$k = 7$ $N_k = 1$			$k = 8$ $N_k = 1$			$k = 10$ $N_k = 1$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
$\underline{S_5}$	$\underline{A_5}$	1	$\underline{7\colon 6}$	$\underline{7\colon 3}$	1	$\underline{D_{16}}$	$\underline{D_8}$	1	$\underline{\mathrm{P\Gamma L}(2,9)}$	$\underline{\mathrm{PGL}(2,9)}$	1

PG(2,11)									
$k = 7$ $N_k = 1$		$k = 8$ $N_k = 9$		$k = 9$ $N_k = 3$		$k = 10$ $N_k = 1$		$k = 12$ $N_k = 1$	
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
$\underline{7\colon 3}$	1	2	5	2	1	$\underline{A_5}$	1	$\underline{\mathrm{PGL}(2,11)}$	1
		2^2	1	3	1				
		D_8	1	S_3	1				
		D_{10}	1						
		$8\colon 2$	1						

PG(2,13)									
$k = 8$ $N_k = 2$		$k = 9$ $N_k = 29$		$k = 10$ $N_k = 21$		$k = 12$ $N_k = 1$		$k = 14$ $N_k = 1$	
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
S_3	1	1	17	1	1	$\underline{S_4\colon 3}$	1	$\underline{\mathrm{PGL}(2,13)}$	1
$\underline{D_{14}}$	1	2	4	2	11				
		3	5	2^2	4				
		4	1	4	2				
		$\underline{3^2}$	2	S_3	2				
				$\underline{S_4}$	1				

PG(2,16)											
$k=9$ $N_k=2$			$k=10$ $N_k=501$			$k=11$ $N_k=30$			$k=12$ $N_k=9$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
3	3	1	1	1	342	1	1	19	2	2	2
6	3	1	2	1	14	2	1	2	6	3	1
			2	2	116	2	2	8	S_3	S_3	3
			2^2	2	4	4×2	2	1	D_{10}	D_{10}	1
			4	1	3				D_{12}	S_3	1
			4	2	3				$3^2\colon 2$	$3^2\colon 2$	1
			4	4	2						
			S_3	S_3	3						
			2^3	2^3	10						
			$2D_4$	2^3	2						
			$8\colon 2$	4	1						
			D_{20}	D_{10}	1						

PG(2,16)					
$k=13$ $N_k=1$			$k=18$ $N_k=2$		
Γ_S	G_S	#	Γ_S	G_S	#
$\underline{13\colon 12}$	$\underline{13\colon 3}$	1	$\underline{[144]}$	$\underline{[36]}$	1
			$\underline{\mathrm{P\Gamma L}(2,16)}$	$\underline{\mathrm{PGL}(2,16)}$	1

PG(2,17)											
$k = 10$		$k = 11$		$k = 12$		$k = 13$		$k = 14$		$k = 18$	
$N_k = 560$		$N_k = 2644$		$N_k = 553$		$N_k = 8$		$N_k = 1$		$N_k = 1$	
G_S	#	G_S	#	G_S |	#	G_S	#	G_S	#	G_S	#
1	341	1	2569	1	336	1	1	D_8	1	$\underline{\mathrm{PGL}(2,17)}$	1
2	179	2	75	2	152	2	4				
3	10			3	18	3	1				
2^2	8			2^2	18	4	1				
4	7			4	1	S_3	1				
S_3	9			S_3	20						
$\underline{Q_8}$	1			D_8	2						
A_4	2			A_4	1						
$\underline{8:2}$	1			$\underline{D_{12}}$	2						
$\underline{D_{18}}$	1			$\underline{S_4}$	3						
$\underline{S_4}$	1										

PG(2,19)									
$k=10$		$k=11$		$k=12$		$k=13$		$k=14$	
$N_k=29$		$N_k=9541$		$N_k=30135$		$N_k=2232$		$N_k=70$	
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
1	1	1	9501	1	28301	1	2090	1	8
2	18	2	36	2	1640	2	137	$\underline{2}$	35
3	1	3	4	3	82	3	3	2^2	14
2^2	2			2^2	47	S_3	2	4	8
4	1			4	11			S_3	4
S_3	2			S_3	37			D_{12}	1
D_5	2			D_8	4				
A_4	1			3^2	2			$k=20$	
$\underline{A_5}$	1			A_4	3			$N_k=1$	
				D_{12}	1			G_S	#
				$\underline{D_{18}}$	1			$\underline{\mathrm{PGL}(2,19)}$	1
				$3^2:2$	2				
				$\underline{S_4}$	3				
				$\underline{S_4:3}$	1				

PG(2,23)							
$k = 10$		$k = 12$		$k = 13$		$k = 14$	
$N_k = 1$		$N_k = 112449$		$N_k = 4341514$		$N_k = 1828196$	
G_S	#	G_S	#	G_S	#	G_S	#
S_3	1	1	107770	1	4339330	1	1810741
		2	4387	2	1959	2	17147
		3	151	3	223	4	85
		4	7	S_3	2	2^2	222
		2^2	30			$\underline{D_{22}}$	1
		S_3	97				
		D_8	3				
		D_{12}	2				
		$\underline{S_4}$	2				

PG(2,23)							
$k = 15$		$k = 16$		$k = 17$		$k = 24$	
$N_k = 58361$		$N_k = 564$		$N_k = 5$		$N_k = 1$	
G_S	#	G_S	#	G_S	#	G_S	#
1	57184	1	213	2	5	$\underline{\mathrm{PGL}(2,23)}$	1
2	1040	2	275				
3	110	3	3				
S_3	27	4	5				
		2^2	41				
		S_3	14				
		D_8	11				
		D_{16}	1				
		$\underline{16:2}$	1				

PG(2,25)								
$k=12$ $N_k=606$			$k=13$ $N_k=4072545$			$k=14$ $N_k=29151431$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
1	1	290	1	1	4070197	1	1	29089885
2	1	37	2	1	1827	2	1	11972
2	2	223	2	2	464	2	2	48897
3	3	21	3	3	41	3	3	55
2^2	2	13	2^2	2	6	2^2	2	157
2^2	2^2	4	4	2	1	2^2	2^2	210
S_3	3	3	4	4	1	4	2	95
S_3	S_3	11	s_3	3	2	4	4	73
6	3	1	6	3	5	S_3	S_3	40
D_{12}	S_3	2	6	6	1	6	3	11
$3^2\colon 2$	$3^2\colon 2$	1				D_8	2^2	22
						D_8	D_8	2
						4×2	4	4
						A_4	A_4	1
						D_{12}	D_{12}	1
						D_{12}	S_3	3
						6×2	6	1
						$3\colon D_8$	D_{12}	1
						$\underline{13\colon 4}$	$\underline{D_{26}}$	1

PG(2,25)								
$k = 15$ $N_k = 5709597$			$k = 16$ $N_k = 124577$			$k = 17$ $N_k = 434$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
1	1	5701537	1	1	119311	1	1	313
2	1	2214	2	1	977	2	1	18
2	2	5415	2	2	4112	2	2	84
3	3	386	3	3	24	3	3	3
2^2	2	9	2^2	2	23	4	2	2
S_3	3	10	2^2	2^2	83	4	4	3
S_3	S_3	14	4	2	2	S_3	S_3	6
6	3	10	4	4	6	6	3	1
D_{10}	5	1	5	5	1	4×2	4	1
D_{12}	S_3	1	S_3	S_3	17	8	4	3
			6	3	5			
			D_8	2^2	1			
			D_8	D_8	8			
			4×2	4	1			
			8	4	1			
			D_{10}	D_{10}	2			
			D_{16}	D_{16}	1			
			D_{16}	D_8	2			

PG(2,25)

$k=18$, $N_k=41$						$k=21$, $N_k=1$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
2	1	1	3^2	3^2	1	$\underline{21:6}$	$\underline{21:3}$	1
2	2	4	A_4	A_4	1			
2^2	2	1	D_{12}	D_{12}	1	$k=26$, $N_k=1$		
2^2	2^2	8	D_{12}	S_3	2			
S_3	S_3	5	D_{16}	D_8	1	Γ_S	G_S	#
6	3	1	$S_3 \times 3$	3^2	4	$\underline{\mathrm{P\Gamma L}(2,q)}$	$\underline{\mathrm{PGL}(2,q)}$	1
D_8	2^2	2	$3^2:2$	$3^2:2$	1			
D_8	D_8	2	$\underline{S_4}$	S_4	1			
Q_8	4	1	S_3^2	$3^2:2$	1			
4×2	2^2	1	$\underline{[144]}$	$\underline{[72]}$	1			
4×2	4	1						

PG(2,27)

$k=12$, $N_k=7$			$k=13$, $N_k=221429$			$k=14$, $N_k=106320273$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
S_3	S_3	6	1	1	221342	1	1	106238792
$\underline{S_4}$	$\underline{S_4}$	1	2	2	14	2	2	81129
			3	1	31	3	1	15
			3	3	42	2^2	2^2	224
						4	4	101
						6	2	7
						12	4	3
						$\underline{D_{14}}$	$\underline{D_{14}}$	2

PG(2,27)								
$k = 15$			$k = 16$			$k = 17$		
$N_k = 198631499$			$N_k = 20335114$			$N_k = 276112$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
1	1	198614859	1	1	20291521	1	1	274230
2	2	15506	2	2	42834	2	2	1861
3	1	192	3	1	223	3	1	21
3	3	936	3	3	159			
6	2	2	2^2	2^2	235			
S_3	S_3	4	4	4	19			
			6	2	49			
			S_3	S_3	42			
			D_8	D_8	12			
			3^2	3	1			
			12	4	2			
			6×2	2^2	12			
			A_4	2^2	3			
			$\underline{\mathrm{SL}(2,3)}$	$\underline{Q_8}$	1			
			$\underline{13:6}$	$\underline{D_{26}}$	1			

PG(2,27)								
$k=18$ $N_k=950$			$k=19$ $N_k=5$			$k=22$ $N_k=1$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
1	1	534	2	2	2	$\underline{7:6}$	$\underline{D_{14}}$	1
2	2	333	$\underline{6}$	$\underline{2}$	1			
3	1	3	S_3	S_3	2	$k=28$ $N_k=1$		
3	3	19				Γ_S	G_S	#
2^2	2^2	30				$\underline{\mathrm{P\Gamma L}(2,27)}$	$\underline{\mathrm{PGL}(2,27)}$	1
4	4	3						
$\underline{S_3}$	$\underline{S_3}$	25						
9	3	1						
A_4	A_4	1						
$\underline{3^2:2}$	$\underline{3^2:2}$	1						

PG(2,29)							
$k = 13$		$k = 14$		$k = 15$		$k = 16$	
$N_k = 708$		$N_k = 171139332$		$N_k = 7402140892$		$N_k = 4776509549$	
G_S	#	G_S	#	G_S	#	G_S	#
1	688	1	170929611	1	7402054723	1	4775412456
3	19	2	208889	2	78862	2	1092537
$\underline{13:3}$	1	4	212	3	7266	3	2530
		2: 2	612	5	11	4	104
		D_8	6	S_3	29	2: 2	1643
		$\underline{D_{14}}$	2	D_{10}	1	5	7
						S_3	210
						7	1
						D_8	39
						Q_8	1
						D_{10}	11
						A_4	4
						D_14	5
						$\underline{D_{30}}$	1

PG(2,29)							
$k=17$		$k=18$		$k=19$		$k=20$	
$N_k = 271929757$		$N_k = 2457679$		$N_k = 4190$		$N_k = 57$	
G_S	#	G_S	#	G_S	#	G_S	#
1	271852322	1	2421150	1	3615	1	1
2	77365	2	35080	2	546	2	26
4	68	3	525	3	21	2^2	18
7	1	2^2	529	S_3	8	4	1
D_{14}	1	4	91			D_8	4
		S_3	263			D_{10}	6
		6	1			$\underline{D_{20}}$	1
		D_8	14				
		Q_8	4				
		A_4	13				
		D_{12}	5				
		$\underline{S_4}$	4				

PG(2,29)					
$k=21$		$k=24$		$k=30$	
$N_k = 2$		$N_k = 1$		$N_k = 1$	
G_S	#	G_S	#	G_S	#
$\underline{S_3}$	2	$\underline{\mathrm{PSL}(2,7)}$	1	$\underline{\mathrm{PGL}(2,29)}$	1

5.2 Geometric forms of the complete $(k,2)$-arcs

Many constructions of $(k,2)$-arcs have been described in the literature: some arcs are constructed by adding a small number of points to a subset of a conic [23, 39], some can be obtained as unions of subsets of two distinct conics [17] and others as subsets of points of cubic curves [18, 41, 42, 43]. For this reason we enumerate the complete $(k,2)$-arcs according to their size (columns) and to the type of algebraic curve into which they can be embedded (rows) (the numbers listed refer to PΓL-inequivalent arcs). Each arc is listed with its most specific type. For example, an arc all of whose points belong to an irreducible cubic can also be embedded on a quartic, but will only be listed in the row labelled 'irred. cubic'.

Note that any set of 5 (resp. 9, 14, 20) points always lies on a curve of at least degree 2 (resp. 3, 4, 5), and hence we have restricted ourselves to conics, cubics and quartics. Clearly the only complete arc which lies on a conic is the conic itself.

When the (cubic or quartic) curve to which the arc belongs is reducible, it contains a component curve of lower degree. In that case we have catalogued the arc in a different way. For example, when an arc belongs to a cubic curve which consists of a conic and a line, then the arc can always be obtained by adding at most two points to a subset of a conic, and similar situations occur with reducible quartics. For reasons of brevity we left out the qualifier 'irreducible' in the table for the case of an irreducible cubic with one or two extra points. (If in that case the cubic is reducible, we obtain arcs that can be obtained from a subset of a conic by adding 3 or 4 points.)

q=5		6	total
	conic	1	1

q=7		6	8	total
	conic		1	1
	conic + 1 point	1		1

		6	10	total
q=8	conic + 1 point	1	1	2

		6	7	8	10	total
q=9	conic				1	1
	conic + 1 point	1				1
	conic + 2 points		1	1		2

		7	8	9	10	12	total
q=11	conic					1	1
	irred. cubic			2			2
	conic + 1 point		3				3
	conic + 2 points	1	6	1			8
	cubic + 1 point				1		1

		8	9	10	12	14	total
q=13	conic					1	1
	irred. cubic		14	4			18
	conic + 1 point	1	2				3
	conic + 2 points	1	13	2			16
	conic + 3 points			4			4
	cubic + 1 point			11			11
	conic + 4 points				1		1

q=16		9	10	11	12	13	18	total
	irred. cubic	2	21	1	1			25
	conic + 1 point		6				1	7
	conic + 2 points		32	1				33
	conic + 3 points		119	7	1			127
	cubic + 1 point		323	7				330
	conic + 4 points			4	2			6
	cubic + 2 points			10	5			15
	2 conics					1		1
	other						1	1

q=17		10	11	12	13	14	18	total
	conic						1	1
	irred. cubic	19	2	9	1			31
	conic + 1 point	5	7					12
	conic + 2 points	35	27	3				65
	conic + 3 points	122	307	17				446
	cubic + 1 point	379	1071	23	1			1474
	conic + 4 points	282	96	1	1			380
	cubic + 2 points		948	396				1344
	2 conics			9	4			13
	irred. quartic				1			1

q=19		10	11	12	13	14	20	total
	conic						1	1
	irred. cubic	2	18	25	2	2		49
	conic + 1 point		7	21				28
	conic + 2 points	3	51	85	1			140
	conic + 3 points	7	857	536	9	1		1410
	cubic + 1 point	17	3589	911	26			4543
	conic + 4 points		932	3925	83	2		4942
	cubic + 2 points		4087	24166	337	4		28594
	2 conics			465	1082	28		1575
	irred. quartic			1	692	33		726

q=23		10	12	13	14	15
	conic					
	irred. cubic		32	21	6	7
	conic + 1 point			48	59	
	conic + 2 points		92	453	147	3
	conic + 3 points	1	854	5513	715	8
	cubic + 1 point		1941	5577	676	28
	conic + 4 points		8965	72263	6112	46
	cubic + 2 points		96323	429343	15495	157
	2 conics		4203	1443866	130824	1083
	irred. quartic		39	2384430	1674162	3020
	other					54009

q=23		16	17	24	total
	conic			1	1
	irred. cubic	4			70
	conic + 1 point				107
	conic + 2 points				695
	conic + 3 points				7091
	cubic + 1 point	2			8224
	conic + 4 points	6			87392
	cubic + 2 points	2			541320
	2 conics	48			1580024
	irred. quartic	52			4061703
	other	450	5		54464

q=25		12	13	14	15
	irr.cubic	1	24	23	3
	conic + 1			67	48
	conic + 2	1	148	613	66
	conic + 3	9	2949	5003	297
	cubic + 1	18	3154	3409	381
	conic + 4	85	45638	55273	2338
	cubic + 2	468	355525	155364	4257
	2 conics	21	1099870	1434419	49669
	irr.quart.	3	2565237	27497260	220805
	other				5431733

q=25		16	17	18	21	total
	irr.cubic	5	2	4		62
	conic + 1					115
	conic + 2	3				831
	conic + 3	6				8264
	cubic + 1	28				6990
	conic + 4	34	1			103369
	cubic + 2	74	1			515689
	2 conics	521	1	7		2584508
	irr.quart.	784	11	2		30284102
	other	123122	418	28	1	5555302

q=27		12	13	14	15	16
	conic					
	irr.cubic		1	31	6	3
	conic + 1				79	69
	conic + 2		7	527	561	96
	conic + 3		61	8792	4689	202
	cubic + 1		136	4435	2261	270
	conic + 4	2	1667	123432	43818	1255
	cubic + 2	5	17104	387014	65361	2272
	2 conics		48557	3713947	1087165	21750
	irr.quart.		153896	102082095	7159569	30705
	other				190267990	20278492

q=27		17	18	19	22	28	total
	conic					1	1
	irr.cubic		4	1			46
	conic + 1						148
	conic + 2						1191
	conic + 3	1	1				13746
	cubic + 1	24					7126
	conic + 4	3					170177
	cubic + 2	48	2				471806
	2 conics	104	8				4871531
	irr.quart.	61	14	2			109426342
	other	275871	921	2	1		210823277

q=29		13	14	15	16	17
	conic					
	irr.cubic		25	106	18	3
	conic + 1				508	305
	conic + 2		266	3761	2769	249
	conic + 3		6518	64204	17739	620
	cubic + 1		4218	20893	8600	942
	conic + 4	2	117712	849236	139307	2755
	cubic + 2	36	486746	1292115	145957	4327
	2 conics	140	4295022	26135224	2873149	35581
	irr.quart.	530	166228825	251767733	5520429	12258
	other			7122007620	4767801073	271872717

q=29		18	19	20	21	24	30	total
	conic						1	1
	irr.cubic	20	2	3				177
	conic + 1							813
	conic + 2	14						7059
	conic + 3	12						89093
	cubic + 1	67						34720
	conic + 4	43						1109055
	cubic + 2	83	1					1929265
	2 conics	471	4	4				33339595
	irr.quart.	277		4		1		423530057
	other	2456692	4183	46	2			12164142333

5.3 The $(k,2)$-arcs of $\mathrm{PG}(2,q)$, $q \leq 29$, not necessarily complete

Finally, in the following two tables we list the number of PGL-inequivalent k-arcs in $\mathrm{PG}(2,q)$, $q \leq 29$, not necessarily complete. To obtain these results we used the same algorithms of Chapter 4, except that we do not filter for completeness. Running times are essentially the same as for complete arcs.

	$q=5$	$q=7$	$q=8$	$q=9$	$q=11$	$q=13$	$q=16$	$q=17$
$k=4$	1	1	1	1	1	1	1	1
$k=5$	1	1	1	2	2	3	4	4
$k=6$	1	3	5	7	15	26	61	74
$k=7$		1	2	4	21	80	454	733
$k=8$		1	2	2	21	181	2633	5441
$k=9$			2	1	5	110	6014	17633
$k=10$			1	1	2	27	4899	21064
$k=11$					1	2	1171	6814
$k=12$					1	2	587	629
$k=13$						1	260	15
$k=14$						1	100	4
$k=15$							30	1
$k=16$							9	1
$k=17$							3	1
$k=18$							2	1

	$q=19$	$q=23$	$q=25$	$q=27$	$q=29$
$k=4$	1	1	1	1	1
$k=5$	5	6	8	4	10
$k=6$	117	257	365	174	682
$k=7$	1768	7613	14114	8261	41301
$k=8$	20361	172416	419385	311313	1933469
$k=9$	115492	2235523	7490938	7348659	58423579
$k=10$	280104	15032508	74026338	101047498	1072049736
$k=11$	235320	46333282	366007216	744145433	11123944005
$k=12$	55708	56846595	806719354	2665334400	60140705285
$k=13$	2733	23362684	690593155	4145194407	153994534160
$k=14$	83	2634266	195308347	2452359922	167238862321
$k=15$	5	64773	15070303	472714330	67799467128
$k=16$	4	692	263843	24808360	8854773945
$k=17$	1	41	1492	290532	314349510
$k=18$	1	22	222	1431	2540088
$k=19$	1	6	58	183	7280
$k=20$	1	4	29	82	1477
$k=21$		1	9	32	646
$k=22$		1	5	15	293
$k=23$		1	1	4	98
$k=24$		1	1	3	43
$k=25$			1	1	10
$k=26$			1	1	5
$k=27$				1	1
$k=28$				1	1
$k=29$					1

5.4 The complete $(k,3)$-arcs of $\mathrm{PG}(2,q)$, $q \leq 13$

For the complete $(k,3)$-arcs we have also determined the subgroups G_S of $\mathrm{PGL}(3,q)$ and Γ_S of $\mathrm{P\Gamma L}(3,q)$ that stabilize the set S of points of the arc. The results are summarised in the tables below.

Our programs, which were written in Java, were run on a cluster of Debian Linux systems with 56 quad core Intel Xeon X3220 2.40GHz processors. The generation of all complete arcs of $\mathrm{PG}(2,11)$ up to equivalence takes approximately 6 hours of CPU time. For $q = 13$ it takes approximately 152 days of CPU time. The generation for all $q \leq 9$ takes less than half an hour. To store the results (in compressed form) we need about 35 MByte of disk space for $q = 11$ and about 14 GByte for $q = 13$.

PG(2,5)

$k = 9$		$k = 10$		$k = 11$	
$N_k = 2$		$N_k = 2$		$N_k = 2$	
G_S	#	G_S	#	G_S	#
S_3	1	3	2	D_8	1
D_{12}	1			5 : 4	1

PG(2,7)

$k = 9$		$k = 11$		$k = 12$		$k = 13$		$k = 14$		$k = 15$	
$N_k = 1$		$N_k = 8$		$N_k = 69$		$N_k = 44$		$N_k = 2$		$N_k = 1$	
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
$\underline{[216]}$	1	1	1	1	55	1	23	1	1	$S_4 : 3$	1
		2	4	2	4	2	15	6	1		
		2^2	1	3	7	3	2				
		$\underline{S_3}$	2	S_3	1	2^2	2				
				$\underline{3^2}$	1	S_3	2				
				$3S_3$	1						

PG(2,8)														
$k=11$ $N_k=2$			$k=12$ $N_k=8$			$k=13$ $N_k=230$			$k=14$ $N_k=158$			$k=15$ $N_k=19$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
2	2	1	1	1	6	1	1	193	1	1	157	1	1	7
$\underline{2A_4}$	$\underline{2^3}$	1	3	1	1	3	1	5	6	2	1	3	1	4
			3	3	1	2	2	22				2	2	1
						6	2	1				3	3	1
						3	3	6				12	4	1
						4	12	1				2^2	2^2	2
						S_3	S_3	1				S_3	S_3	1
						$3S_3$	S_3	1				$\underline{3A_4}$	$\underline{A_4}$	2

PG(2,9)								
$k=12$ $N_k=4$			$k=13$ $N_k=245$			$k=14$ $N_k=3673$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
4	2	1	1	1	177	1	1	3577
D_{12}	S_3	1	2	1	30	2	1	79
$\underline{3^2:Q_8}$	$\underline{3^2:4}$	1	2	2	27	2	2	12
$\underline{3^2:D_{12}}$	$\underline{3^2:6}$	1	2^2	2	3	2^2	2	4
			3	3	2	$\underline{4}$	$\underline{4}$	1
			6	3	2			
			S_3	3	1			
			2^2	2^2	2			
			D_{12}	S_3	1			

PG(2,9)								
$k = 15$ $N_k = 4014$			$k = 16$ $N_k = 335$			$k = 17$ $N_k = 4$		
Γ_S	G_S	#	Γ_S	G_S	#	Γ_S	G_S	#
1	1	3704	1	1	296	1	1	1
2	1	115	2	1	21	2	1	2
2	2	125	2	2	7	2	2	1
4	2	1	3	3	5			
2^2	2	10	6	3	1			
3	3	28	4	4	1			
6	3	4	2^2	2^2	1			
S_3	3	13	5	5	1			
4	4	1	12	6	1			
2^2	2^2	3	$\underline{(3:4):2}$	$\underline{3:4}$	1			
D_8	2^2	1						
6	6	1						
6×2	6	1						
S_3	S_3	3						
D_{12}	S_3	3						
$\underline{D_{10}}$	$\underline{D_{10}}$	1						

PG(2,11)							
$k=13$		$k=14$		$k=15$		$k=16$	
$N_k=5$		$N_k=146$		$N_k=71584$		$N_k=1574490$	
G_S	#	G_S	#	G_S	#	G_S	#
2	1	1	138	1	70705	1	1573677
6	1	2	8	2	794	2	613
S_3	2			3	56	3	196
$\underline{D_{10}}$	1			2^2	6	2^2	1
				4	2	6	2
				6	2	S_3	1
				S_3	15		
				$\underline{D_{10}}$	2		
				$\underline{S_4}$	2		

PG(2,11)									
$k=17$		$k=18$		$k=19$		$k=20$		$k=21$	
$N_k=2082781$		$N_k=259585$		$N_k=4176$		$N_k=15$		$N_k=2$	
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
1	2078955	1	259174	1	4055	1	13	$\underline{7:3}$	2
2	3782	2	234	2	76	2	2		
2^2	20	3	166	3	35				
4	9	2^2	1	2^2	5				
$\underline{5}$	5	4	4	4	1				
8	1	$\underline{5}$	1	S_3	3				
D_8	5	S_3	3	$\underline{19:3}$	1				
Q_8	1	A_4	1						
$\underline{D_{10}}$	3	$\underline{S_4}$	1						

PG(2,13)							
$k = 15$		$k = 16$		$k = 17$		$k = 18$	
$N_k = 33$		$N_k = 95497$		$N_k = 27833779$		$N_k = 487287851$	
G_S	#	G_S	#	G_S	#	G_S	#
1	13	1	95149	1	27819765	1	487274273
2	4	2	314	2	13907	2	10588
3	10	3	25	3	54	3	2927
6	3	4	4	2^2	26	2^2	2
S_3	2	6	1	4	1	4	11
$\underline{[36]}$	1	S_3	4	6	1	6	13
				S_3	23	S_3	18
				D_8	2	3^2	15
						$3S_3$	1
						$\underline{S_4}$	1
						$\underline{3^{1+2}_+}$	1
						$\underline{[36]}$	1

PG(2,13)									
$k=19$ $N_k=644018777$		$k=20$ $N_k=96109026$		$k=21$ $N_k=2300204$		$k=22$ $N_k=9669$		$k=23$ $N_k=7$	
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
1	643963031	1	96105103	1	2297792	1	9618	1	5
2	55128	2	3733	2	1954	2	28	2	1
3	459	3	161	3	425	3	16	4	1
2^2	78	2^2	2	2^2	9	4	4		
4	59	4	24	4	3	6	1		
6	1	6	3	6	8	S_3	1		
S_3	14			S_3	6	7	1		
D_8	7			$\underline{3^2}$	2				
				$\underline{D_{12}}$	2				
				$\underline{D_{14}}$	1				
				$\underline{3S_3}$	2				

5.5 Regular $(k,3)$-arcs of $\mathrm{PG}(2,q)$, $q \leq 13$

Among the complete $(k,3)$-arcs of $\mathrm{PG}(2,q), 7 \leq q \leq 13$ there are a few that are *regular* in the sense that every point of the arc lies on the same number of trisecants to that arc (and hence also the same number of bisecants and unisecants). We list some information on these arcs in the following table. k denotes the size of the arcs, u, b and t denote the number of unisecants, bisecants and trisecants respectively through each point of the arc and # denotes the number of distinct arcs up to PΓL-equivalence of that size with corresponding number of unisecants, bisecants and trisecants.

PG(2,7)					PG(2,8)					PG(2,9)				
#	k	u	b	t	#	k	u	b	t	#	k	u	b	t
1	9	4	0	4	1	15	0	4	5	4	15	1	4	5
1	14	1	1	6						4	15	2	2	6
1	15	0	2	6						2	16	1	3	6

PG(2,11)					PG(2,13)				
#	k	u	b	t	#	k	u	b	t
2	15	3	4	5	2	15	6	2	6
7	15	4	2	6	4	17	4	4	6
9	16	3	3	6	1	18	5	1	8
21	17	2	4	6	30	18	4	3	7
1	18	1	5	6	12	18	3	5	6
11	18	2	3	7	2	19	2	6	6
1	19	3	0	9	1	21	2	4	8
2	21	1	2	9	3	21	3	2	9

5.6 The $(k,2)$- and $(k,3)$-arcs of $\mathrm{PG}(2,q)$, $q \leq 13$, not necessarily complete

Below we list the number of PGL-inequivalent arcs in $\mathrm{PG}(2,q), q \leq 13$, not necessarily complete. To obtain these results we used the same algorithm of Chapter 4, except that we do not filter for completeness. Running times are

essentially the same as for complete arcs.

	$q=5$	$q=7$	$q=8$	$q=9$	$q=11$	$q=13$
$k=4$	2	2	2	2	2	2
$k=5$	3	4	3	5	5	7
$k=6$	8	17	20	31	52	88
$k=7$	13	54	100	192	564	1429
$k=8$	13	181	507	1343	6764	25851
$k=9$	16	526	2250	8232	70555	405923
$k=10$	7	907	6681	36573	574777	5175927
$k=11$	2	923	12664	111833	3520995	52242283
$k=12$		395	12781	209172	15291648	403124643
$k=13$		65	5822	211818	44020760	2282452775
$k=14$		4	871	97050	76936027	9001288813
$k=15$		1	43	16386	73157838	23188169036
$k=16$				734	32916332	36058738738
$k=17$				6	5884405	30742092308
$k=18$					333858	12779923892
$k=19$					4467	2246238494
$k=20$					17	140208097
$k=21$					2	2507054
$k=22$						9805
$k=23$						7

6

Special $(k,2)$-arcs in $\mathrm{PG}(2,q), q \leq 29$

One of the purposes of doing a computer classification as in this text is to gain further insight into the general class of objects under investigation. In our case we hope to find patterns in the vast amount of data which may for instance allow us, or other researchers, to derive new general constructions of arcs that also work for larger fields. Using the results presented in Chapter 5, we managed to discover several general types of arc. These are described in Sections 6.1, 6.2 and 6.3. In Sections 6.4-6.14, we have a closer look at some of the arcs for each q up to 29.

6.1 Well-known constructions

Some $(k,2)$-arcs have well-known constructions that can be generalized. Examples have already been given in Chapter 3. We describe three more constructions below.

First, it is well known that a conic has size $q+1$ and is a $(q+1,2)$-arc. Also, when q is odd, it is the largest possible arc in PG$(2,q)$. When q is even, the conic is not a complete arc: one can always add the nucleus to the conic. This new set is a $(q+2,2)$-arc and is called a hyperoval.

Secondly, consider an absolutely irreducible cubic curve $\mathcal{F}$. As mentioned before, the rational non-singular points of the cubic form an abelian group $G_{\mathcal{F}}$. If the order of $\mathcal{F}$ is even, then we can find a $(k,2)$-arc of size $|G_{\mathcal{F}}|/2$ (see [42]):

Lemma 6.1 *Consider the abelian group $G_{\mathcal{F}}$ of an absolutely irreducible cubic curve $\mathcal{F}$ with an even number of points. Let $H_{\mathcal{F}}$ be a subgroup of index 2 of $G_{\mathcal{F}}$ with identity O. Let O' be the second point on the tangent through O. If $O' \in H_{\mathcal{F}}$, then the coset $H^*_{\mathcal{F}} = G_{\mathcal{F}} \backslash H_{\mathcal{F}}$ of $H_{\mathcal{F}}$ is a $(k,2)$-arc. If $O' \notin H_{\mathcal{F}}$, then the subgroup $H_{\mathcal{F}}$ itself is a $(k,2)$-arc.*

Proof : Three points P, Q and R are collinear if and only if $P \oplus Q \oplus R = O'$. First, assume $O' \in H_{\mathcal{F}}$ and let $P, Q, R \in H^*_{\mathcal{F}}$.

$$P \oplus Q \oplus R \in P \oplus P \oplus H_{\mathcal{F}} \oplus P \oplus H_{\mathcal{F}} = 3P \oplus H_{\mathcal{F}} = P \oplus H_{\mathcal{F}} = H^*_{\mathcal{F}}$$

in which the last step makes use of $2P \in H_{\mathcal{F}}$ (because $H_{\mathcal{F}}$ is a subgroup of index 2 of $G_{\mathcal{F}}$). This implies $P \oplus Q \oplus R \neq O'$. Hence three points of the coset $H^*_{\mathcal{F}}$ never are collinear and $H^*_{\mathcal{F}}$ is a $(k,2)$-arc.

Secondly, assume $O' \notin H_{\mathcal{F}}$ and let $P, Q, R \in H_{\mathcal{F}}$. Then $P \oplus Q \oplus R \in H_{\mathcal{F}}$ and again $P \oplus Q \oplus R \neq O'$. Therefore, in this case three points of $H_{\mathcal{F}}$ are never collinear and hence $H_{\mathcal{F}}$ is a $(k,2)$-arc. ∎

Note that if O is an inflexion point, then $O' = O \in H_{\mathcal{F}}$.

A third kind of a known arc is related to a Singer cycle. A projectivity g which permutes the points of $\mathrm{PG}(2,q)$ in a single cycle is called a cyclic projectivity or *Singer cycle*. The order of a Singer cycle is q^2+q+1. Let $a, b \in \mathbb{R}$, such that $ab = q^2+q+1$. The a-th power of a Singer cycle then has order b and the orbit x^{g^a} of a point $x \in \mathrm{PG}(2,q)$ has size b. In some cases, such an orbit x^{g^a} is a $(k,2)$-arc. In that case it is called a *cyclic* arc [40]. The subgroup of the Singer cycle generated by g^a is evidently a group of automorphisms of the arc, but usually the full stabilizer group G_S turns out to be somewhat larger.

For every field of square order, an orbit of the $(q+\sqrt{q}+1)$-th power of a Singer cycle always is a complete arc of size $q-\sqrt{q}+1$. Alternatively, this arc can be constructed as an intersection of two Hermitian curves [4, 16, 22]. For $q=9$ this arc has size 7 with $\Gamma_S \approx 7\colon 6$ and $G_S \approx 7\colon 3$, for $q=16$ it has size 13 with $\Gamma_S \approx 13\colon 12$ and $G_S \approx 13\colon 3$ and for $q=25$ it has size 21 with $\Gamma_S \approx 21\colon 6$ and $G_S \approx 21\colon 3$.

Note that also $(k,3)$-arcs can often be constructed in this way.

6.2 Some arcs with automorphism group S_4

Among the results, there are some arcs that accept the symmetric group S_4 of degree 4 (and order 24) as a group of automorphisms. These arcs can be generalized to other values of q. There are three types of arc, one of size 10, one of size 12 and one of size 18.

Theorem 6.2 *Let $a \in \mathbb{F}_q$, q odd. Let $S^*(a)$ denote the set of points of $\mathrm{PG}(2,q)$ with coordinates of the form $(a,\pm1,\pm1)$, $(\pm1,a,\pm1)$ or $(\pm1,\pm1,a)$, with independent choices of sign.*

Then $S^*(a)$ $(= S^*(-a))$ is a $(12,2)$-arc of $\mathrm{PG}(2,q)$ if and only if

$$a \notin \{0, \pm1, \pm2, \pm\sqrt{-1}, \pm\sqrt{-3}, \frac{1}{2}(\pm1 \pm \sqrt{-7})\}. \tag{6.1}$$

If these conditions hold, then

- *If $a^2 = -2$, the points of $S^*(a)$ lie on the conic C with equation*

$$C : x^2 + y^2 + z^2 = 0,$$

- *Otherwise, $S^*(a)$ is the disjoint union of three sets $C_0 \cap C_1$, $C_1 \cap C_2$, $C_2 \cap C_0$ of size 4 which are the pairwise intersections of the three conics C_0, C_1, C_2 with equations*

$$\begin{aligned} C_0 : (a^2+1)x^2 &= y^2 + z^2, \\ C_1 : (a^2+1)y^2 &= z^2 + x^2, \\ C_2 : (a^2+1)z^2 &= x^2 + y^2. \end{aligned}$$

Proof : We leave it to the reader to verify that $|S^*(a)| = 12$ if and only if $a \neq 0, 1$ or -1.

We first consider the case $a^2 = -1$. Note that in that case the four points with coordinates $(a, 1, \pm 1)$ and $(-1, a, \pm 1)$ lie on the line with equation $x = ay$, and then $S^*(a)$ is not an arc.

If $a^2 \neq -1$, the conics C_0, C_1, C_2 are nondegenerate. It is easily seen that any point with coordinates of the form $(a, \pm 1, \pm 1)$ lies on the conic C_1 and C_2. Similarly $(\pm 1, a, \pm 1) \in C_2 \cap C_0$ and $(\pm 1, \pm 1, a) \in C_0 \cap C_1$. It also follows that $C_0 \cap C_1 \cap C_2$ will be nonempty if and only if $a^2 = 1$ or $a^2 = -2$. In the first case $|S^*(a)| < 12$, in the second case we have $C_0 = C_1 = C_2 = C$.

Because different (nondegenerate) conics can intersect in at most 4 points, this proves our claim that $S^*(a)$ is the disjoint union of these three intersections, when (6.1) holds and $a^2 \neq -2$.

The set $S^*(a)$ is not an arc if and only if there exist three different points of $S^*(a)$ that are collinear. Note that for any pair of points in $S^*(a)$ there is a conic $C_i, i = 0, 1, 2$ that contains this pair. Because conics are arcs, a third point of $S^*(a)$ collinear to this pair cannot lie on that same conic. It follows

that any collinear triple must consist of one point with coordinates of the form $(a, \pm 1, \pm 1)$, one with coordinates of the form $(\pm 1, a, \pm 1)$ and one with coordinates of the form $(\pm 1, \pm 1, a)$.

In other words, $S^*(a)$ is not an arc if and only if

$$\begin{vmatrix} a & \pm 1 & \pm 1 \\ \pm 1 & a & \pm 1 \\ \pm 1 & \pm 1 & a \end{vmatrix} = 0,$$

for at least one of the 64 different sign combinations in this determinant.

By multiplying the second and third rows and columns of this determinant by -1 if necessary, we may reduce this condition to

$$\begin{vmatrix} a & 1 & 1 \\ 1 & \pm a & \pm 1 \\ 1 & \pm 1 & \pm a \end{vmatrix} = 0,$$

which, after multiplying the second and third row by a and subtracting the first row, reduces to

$$(1 \pm a^2)(1 \pm a^2) = (1 \pm a)(1 \pm a),$$

with 16 different combinations of signs. Note however that the left hand side of this equation can only take three different values and the same holds for right hand side. This leaves us 9 conditions in all. The following table lists the 9 differences between the possible values of the left hand sides (rows) and right hand sides (columns):

	$(1+a)^2$	$(1-a)^2$	$1-a^2$
$(1+a^2)^2$	$a(a-1)(a^2+a+2)$	$a(a+1)(a^2-a+2)$	$a^2(a^2+3)$
$(1-a^2)^2$	$a(a-2)(a+1)^2$	$a(a+2)(a-1)^2$	$a^2(a-1)(a+1)$
$1-a^4$	$-a(a+1)(a^2-a+2)$	$-a(a-1)(a^2+a+2)$	$-a^2(a-1)(a+1)$

(Note that the second column can be obtained from the first by substituting $-a$ for a. This is a consequence of the fact that $S^*(a) = S^*(-a)$.)

The set $S^*(a)$ is not an arc if and only if any of the 9 entries in this table becomes zero, or equivalently, if and only if at least one of the factors of one of these entries becomes zero. These factors are

$$a, a-1, a+1, a-2, a+2, a^2+3, a^2-a+2, a^2+a+2,$$

whence the values of a listed in (6.1). ∎

Clearly any permutation of the three coordinates fixes $S^*(a)$. Also, changing the sign of one or more of the coordinates fixes $S^*(a)$. The group generated by these transformations is therefore a group of automorphisms of $S^*(a)$. This group is isomorphic to the symmetric group S_4 (see Section 2.7).

We can also represent the arc $S^*(a)$ as embedded in the hyperplane of $\mathrm{PG}(3,q)$ with equation $x+y+z+u=0$. The arc then consists of the points whose coordinates are the permutations of $(a, a, -a-2, -a+2)$. The group S_4 of automorphisms acts on this representation by permuting the four coordinates.

Coordinates for the points of the arc $S^*(a)$ for the case $q = 27$ were already given by Marcugini et al. [31], where it is also mentioned that the arc consists of a single orbit of its group S_4 of automorphisms. They also report that there are three conics that each intersect the arc in 8 points. However, they did not provide a description for general q.

In general the arc $S^*(a)$ is not complete. The following theorem shows that for $q = 1 \bmod 4$ and for certain values of a, (at least) six additional points can be added.

Theorem 6.3 *Let $q = 1 \bmod 4$. Let $a, i \in \mathbb{F}_q$, such that $i^2 = -1$. Let $S^*(a)$ be defined as in Theorem 6.2. Let I denote the set of six points whose coordinates are permutations of $(1, i, 0)$. (I is a subset of the conic $C : x^2+y^2+z^2 = 0$.)*

Then $S^*(a) \cup I$ is an $(18,2)$-arc of $\mathrm{PG}(2,q)$ if and only if

$$a \notin \{0, \pm 1, \pm 2, \pm i, \pm 2i, \pm i\sqrt{3}, \pm i \pm 1, \frac{1}{2}(\pm 1 \pm i\sqrt{7}), \frac{1}{2}(\pm i \pm \sqrt{-5 \pm 4i})\}. \tag{6.2}$$

Proof : Note that the coordinates $(1, i, 0)$ and $(i, -1, 0)$ represent the same point (analogous for the other points in I). Hence I is an orbit of size 6 of S_4.

For $S^*(a) \cup I$ to be an arc $S^*(a)$ must be an arc, and therefore all conditions of Theorem 6.2 must be fullfilled. Also I must be an arc, but this is trivially true as I is a subset of a conic.

Therefore, if $S^*(a)$ is an arc then $S^*(a) \cup I$ will not be an arc if and only if it contains a collinear triple that intersects both $S^*(a)$ and I.

Because S_4 acts transitively on $S^*(a)$ and I we may without loss of generality assume that the collinear triple contains the point P with coordinates $(1, 1, a)$.

Interchanging the first two coordinates leaves P invariant and the stabilizer of P splits I into three pairs as follows:

$$\begin{array}{lllllll} Q_1 & = & (1,i,0) & \text{and} & Q_1' & = & (i,1,0), \\ Q_2 & = & (0,1,i) & \text{and} & Q_2' & = & (1,0,i), \\ Q_3 & = & (0,i,1) & \text{and} & Q_3' & = & (i,0,1). \end{array}$$

Hence, taking Q_1, Q_2 and Q_3 as representatives for these orbits, it suffices to show that for each $i = 1, 2, 3$ the line PQ_i contains no other points of $S^*(a)$ and I.

However, applying the simultanous substituion of z by $-z$ and a by $-a$ to Q_2 yields Q_3 and leaves P invariant. This implies that PQ_3 will contain a third point of $S^*(a) \cup I$ if and only if PQ_2 does so. Hence we do not need to investigate the line PQ_3.

We have:

1. PQ_1 has equation $f_1(x, y, z) = ax + iay - (i + 1)z = 0$,
2. PQ_2 has equation $f_2(x, y, z) = (i - a)x - iy + z) = 0$.

In Table 6.1 we list the values of $f_i(r)$ for each point r in the sets $S^*(a)$ and I. For $S^*(a) \cup I$ to be a $(k, 2)$-arc, both colums $f_1(r)$ and $f_2(r)$ may contain

		$f_1(r)$ $ax+iay-(i+1)z$	$f_2(r)$ $(i-a)x-iy+z$
$S^*(a)$	$(1,1,a)$	0	0
	$(-1,-1,a)$	$-2(i+1)a$	$2a$
	$(1,-1,a)$	$-2ia$	$2i$
	$(-1,1,a)$	$-2a$	$2(a-i)$
	$(1,a,1)$	$(a-1)(ia+i+1)$	$-(a-1)(i+1)$
	$(1,a,-1)$	$ia^2+a+i+1$	$-(i+1)a+i-1$
	$(-1,a,-1)$	$ia^2-a+i+1$	$-(i-1)a-i-1$
	$(-1,a,1)$	$(a+1)(ia-i-1)$	$-(i-1)(a+1)$
	$(a,1,1)$	$(a-1)(a+i+1)$	$-(a-1)(a-i+1)$
	$(a,-1,-1)$	$a^2-ia+i+1$	$-a^2+ia+i-1$
	$(a,1,-1)$	$a^2+ia+i+1$	$-a^2+ia-i-1$
	$(a,-1,1)$	$(a+1)(a-i-1)$	$-(a+1)(a-i-1)$
I	$(1,i,0)$	0	$-a+i+1$
	$(1,0,i)$	$a-i+1$	$2i-a$
	$(0,1,i)$	$ia-i+1$	0
	$(0,i,1)$	$-(a+i+1)$	2
	$(i,1,0)$	$2ia$	$-(ia+i+1)$
	$(i,0,1)$	$ia-i-1$	$-ia$

Table 6.1: Lists the values of $f_i(r)$ for each of the points in the left column (cf. proof of Theorem 6.3) and Theorem 7.2.

q	a	$S^*(a)$	$S^*(a) \cup I$
11	± 3	complete	
13	$\pm 3, \pm 4$	complete	
17	$\pm 3, \pm 5, \pm 6$	complete	
	± 7	not complete	complete
	± 8	not complete	
19	$\pm 3, \pm 5, \pm 7, \pm 8, \pm 9$	complete	
	± 6	not complete	
23	$\pm 7, \pm 8$	complete	
	$\pm 3, \pm 4, \pm 5, \pm 6, \pm 11$	not complete	
25	$\pm \alpha^9$	not complete	not complete
	$\pm \alpha^2, \pm \alpha^7, \pm \alpha^{10}, \pm \alpha^{11}$	not complete	
	$\pm \alpha^4, \pm \alpha^8$	not complete	complete
27	$\pm \alpha^7, \pm \alpha^8, \pm \alpha^{11}$	complete	
	$\pm \alpha, \pm \alpha^2, \pm \alpha^3, \pm \alpha^4, \pm \alpha^5$	not complete	
	$\pm \alpha^6, \pm \alpha^9, \pm \alpha^{10}, \pm \alpha^{12}$	not complete	
29	$\pm 4, \pm 6, \pm 9, \pm 10$	not complete	complete
	$\pm 3, \pm 5, \pm 11, \pm 13, \pm 14$	not complete	

Table 6.2: Lists the values of a for which an arc of type $S^*(a)$ or $S^*(a) \cup I$ exists for all $q \leq 29$.

at most two zeroes. We find that apart from the conditions of Theorem 6.2, a also needs to satisfy $a \neq \pm 2i, \pm i \pm 1$ and $a^2 \pm ai + (1 \pm i) \neq 0$. ∎

When $a^2 = -2$ all points of this arc lie on the conic C. When $a^2 \neq -2$ each of the conics C_0, C_1, C_2 (cf. Theorem 6.2) contains two points of I.

In Table 6.2 we present the values of a for which an arc of type $S^*(a)$ of size 12 or $S^*(a) \cup I$ of size 18 exists for all $q \leq 29$. If the arc exists, the table mentions whether the arc is complete or not. If the set is not a $(k, 2)$-arc, then the space is left blank.

For $a = 1$, the set $S^*(a)$ reduces to a set of size 4. This set lies on the conic with equation $x^2 + y^2 - 2z^2 = 0$ and therefore is a $(k,2)$-arc. This arc never is complete. In some cases, the set I can be added to $S^*(1)$:

Theorem 6.4 *Let $q = 1 \bmod 4$. Let $i \in \mathbb{F}_q$, such that $i^2 = -1$. Let $S^*(1)$ denote the set of points of $\mathrm{PG}(2,q)$ with coordinates $(1,1,1)$, $(-1,1,1)$, $(1,-1,1)$ or $(1,1,-1)$. Let I be defined as in Theorem 6.3.*

Then $S^*(1) \cup I$ is a $(10,2)$-arc of $\mathrm{PG}(2,q)$ if and only if $i \neq \pm 2$.

Proof : To prove that $S^*(1) \cup I$ is an arc, we have to show that no triple of collinear points of $S^*(1) \cup I$ exists. Both sets $S^*(1)$ and I are arcs, so a collinear triple must contain at least one point of both sets. Because of the automorphisms of $S^*(1)$ we may chose an arbitrary element of this set as the first point of each triple, say $R(1,1,1)$. Permuting the coordinates leaves P invariant. The set I is also left invariant when permuting the coordinates. Therefore, taking $Q_1(1,i,0)$ as representative of this orbit, it suffices to show that the line RQ_1 does not contain any other point of $S^*(1) \cup I$. This line has equation $f(x,y,z) = x + iy - (i+1)z = 0$. The values of $f(r)$ for each point r of $S^*(1) \cup I$ are listed in Table 6.3. Clearly, when $i \neq \pm 2$, this colum contains no three zeroes, so $S^*(1) \cup I$ is indeed a $(k,2)$-arc. ∎

In the following table we list the values of q for wich the set $S^*(1) \cup I$ is an arc.

q	$S^*(1) \cup I$
9	complete
13	complete
17	complete
29	not complete

The symmetric group S_4 clearly is a group of automorphisms of the sets $S^*(a)$, $S^*(1)$ and I. However, in some cases, S_4 is not the full automorphism group of $S^*(a)$. For instance, if $q \equiv 1 \pmod 3$ and $a^3 = 1$, $a \neq 1$, then $(x,y,z) \mapsto (x, ay, a^2 z)$ extends the group of automorphisms of $S^*(a)$ to $S_4 : 3$.

		$f_1(r)$ $x+iy-(1+i)z$
$S^*(1)$	$(1,1,1)$	0
	$(1,1,-1)$	$2+2i$
	$(1,-1,1)$	$-2i$
	$(-1,1,1)$	-2
I	$(1,i,0)$	0
	$(1,0,i)$	$2-i$
	$(0,1,i)$	1
	$(0,i,1)$	$-2-i$
	$(1,-i,0)$	2
	$(1,0,-i)$	i

Table 6.3: Lists the values of $f(r)$ for each of the points in the left column (cf. proof of Theorem 6.4).

6.3 Some arcs with automorphism group A_5

For $q = 0, 1$ or $4 \bmod 5$, q odd, we will describe two sets of points in the plane that are $(k,2)$-arcs having the alternating group on five elements as a group of automorphisms.

Theorem 6.5 *Let $q = 0, 1$ or 4 mod 5, q odd. Let $\tau = \frac{\sqrt{5}+1}{2}$. Consider the following sets:*

$$R = \{(0,1,\pm\tau),(1,\pm\tau,0),(\pm\tau,0,1)\}$$

$$S = \{(0,\pm\tau,\pm\tau^{-1}),(\pm\tau,\pm\tau^{-1},0),(\pm\tau^{-1},0,\pm\tau),(\pm1,\pm1,\pm1)\}.$$

The set R is a $(6,2)$-arc of $\mathrm{PG}(2,q)$. The set S is a $(10,2)$-arc of $\mathrm{PG}(2,q)$ if and only if $q \neq 0$ mod 5.

The alternating group A_5 of order 60 generated by

$$\begin{aligned}
\psi_1 : (x\ y\ z) &\mapsto (x\ -y\ z),\\
\psi_2 : (x\ y\ z) &\mapsto (y\ z\ x),\\
\psi_3 : (x\ y\ z) &\mapsto \frac{1}{2}(x\ y\ z)\begin{pmatrix} \tau^{-1} & -\tau & 1\\ 1 & \tau & \tau^{-1}\\ -1 & \tau^{-1} & \tau \end{pmatrix},
\end{aligned}$$

acts as a group of automorphisms for both sets.

Proof : Note that $\sqrt{5}$ only exists when $q = 0, 1$ or 4 mod 5. Also note that $\tau^{-1} = \tau - 1$, $\tau^2 = \tau + 1$ and $\tau^3 = 2\tau + 1$.

Note that $|R| = 6$ if and only if $\tau \neq 0$ and $|S| = 10$ if and only if $\tau \neq 0$ and $1 \neq -1$. (If $\tau = 0$ then $\sqrt{5} = -1$ and then $5 = 1$, so q is even.) Hence, if q is odd then $|S| = 6$ and $|S| = 10$.

To prove that the set R is a $(k,2)$-arc we shall show that no triple of different points of the set is collinear. Because A_5 is a transitive group of automorphisms of the set R, we may choose an arbitrary element of R as the first point of each triple in the set, say $R_0(0,1,\tau)$.

The automorphism ψ_3 splits R into the singleton orbit $\{R_0\}$ and the set $\{R_1, \ldots R_5\}$ with:

$$\begin{aligned}
R_1 &= (0,1,-\tau), & & \\
R_2 &= (\tau,0,1), & R_3 &= (-\tau,0,1),\\
R_4 &= (1,\tau,0), & R_5 &= (-1,\tau,0).
\end{aligned}$$

Taking R_1 as a representative of this second orbit, it is now easily seen that the line R_0R_1 with equation $x = 0$ intersects R in at most two points if and only if $\tau \neq 0$, which implies q is even. Hence, for the set R to be a $(6,2)$-arc, q must be odd.

Similarly, to prove that the set S is a $(k,2)$-arc we shall show that no collinear triple of different points of the set exists. Again, we may choose an arbitrary

element of S as the first point of each triple in the set, say $S_0(1,1,1)$.

ψ_2 leaves the point S_0 invariant and splits $S \setminus S_0$ into three orbits $\{S_1, S_2, S_3\}$, $\{S_4, S_5, S_6\}$ and $\{S_7, S_8, S_9\}$:

$$\begin{array}{lllllllll} S_1 & = & (-1,1,1), & S_2 & = & (1,-1,1), & S_3 & = & (1,1,-1), \\ S_4 & = & (0,\tau,\tau^{-1}), & S_5 & = & (\tau,\tau^{-1},0), & S_6 & = & (\tau^{-1},0,\tau), \\ S_7 & = & (0,\tau,-\tau^{-1}), & S_8 & = & (\tau,-\tau^{-1},0), & S_9 & = & (-\tau^{-1},0,\tau). \end{array}$$

Hence, taking S_1, S_4 and S_7 as representatives of these two orbits, it suffices to show that the lines through these points and S_0 intersects S in at most two points:

1. the line S_0S_1, with equation $f_1(x,y,z) = y - z = 0$,
2. the line S_0S_4, with equation $f_2(x,y,z) = -\tau x - y + (1+\tau)z = 0$,
3. the line S_0S_7, with equation $f_3(x,y,z) = -(2+\tau)x + y + (1+\tau)z = 0$.

	$f_1(r)$	$f_2(r)$	$f_3(r)$
			$-(2+\tau)x+y$
	$y-z$	$-\tau x - y + (1+\tau)z$	$+(1+\tau)z$
$(1,1,1)$	0	0	0
$(-1,1,1)$	0	2τ	$2(\tau+2)$
$(1,-1,1)$	-2	2	-2
$(1,1,-1)$	2	$-2(\tau+1)$	$-2(\tau+1)$
$(0,\tau,\tau^{-1})$	1	0	2τ
$(\tau,\tau^{-1},0)$	$\tau-1$	-2τ	$-2(\tau+1)$
$(\tau^{-1},0,\tau)$	$-\tau$	2τ	2
$(0,\tau,-\tau^{-1})$	$2\tau-1$	-2τ	0
$(\tau,-\tau^{-1},0)$	$1-\tau$	-2	-4τ
$(-\tau^{-1},0,\tau)$	$-\tau$	$2(1+\tau)$	4τ

Table 6.4: Lists the values of $f_i(r)$ for each of the points in the left column (cf. proof of Theorem 6.5).

In Table 6.4 we list the values of $f_i(r)$ for each of the 10 points r of S. For S to be a $(k,2)$-arc, none of these colums may contain more than 2 zeroes. We find that q must be even together with the following 4 conditions:

$$\begin{aligned} \tau \neq 0 &\mapsto \sqrt{5} \neq -1 \\ \tau \neq 1/2 &\mapsto \sqrt{5} \neq 0 \\ \tau \neq 1 &\mapsto \sqrt{5} \neq 1 \\ \tau \neq -1 &\mapsto \sqrt{5} \neq -3 \\ \tau \neq -2 &\mapsto \sqrt{5} \neq 3 \end{aligned}$$

It holds that $\sqrt{5} = \pm 1$ if and only if $5 = 1$ and then q even. Also $\sqrt{5} = \pm 3$ if and only if $5 = 9$ and then q even. $\sqrt{5} = 0$ if and only if $5 = 0$ or $q = 0 \bmod 5$. Hence, for the set S to be a $(10,2)$-arc, q must be odd and $q \neq 0 \bmod 5$. ∎

Note that substituting $\sqrt{5}$ for $-\sqrt{5}$, replaces τ with $-\tau^{-1} = 1 - \tau$ and results in isomorphic sets R and S.

Also note that the set $R \cup -R$ considered as a subset of $\mathbb{R}^3$ is the set of vertices of an icosahedron. The set and $S \cup -S$ is the set of vertices of a dodecahedron.

In the following table, we indicate for all $q \leq 29$, $q = 0, 1, 4 \bmod 5$ whether the set is a (complete) 2-arc or not.

q	R	S
5	complete	not a 2-arc
9	complete	complete
11	not complete	complete
19	not complete	complete
25	not complete	not a 2-arc
29	not complete	not complete

For $q = 5$ the set R is the conic, while for $q = 9$ the set S is the conic. In both cases the conic has equation $x^2 + y^2 + z^2 = 0$.

For $q = 9$ the group of automorphisms in $\mathrm{P\Gamma L}(3,q)$ is the symmetric group S_5 on 5 elements.

6.4 Special $(k,2)$-arcs for $q = 8$

In what follows let α denote a primitive generating element of $\mathbb{F}_8$ which satisfies $\alpha^3 + \alpha^2 + 1 = 0$. The Frobenius automorphism σ of the field corresponds to $k \mapsto k^2$.

General constructions

The unique (complete) arc of size 10 is a hyperoval. It is a conic together with its nucleus. Its automorphism group G_S is isomorphic to $\mathrm{PGL}(2,8)$, Γ_S is isomorphic to $\mathrm{P\Gamma L}(2,8)$.

The complete arc of size 6 with $G_S \approx \Gamma_S \approx S_4$

$\mathrm{PG}(2,8)$ contains a complete arc of size 6 having S_4 as automorphism group. A representative of the arc is the set of points with the following coordinates:

$$S : (1,0,0), (0,1,0), (1,0,1), (0,1,1), (1,1,\alpha^4), (1,1,\alpha^6).$$

Consider the following three elements of order 2 of the automorphism group of the arc S:

$$\begin{aligned} \phi_1 : (x\ y\ z) &\mapsto (y\ x\ z), \\ \phi_2 : (x\ y\ z) &\mapsto (x+y\ y\ \alpha^4 y + z), \\ \phi_3 : (x\ y\ z) &\mapsto (y\ x\ x+y+z), \end{aligned}$$

and consider the four lines with the following coordinates:

$$[1,1,\alpha^3], [1,1,\alpha], [1,\alpha^5,\alpha], [1,\alpha^2,\alpha^3]$$

The action of ϕ_1, ϕ_2 and ϕ_3 on these lines generates the symmetric group on four elements.

By applying the Frobenius automorphism $\phi : k \mapsto k^2$ to S and G_S, one finds the other two complete arcs S^ϕ and S^{ϕ^2} and their automorphism groups. Note that these groups are conjugate but not equal.

6.5 Special $(k,2)$-arcs for $q = 9$

In what follows let α denote a primitive generating element of $\mathbb{F}_9$ which satisfies $\alpha^2 + \alpha - 1 = 0$. The Frobenius automorphism σ of the field corresponds to $k \mapsto k^3$.

General constructions

The unique (complete) arc of size 10 is a conic with automorphism group G_S isomorphic to $\mathrm{PGL}(2,9)$, Γ_S isomorphic to $\mathrm{P\Gamma L}(2,9)$. This arc also corresponds to the complete arc S that is described in Section 6.3 and to the arc $S^*(1) \cup I$ as described in Section 6.2.

The unique complete arc of size 6 is the complete arc R discussed in Section 6.3.

For every field of square order a complete arc of size $q - \sqrt{q} + 1$ exists (Section 6.1). For $q = 9$ it has size 7 with $\Gamma_S \approx 7\colon 6$ and $G_S \approx 7\colon 3$.

The unique complete arc of size 8 with $G_S \approx D_8$ and $\Gamma_S \approx D_{16}$

This is an arc of type E with two external points as described in Section 3.4. A representative of this arc consists of the points with coordinates $(1, t, t^2)$ with $t = \alpha^2, \alpha^4, \alpha^5, \alpha^7$, together with the two external points with coordinates

$(0,1,0)$ and $(1,1,\alpha)$ and the tangent points of $(0,1,0)$ with coordinates $(1,0,0)$ and $(0,0,1)$. The automorphism group G_S is isomorphic to the dihedreal group of order 8, Γ_S is isomorphic to that of order 16. Note that this arc has size $q-1$ which is exceptionally.

6.6 Special (k,2)-arcs for $q = 11$

General constructions

The unique (complete) arc of size 12 is a conic with automorphism group isomorphic to $\mathrm{PGL}(2,11)$. This arc also is of type $S^*(a)$ as described in Section 6.2.

The unique complete arc of size 10 corresponds to the complete arc S as described in Section 6.3. Note that this arc has size $q-1$, which is exceptional.

There is a unique complete arc of size 7 with $G_S \approx 7:3$ which can be constructed as an orbit of the 19th power of a Singer cycle (see Section 6.1).

6.7 Special (k,2)-arcs for $q = 13$

General constructions

The unique (complete) arc of size 14 is a conic with automorphism group isomorphic to $\mathrm{PGL}(2,13)$.

In $\mathrm{PG}(2,13)$ there is an arc of size 8 with automorphism group isomorphic to the dihedral group D_{14}. It is an arc of type I with excess 1 as described in Section 3.7.

When applying Theorem 6.2 to $q = 13$, we find that $S^*(a)$ is an arc only for

the values $a = \pm 3, \pm 4$. These arcs are equivalent and have $S_4 \colon 3$ as group of automorphisms. Note that an arc of size $q-1$ is exceptional.

PG$(2,13)$ has a unique complete arc of size 10 having S_4 as group of automorphisms. It is the arc $S^*(1) \cup I$ described in Theoreom 6.4 with $i = 5$.

The two complete arcs of size 9 with $G_S \approx 3^2$

PG$(2,13)$ contains 2 complete arcs of size 9 with the same automorphism group 3^2. This group can be represented by

$$\phi_1 : (x,y,z) \mapsto (x,3y,9z)$$

and

$$\phi_2 : (x,y,z) \mapsto (y,4z,x).$$

The first arc S_1 consists of the points of the orbit of the point with coordinates $(1,1,-1)$, while the second arc S_2 consists of the points of the orbit of the point with coordinates $(1,2,1)$. Each arc lies on a cubic with respective equations C_1 and C_2:

$$C_1 \leftrightarrow x^3 - 3y^3 + 4z^3 - 6xyz = 0$$
$$C_2 \leftrightarrow x^3 - 3y^3 + 4z^3 + 3xyz = 0.$$

Note that each cubic of the form $x^3 - 3y^3 + 4z^3 - cxyz = 0$ is invariant for ϕ_1 and ϕ_2.

The points of the first cubic C_1 are:

(-4,4,1)	(-4,1,1)	(-3,4,1)	(1,-6,1)	(-6,-2,1)	(-5,-3,1)
(3,3,1)	(-1,-1,1)	(3,-1,1)	(-2,-6,1)	(-6,4,1)	(-4,-5,1)
(4,-3,1)	(1,-3,1)	(1,-4,1)	(-2,-1,1)	(3,-2,1)	(-5,-5,1),

(6.3)

in which the left hand side contains the 9 points of S_1.

The abelian group of C_1 is of type 2×3^2 and can be represented as follows. Take $O(1,1,-1)$ to be the point of reference. Then the element $(3,-1,1)$ has order 3 and permutes the columns in each part of (6.3). The element $(1,-3,1)$

also has order 3 and permutes the rows in each part of (6.3). Finally, the element $(-6,4,1)$ has order 2 and maps the points on the left hand side of (6.3) to the points at the corresponding positions on the right hand side.

The points of the second cubic C_2 are:

(1,2,1)	(2,2,1)	(2,4,1)	(-6,-4,1)	(-1,6,1)	(5,-5,1)
(5,6,1)	(5,-1,1)	(-4,6,1)	(4,5,1)	(6,-2,1)	(-2,1,1)
(6,-3,1)	(3,5,1)	(6,5,1)	(2,-6,1)	(-5,3,1)	(-3,2,1)

(6.4)

in which the left hand side contains the 9 points of S_2.

The abelian group of C_2 looks very similar to that of C_1. It also is 2×3^2. We now take $O(1,2,1)$ to be the point of reference. The elements $(2,2,1)$ and $(5,6,1)$ have order 3. The first element permutes the columns in each part of (6.4), the second permutes the rows in each part of (6.4). Finally, the element $(-6,-4,1)$ has order 2 and maps the points on the left hand side of (6.4) to the points at the corresponding positions on the right hand side.

See Section 6.1 for more information on half cubics.

6.8 Special $(k,2)$-arcs for $q = 16$

In what follows let α denote a primitive generating element of $\mathbb{F}_{16}$ which satisfies $\alpha^4 + \alpha^3 + 1 = 0$. The Frobenius automorphism σ of the field corresponds to $k \mapsto k^2$.

General constructions

PG$(2,16)$ has two complete arcs of size 18. One arc is a conic toghether with its nucleus, also called a *regular hyperoval*. It has PGL$(2,16)$ as automorphism group G_S and PΓL$(2,16)$ as Γ_S.

The other arc of size 18 is an *irregular hyperoval* called the *Lunelli-Sce hyperoval* [28]. It consists of the four points with coordinates $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,1)$ and the 16 points with coordinates $(x, f(x), 1)$ with

$$f(x) = x^{12} + x^{10} + \alpha^2 x^8 + x^6 + \alpha^{14} x^4 + \alpha^3 x^2.$$

The automorphism group G_S of this arc has order 36, Γ_S has order 144. For more details, we refer to Bill Cherowitzo's hyperoval webpage [8].

As mentioned in Section 6.1, a complete arc of size $q - \sqrt{q} + 1$ exists for every field of square order. For $q = 16$ it has size 13 with $\Gamma_S \approx 13\colon 12$ and $G_S \approx 13\colon 3$.

6.9 Special (k,2)-arcs for $q = 17$

General constructions

The unique (complete) arc of size 18 is a conic with automorphism group isomorphic to $\mathrm{PGL}(2,17)$. This arc also corresponds to the arc $S^*(a) \cup I$ as described in Section 6.2.

In $\mathrm{PG}(2,17)$ there is a unique complete arc of size 10 with the dihedral group D_{18} as automorphism group. It is an arc of type I with excess 1 as described in Section 3.7.

When applying Theorem 6.2 to $q = 17$, we find that the set $S^*(a)$ is an arc for all values $a = \pm 3, \pm 5, \pm 6, \pm 7, \pm 8$. This arc is only complete for $a = \pm 3, \pm 5, \pm 6$. These three arcs are not equivalent. Adding a set I to $S^*(\pm 7)$ as in Theorem 6.3 yields the complete arc of size 18 that is the conic.

Applying Theorem 6.4 to $\mathrm{PG}(2,17)$ with $i = 4$ yields a unique complete arc of type $S^*(1) \cup I$ of size 10 having S_4 as group of automorphisms.

The unique complete arc of size 10 with $G_S \approx Q_8$ and the unique complete arc of size 10 with $G_S \approx 8\colon 2$

There is a unique complete arc of size 10 in $\mathrm{PG}(2,17)$ that has the quaternion group of order 8 as automorphism group. We list coordinates for the points of one respresentative below.

$$\begin{array}{cc} (5,8,\pm 1) & (3,2,\pm 1) \\ (8,-5,\pm 1) & (2,-3,\pm 1) \\ (1,0,0) & (0,1,0) \end{array}$$

The group is generated by the following linear transformations:

$$\begin{aligned} \pm 1 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \\ \pm i : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \\ \pm j : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \\ \pm k : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 0 & 4 & 0 \\ 4 & 0 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \end{aligned}$$

such that $i^2 = j^2 = k^2 = ijk = -1$.

If we replace the points $(1,0,0)$ and $(0,1,0)$ by $(1,4,0)$ and $(1,-4,0)$, then we obtain another complete 10-arc having the quasidihedral group of order 16 ($\approx 8\colon 2$) as automorphism group. This group consists of the elements of Q_8

together with the following eight elements:

$$\begin{aligned}
\pm l : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 5 & 5 & 0 \\ -5 & 5 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \\
\pm m : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 5 & -5 & 0 \\ 5 & 5 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \\
\pm n : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 3 & 3 & 0 \\ 3 & -3 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \\
\pm o : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} -3 & 3 & 0 \\ 3 & 3 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix},
\end{aligned}$$

such that $l^4 = m^4 = -1$ and $n^2 = o^2 = 1$. Note that $m^o = m^3$.

The two complete arcs of size 12 with $G_S \approx D_{12}$

The projective plane PG$(2,17)$ has two inequivalent complete arcs of size 12 with the dihedral group of order 12 as group of automorphisms. Both arcs can be partitioned into two sets of size 6 and each of these sets is contained in a conic. If we take one of the conics of each arc to be the conic C with equation $x^2 - 3y^2 = z^2$, then we find the following representatives for the arcs: both arcs contain the six points with the following coordinates:

$$(1,0,1), (-8,-2,1), (8,-2,1), (-1,0,1), (8,2,1), (-8,2,1).$$

The remaining points of the first arc S_1 lie on the conic C_1 with equation $x^2 - 3y^2 = -7z^2$. These 6 arc points are

$$(0,5,1), (4,-6,1), (4,6,1), (0,-5,1), (-4,6,1), (-4,-6,1).$$

The remaining points of the second arc S_2 lie on the conic C_2 with equation $x^2 - 3y^2 = -6z^2$. These 6 arc points are

$$(0,6,1), (-2,3,1), (-2,-3,1), (0,-6,1), (2,-3,1), (2,3,1).$$

The automorphism group of both arcs is the same, and can be generated by

$$\begin{aligned} \phi_1 : (x\ y\ z) &\mapsto (x\ -y\ z), \\ \phi_2 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} -8 & -2 & 0 \\ -6 & -8 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

The transformation ϕ_1 has order 2. ϕ_2 has order 6 and permutes the 6 arc points of each conic in the above order. We also have $\phi_2^{\phi_1} = \phi_2^{-1}$.

6.10 Special (k,2)-arcs for $q = 19$

General constructions

The unique (complete) arc of size 20 is a conic with automorphism group isomorphic to $\mathrm{PGL}(2,19)$.

The arc of size 10 with A_5 as group of automorphisms corresponds to the arc S described in Section 6.3.

The unique complete arc of size 12 with the dihedral group D_{18} as automorphism group is an arc of type E with excess 1 as described in Section 3.7.

When applying Theorem 6.2 to $q = 19$, we find that $S^*(a)$ is an arc except for the values $a = 0, \pm 1, \pm 2, \pm 4$. For $a = \pm 6$, the arc is not complete. For $a = \pm 3, \pm 5, \pm 9$, the arcs have S_4 as group of automorphisms. For $a = \pm 7, \pm 8$ the automorphism group is larger: it is $S_4 : 3$. Note that the arcs $S^*(7)$ and $S^*(8)$ are equivalent.

Finally, there are two complete arcs of size 14 in $\mathrm{PG}(2,19)$ that can be embedded onto a non-singular irreducible cubic curve with one rational inflexion

point. In Section 6.1 we showed that a subgroup of index two of the abelian group of the curve is an arc.

The first arc lies on the curve with equation $C_1 \leftrightarrow z^2y + x^3 - 8y^3 = 0$. This curve is of type (i), as classified in [19, Theorem 11.54]. It is a non-singular equianharmonic cubic curve. The inflexion point has coordinates $(0,0,1)$. The abelian group of the 28 rational non-singular points of the cubic is isomorphic to 7×2^2. This group has three subgroups of order 14. A coset of each of these subgroups yields a $(k,2)$-arc. These three arcs are equivalent. The abelian group can be generated by the element of order 14 with coordinates $(7,7,1)$ and the element of order 2 with coordinates $(3,1,0)$. The arc points are the 14 points in the orbit of the first generator.

The second arc lies on the curve with equation $C_2 \leftrightarrow z^2y + x^3 + 6xy^2 + 3y^3 = 0$. This curve is also of type (i), as classified in [19, Theorem 11.54]. It is a non-singular general cubic curve. The inflexion point has coordinates $(0,0,1)$. The abelian group of the 28 rational non-singular points of the cubic is isomorphic to the cyclic group of order 28 and can be generated by the element with coordinates $(0,5,1)$. The arc points are the 14 odd multiples of this generator, in other words they correspond to a coset of a subgroup of index two.

The automorphism group G_S of both arcs is a cyclic group of order 2 containing the following automorphism: $(x,y,z) \to (x,y,-z)$.

6.11 Special (k,2)-arcs for $q = 23$

General constructions

The unique (complete) arc of size 24 is a conic with automorphism group isomorphic to $\mathrm{PGL}(2,23)$.

There is a unique complete arc of size 14 with automorphism group isomorphic to the dihedral group D_{22}. It is an arc of type E with excess 1 as described in Section 3.7.

PG$(2, 23)$ has two inequivalent complete arcs of size 12 with automorphism group isomorphic to the symmetric group on 4 elements. These are the arcs $S^*(a)$ as described in Theorem 6.2 with $a = \pm 7, \pm 8$. The set $S^*(a)$ also is an arc for $a = \pm 3, \pm 4, \pm 5, \pm 6, \pm 11$, but in these cases the arc is not complete.

The unique complete arc S with $G_S \approx 16 : 2$

PG$(2, 23)$ contains a unique complete arc of size 16 with an automorphism group of size 32. The arc can be partitioned into two sets of size 8 each of which is contained in a conic.

We may choose coordinates in such a way that the first set S_1 consists of the points with coordinates of the form $(1, 0, \pm 1)$, $(1, \pm 1, 0)$ and $(1, \pm 9, \pm 9)$. These points lie on the conic C_1 with equation $y^2 + z^2 = x^2$. The second set S_2 contains all points with coordinates of the form $(1, \pm 2, \pm 8)$ and $(1, \pm 8, \pm 2)$. These points lie on the conic C_2 with equation $y^2 + z^2 = -x^2$.

The collineations

$$\phi_1 : (x, y, z) \mapsto (x, 9(y - z), 9(y + z)),$$
$$\phi_2 : (x, y, z) \mapsto (x, -y, z)$$

leave S_1, S_2, C_1 and C_2 invariant. ϕ_1 has order 8, ϕ_2 is an involution and together they generate a dihedral group of order 16 with orbits S_1 and S_2.

To obtain the full automorphism group of the arc, we need to add the collineation

$$\phi_3 : (x, y, z) \mapsto (x, -2y + 8z, -8y - 2z)$$

of order 16, which interchanges S_1 and S_2 (and C_1 and C_2). Note that $\phi_3^2 = \phi_1$.

The full group has the following presentation: $\langle \phi_2, \phi_3 \mid \phi_3^{16} = \phi_2^2 = 1, \phi_3^{\phi_2} = \phi_3^7 \rangle$.

6.12 Special (k,2)-arcs for $q = 25$

In what follows let α denote a primitive generating element of $\mathbb{F}_{25}$ which satisfies $\alpha^2 + \alpha + 2 = 0$. The Frobenius automorphism σ of the field corresponds to $k \mapsto k^5$.

General constructions

The unique (complete) arc of size 26 is a conic with automorphism group $G_S \approx \mathrm{PGL}(2,25)$ and $\Gamma_S \approx \mathrm{P\Gamma L}(2,25)$.

Secondly, $\mathrm{PG}(2,25)$ has a unique complete arc S of size 14 with G_S isomorphic to the dihedral group of order 26, and Γ_S isomorphic to the semidirect product $13:4$. This arc is of type I with excess 1 as described in Section 3.7.

As mentioned in Section 6.1, a complete arc of size $q - \sqrt{q} + 1$ exists for every field of square order. For $q = 25$ it has size 21 with $\Gamma_S \approx 21:6$ and $G_S \approx 21:3$. This arc was already discovered by Chao and Kaneta [7].

In $\mathrm{PG}(2,25)$, the set $S^*(a)$ described in Theorem 6.2 is an arc for the following values of a: $\pm\alpha^2, \pm\alpha^4, \pm\alpha^7, \pm\alpha^8, \pm\alpha^9, \pm\alpha^{10}, \pm\alpha^{11}$. This arc however never is complete. The arcs $S^*(\pm\alpha^4)$ and $S^*(\pm\alpha^8)$ both can be extendend with the set I as described in Theorem 6.3 with $i = \pm\alpha^6$. They turn out to be equivalent in $\mathrm{P\Gamma L}(3,q)$ and have S_4 as group of automorphisms.

The unique complete arc S with $|G_S| = 72$ and $|\Gamma_S| = 144$

There is one more unique complete arc in $\mathrm{PG}(2,25)$ with a large automorphism group. We do not know whether this type of arc can be generalized to other fields. We list coordinates for the points of one representative S below.

We have $|S| = 18$, $|G_S| = 72$ and $|\Gamma_S| = 144$.

$$\begin{array}{ccc|ccc} (1,\alpha^2,\alpha^3) & (\alpha^4,1,\alpha) & (0,\alpha^{13},1) & (0,1,\alpha^{17}) & (\alpha^{17},0,1) & (1,\alpha^{17},0) \\ (\alpha^3,1,\alpha^2) & (\alpha,\alpha^4,1) & (1,0,\alpha^{13}) & (1,\alpha^{20},\alpha^5) & (\alpha^5,1,\alpha^{20}) & (\alpha^{20},\alpha^5,1) \\ (\alpha^2,\alpha^3,1) & (1,\alpha,\alpha^4) & (\alpha^{13},1,0) & (\alpha^{15},\alpha^{10},1) & (1,\alpha^{15},\alpha^{10}) & (\alpha^{10},1,\alpha^{15}) \end{array} \tag{6.5}$$

The group G_S is generated by the following linear transformations:

$$\begin{aligned} \phi_1 : (x\ y\ z) &\mapsto (z\ x\ y), \\ \phi_2 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} \alpha^8 & 0 & \alpha^8 \\ 1 & 1 & 0 \\ 0 & \alpha^{16} & \alpha^{16} \end{pmatrix}, \\ \phi_3 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} \alpha & 1 & \alpha^3 \\ \alpha^{20} & 1 & \alpha^{23} \\ \alpha^9 & \alpha^{22} & 1 \end{pmatrix}, \\ \phi_4 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} \alpha^{17} & \alpha^{15} & \alpha^3 \\ \alpha^8 & \alpha^{19} & \alpha^{22} \\ \alpha^9 & \alpha & 1 \end{pmatrix}. \end{aligned}$$

The transformation ϕ_1 permutes the coordinates cyclicly. This corresponds to a permutation of the rows in the left hand part of (6.5) and a permutation of the columns in the right hand part, leaving the columns on the left and the rows on the right invariant. The transformation ϕ_2 has exactly the opposite effect: it permutes the columns on the left and the rows on the right, and leaves invariant the rows on the left and the columns on the right. We have $\phi_1^3 = \phi_2^3 = 1$ and $\phi_1\phi_2 = \phi_2\phi_1$.

The element ϕ_3 maps the points on the left hand side of (6.5) to the points at the corresponding positions on the right hand side. ϕ_3 has order 4. The element ϕ_4 has order 4, but leaves the two sides of (6.5) invariant, instead of interchanging them. It fixes the points of S with coordinates $(0,\alpha^{13},1)$ and $(1,\alpha^{17},0)$. Moreover, we have $\phi_4^2 = \phi_3^2$.

Finally note that $\phi' : (x,y,z) \mapsto (x^5,z^5,y^5)$, which belongs to $\mathrm{P\Gamma L}(3,25)$ but not to $\mathrm{PGL}(3,25)$, is also an automorphism of S which again interchanges the left hand side and the right hand side of (6.5).

6.13 Special (k,2)-arcs for $q = 27$

In what follows let α denote a primitive generating element of $\mathbb{F}_{27}$ which satisfies $\alpha^3 - \alpha^2 + 1 = 0$. The Frobenius automorphism σ of the field corresponds to $k \mapsto k^3$.

General constructions

First, the unique (complete) arc of size 28 is a conic with $G_S \approx \mathrm{PGL}(2,27)$ and $\Gamma_S \approx \mathrm{P\Gamma L}(2,27)$.

Secondly, the unique complete arc of size 16 with $G_S \approx D_{26}$ is an arc of type E with excess 1 as described in Section 3.7. The full automorphism group Γ_S of the arc is isomorphic to the semidirect product $13 : 6$.

There is a unique complete arc of size 19 in $\mathrm{PG}(2,27)$ that can be embedded onto a non-singular irreducible cubic curve with one rational inflexion point. This curve has equation $z^2y + x^3 - \alpha^5x^2y + \alpha^2y^3 = 0$, and is of type (ii)a, as classified in [19, Theorem 11.54]. The inflexion point has coordinates $(0,0,1)$. The abelian group of the 38 rational non-singular points of the cubic is isomorphic to the cyclic group of order 38 and can be generated by the element with coordinates $(1,\alpha^3,1)$. The arc points are the 19 odd multiples of this generator, in other words they correspond to a coset of a subgroup of index two. In Section 6.1 we proved that this construction yields an arc. The automorphism group G_S of this arc is a cyclic group of order 2, while Γ_S is a cyclic group of order 6.

If we apply Theorem 6.2 to $q = 27$, there are 24 values of a (see Table 6.1) which lead to an arc $S^*(a)$ of size 12 with an automorphism group isomorphic to the symmetric group on 4 elements. Only in the cases $a = \pm\alpha^7, \pm\alpha^8, \pm\alpha^{11}$ this arc turns out to be complete. (And these six cases yield PΓL-equivalent arcs.) This example is of special significance because 12 is the smallest size for a complete arc in $\mathrm{PG}(2,27)$.

The two complete arcs of size 14 with $G_S = \Gamma_S \approx D_{14}$

The projective plane PG(2, 27) has two inequivalent complete arcs of size 14 with the dihedral group of order 14 as group of automorphisms. Both arcs can be partitioned into two sets of size 7 and each of these sets is contained in a conic. If we take one of the conics of each arc to be the conic C with equation $xz = y^2$, then we find the following representatives for the arcs: both arcs contain the points with coordinates $(1, t, t^2)$ with t one of the elements in the following list:

$$\alpha, \alpha^2, -\alpha^5, \infty, \alpha^5, -\alpha^2, -\alpha,$$

where $t = \infty$ corresponds to the point $(0, 0, 1)$.

The remaining points of the first arc S_1 lie on the conic C_1 with equation $x^2 - \alpha^{11}y^2 - \alpha^{11}z^2 + \alpha^9 xz = 0$. These 7 arc points are

$$(1, -\alpha^{10}, \alpha^6), (1, \alpha^7, \alpha^3), (1, \alpha^3, 1), (1, 0, \alpha^{12}), (1, -\alpha^3, 1), (1, -\alpha^7, \alpha^3), (1, \alpha^{10}, \alpha^6).$$

The remaining points of the second arc S_2 lie on the conic C_2 with equation $x^2 - \alpha^8 y^2 - \alpha^{11}z^2 + \alpha^5 xz = 0$. These 7 arc points are

$$(1, \alpha^9, 0), (1, \alpha^3, \alpha^8), (1, -\alpha^4, \alpha^{25}), (1, 0, -1), (1, \alpha^4, \alpha^{25}), (1, -\alpha^3, \alpha^8), (1, -\alpha^9, 0).$$

The automorphism group of both arcs is the same, and can be generated by

$$\begin{aligned} \phi_1 : (x\ y\ z) &\mapsto (x\ -y\ z), \\ \phi_2 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 1 & -\alpha^9 & -\alpha^5 \\ \alpha^8 & -\alpha^{10} & \alpha^9 \\ -\alpha^3 & -\alpha^8 & 1 \end{pmatrix}. \end{aligned}$$

The transformation ϕ_1 fixes the points $(0, 0, 1)$, $(1, 0, \alpha^{12})$ and $(1, 0, -1)$, and reverses the order of the points of S_1 and S_2 as listed above. ϕ_2 has order 7 and permutes the 7 arc points of each conic.

The unique complete arc of size 22 with $G_S \approx D_{14}$ and $\Gamma_S \approx 7\colon 6$

PG(2, 27) has a unique complete arc of size 22 with D_{14} as automorphism group G_S and $7\colon 6$ as Γ_S. This arc was described by Chao and Kaneta [7]. It

consists of 14 points of a conic, 7 external points to this conic and 1 internal point. This last point is a fixed point of the automorphism group.

The unique complete arc of size 16 with $G_S \approx Q_8$ and $\Gamma_S \approx \mathrm{SL}(2,3)$

$\mathrm{PG}(2,27)$ also has a unique complete arc of size 16 with G_S isomorphic to the quaternion group of order 8. We list coordinates for the points of one representative of the arc below.

$$\begin{array}{r|r} (0,1,\pm 1) & (\alpha^2,\alpha,\pm 1) \\ (1,0,\pm 1) & (\alpha,-\alpha^2,\pm 1) \\ (\alpha^9,\alpha^{12},\pm 1) & (\alpha^5,\alpha^7,\pm 1) \\ (\alpha^{12},-\alpha^9,\pm 1) & (\alpha^7,-\alpha^5,\pm 1) \end{array}$$

All points of this arc lie on the quartic with equation $x^4+y^4-z^4-\alpha^7x^3y+\alpha^7xy^3=0$. The group G_S is generated by the following eight linear transformations:

$$\begin{aligned}
\pm 1 : (x\ y\ z) &\mapsto (x\ y\ z)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \\
\pm i : (x\ y\ z) &\mapsto (x\ y\ z)\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \\
\pm j : (x\ y\ z) &\mapsto (x\ y\ z)\begin{pmatrix} \alpha^9 & \alpha^{12} & 0 \\ \alpha^{12} & -\alpha^9 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \\
\pm k : (x\ y\ z) &\mapsto (x\ y\ z)\begin{pmatrix} -\alpha^{12} & \alpha^9 & 0 \\ \alpha^9 & \alpha^{12} & 0 \\ 0 & 0 & \pm 1 \end{pmatrix},
\end{aligned}$$

such that $i^2=j^2=k^2=ijk=-1$. To obtain Γ_S we need to add the automorphism $\phi' : (x,y,z) \mapsto (\alpha^{12}x^3, y^3-\alpha^9x^3, z^3)$ which belongs to $\mathrm{P\Gamma L}(3,27) \setminus \mathrm{PGL}(3,27)$. The group Γ_S is isomorphic to $\mathrm{SL}(2,3)$.

A complete arc of size 18 with $G_S = \Gamma_S \approx S_3$

There are 25 inequivalent complete arcs of size 18 with $G_S = \Gamma_S \approx S_3$, but only one of them consists of 15 (=$(q+3)/2$) points of a conic together with 3 points external to this conic (cf. Chapter 3). This arc was already described by Davydov et al. [14].

The unique complete arc of size 18 with $G_S = \Gamma_S \approx 3^2 : 2$

There is a unique complete arc of size 18 with an automorphism group of size 18. The arc can be partitioned into two sets of size 9 each of which is contained in a conic. We list coordinates of one representative of the arc below.

$$\begin{array}{ccc|ccc} (1,0,0) & (0,1,0) & (0,0,1) & (\alpha^{14},1,1) & (1,\alpha^{14},1) & (1,1,\alpha^{14}) \\ (\alpha^9,\alpha^{16},1) & (1,\alpha^9,\alpha^{16}) & (\alpha^{16},1,\alpha^9) & (\alpha^{11},1,\alpha^8) & (\alpha^8,\alpha^{11},1) & (1,\alpha^8,\alpha^{11}) \\ (\alpha^9,1,\alpha^{16}) & (\alpha^{16},\alpha^9,1) & (1,\alpha^{16},\alpha^9) & (\alpha^{11},\alpha^8,1) & (1,\alpha^{11},\alpha^8) & (\alpha^8,1,\alpha^{11}) \end{array} \tag{6.6}$$

The nine points in the left hand part of (6.6) lie on the conic with equation $xy + xz + yz = 0$, those in the right hand part on the conic with equation $\alpha^2x^2 + \alpha^2y^2 + \alpha^2z^2 + xy + xz + yz = 0$.

The group $G_S = \Gamma_S$ is generated by the projective transformations ϕ_1, ϕ_2, ϕ_3, represented as follows:

$$\begin{aligned} \phi_1 : (x\ y\ z) &\mapsto (z\ x\ y), \\ \phi_2 : (x\ y\ z) &\mapsto (x\ z\ y), \\ \phi_3 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} \alpha^9 & \alpha^{16} & 1 \\ 1 & \alpha^9 & \alpha^{16} \\ \alpha^{16} & 1 & \alpha^9 \end{pmatrix}. \end{aligned}$$

We have $\phi_1^3 = \phi_2^2 = \phi_3^3 = 1$, $\phi_1\phi_3 = \phi_3\phi_1$, $\phi_1^{\phi_2} = \phi_1^{-1}$ and $\phi_3^{\phi_2} = \phi_3^{-1}$.

The transformation ϕ_1 permutes the coordinates cyclicly. This corresponds to a permutation of the columns in the left hand part and in the right hand

part of (6.6), leaving the rows invariant. The transformation ϕ_3 has exactly the opposite effect: it permutes the rows and leaves invariant the columns in (6.6).

6.14 Special (k,2)-arcs for $q = 29$

General constructions

The unique (complete) arc of size 30 is a conic with automorphism group $G_S \approx \mathrm{PGL}(2,29)$.

There is a unique complete arc of size 16 with automorphism group isomorphic to the dihedral group of order 30. It corresponds to an arc of type I with excess 1 as discussed in Section 3.7.

Applying Theorem 6.2 to the case $q = 29$ yields 18 values of a for which $S^*(a)$ is a 12-arc (see Table 6.1). None of these arcs are complete, but for eight of these the set I can be added, i.e. when $a = \pm 4, \pm 6, \pm 9, \pm 10$. This results in four inequivalent complete arcs of size 18 with automorphism group isomorphic to the symmetric group on 4 elements.

The smallest size for a complete arc in PG$(2,29)$ is 13. There is a unique complete arc of that size with an automorphism group of size 39. It can be constructed as the orbit of the 67th power of a Singer cycle as described in Section 6.1. The automorphism group of the arc is isomorphic to the semi-direct product $13 : 3$.

The 2 complete arcs of size 14 with $G_S \approx D_{14}$

Like PG$(2,27)$ also PG$(2,29)$ has two inequivalent complete arcs of size 14 with the dihedral group of order 14 as automorphism group. Again, both arcs can be partitioned into two sets of size 7 and each of these sets is contained in a conic. If we take one of the conics of each arc to be the conic C with

equation $y^2 = xz$, then we find the following representatives for the arcs: both arcs contain the points with coordinates $(1, t, t^2)$ with t one of the elements of the following list:

$$1,\ 7,\ 7^2 = -9,\ 7^3 = -5,\ 7^4 = -6,\ 7^5 = -13,\ 7^6 = -4$$

The remaining points of the first arc S_1 lie on the conic C_1 with equation $y^2 = -4xz$. These are the points $(1, t, 7t^2)$ for the same values of t. The remaining points of the second arc S_2 lie on the conic C_2 with equation $y^2 = -9xz$. These are the points $(1, t, -13t^2)$, again for the same values of t. The automorphism group of both arcs is the same, and can be generated by

$$\begin{aligned} \phi_1 : (x\ y\ z) &\mapsto (x\ 7y\ 7^2 z), \\ \phi_2 : (x\ y\ z) &\mapsto (z\ y\ x). \end{aligned}$$

We have $\phi_1^{\phi_2} = \phi_1^{-1}$.

ϕ_1 acts like $t \mapsto 7t$ on both arcs. ϕ_2 corresponds to $t \mapsto 1/t$ on the conic C, $t \mapsto -4/t$ on $S_1 \setminus C$ and $t \mapsto -9/t$ on $S_2 \setminus C$. It fixes the points $(1,1,1)$, $(1,-5,1)$ of S_1 and $(1,1,1)$, $(1,7,1)$ of S_2.

The unique complete arc of size 20 with $G_S \approx D_{20}$

There is a unique complete arc of size 20 with the dihedral group of order 20 as group of automorphisms. The arc can be partitioned into two sets of size 10 and each of these sets is contained in a conic.

We may choose coordinates in such way that the first conic C_1 has equation $x^2 + y^2 + 10z^2 = 0$. The arc points on this conic are the following:

$$\begin{array}{ccccc} (1,4,6) & (1,10,4) & (1,-3,12) & (1,6,11) & (1,-7,-13) \\ (1,-4,6) & (1,-10,4) & (1,3,12) & (1,-6,11) & (1,7,-13) \end{array} \tag{6.7}$$

The second conic C_2 then has equation $-11xz + 5y^2 - z^2 = 0$, the arc points

on C_2 are:

$$\begin{array}{ccccccc} & & (1,-7,-14) & (1,-9,-5) & (0,1,11) & (1,10,8) & \\ (1,0,0) & & & & & & (1,0,-11) \\ & & (1,7,-14) & (1,9,-5) & (0,-1,11) & (1,-10,8) & \end{array} \tag{6.8}$$

The automorphism group of the arc can be generated by

$$\begin{aligned} \phi_1 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} 4 & 1 & 2 \\ -1 & -1 & -7 \\ -9 & 12 & 7 \end{pmatrix}, \\ \phi_2 : (x\ y\ z) &\mapsto (x\ -y\ z). \end{aligned}$$

ϕ_1 has order 10 and permutes the 10 arc points of each conic in a clockwise order in (6.7) and (6.8). The involution ϕ_2 fixes the points $(1,0,0)$ and $(1,0,-11)$ of C_2 and none of the points of C_1. We have $\phi_1^{\phi_2} = \phi_1^{-1}$.

The two complete arcs of size 21 with $G_S \approx S_3$

The third largest size of a complete arc in $\mathrm{PG}(2,29)$ is 21. There are two arcs of this size. The first arc consists of the points

$$\begin{array}{cccc} (1,0,0) & (1,5,10) & (1,4,9) & (1,-3,-2) \\ (0,1,0) & (1,10,5) & (1,9,4) & (1,-2,-3) \\ (0,0,1) & (5,1,10) & (4,1,9) & (-3,1,-2) \\ & (10,1,5) & (9,1,4) & (-2,1,-3) \\ & (5,10,1) & (4,9,1) & (-3,-2,1) \\ & (10,5,1) & (9,4,1) & (-2,-3,1), \end{array} \tag{6.9}$$

the second arc consists of the points

$$\begin{array}{cccc} (1,0,0) & (1,2,8) & (1,5,13) & (1,-3,-5) \\ (0,1,0) & (1,8,2) & (1,13,5) & (1,-5,-3) \\ (0,0,1) & (2,1,8) & (5,1,13) & (-3,1,-5) \\ & (8,1,2) & (13,1,5) & (-5,1,-3) \\ & (2,8,1) & (5,13,1) & (-3,-5,1) \\ & (8,2,1) & (13,5,1) & (-5,-3,1). \end{array} \tag{6.10}$$

The automorphism group of these arcs is the symmetric group of degree three, which is clearly visible in (6.9) and (6.10) as a permutation group of the coordinates.

The unique complete arc of size 24

The unique complete arc of size 24 has an interesting structure which can be described in various ways. It consists of the points of the well-known Klein quartic [27] on $\mathbb{F}_{29}$. Its automorphism group is $\mathrm{PSL}(2,7) \approx \mathrm{PSL}(3,2)$, of order 168.

The Klein quartic can be represented by the simple equation

$$x^3y + y^3z + z^3x = 0.$$

The automorphism group of this curve is generated by the following elements:

$$\begin{aligned}
\phi_1 : (x,y,z) &\mapsto (z,x,y), \\
\phi_2 : (x,y,z) &\mapsto (7^4x, 7^2y, 7z), \\
\phi_3 : (x\ y\ z) &\mapsto (x\ y\ z) \begin{pmatrix} -7 & 8 & -2 \\ 8 & -2 & -7 \\ -2 & -7 & 8 \end{pmatrix}
\end{aligned}$$

(with $\phi_1^3 = \phi_2^7 = \phi_3^2 = 1$).

An alternative representation of this curve, in three dimensions, is given by

$$x^4 + y^4 + z^4 + u^4 = 19xyzu, \quad x + y + z + u = 0,$$

which displays the action of the symmetric group S_4 (a subgroup of $\mathrm{PSL}(2,7)$) on the arc. In this representation, the points of the arc correspond to the 24 permutations of the coordinates $(1,4,9,15)$.

Chao and Kaneta [7] had already discovered this arc (and the order of its automorphism group) by computer but did not give an explicit description of its points or mention the connection with the Klein quartic.

7

Special $(k,3)$-arcs in $\mathrm{PG}(2,q), q \leq 13$

We continue our investigation of special arcs with the $(k,3)$-arcs in $\mathrm{PG}(2,q)$, $q \leq 13$. As in the case of $(k,2)$-arcs, we managed to discover several general types of arc, using the results presented in Chapter 5. These arcs are described in Sections 7.1, 7.2 and 7.3. In Sections 7.5- 7.8, we have a closer look at some of the arcs for each q up to 13.

7.1 Some arcs with automorphism group S_4

Among the results, we again found some arcs that accept the symmetric group S_4 as a group of automorphisms and that can be generalized to other values of q. In Section 6.2, we described the conditions for which the set $S^*(a)$ of 12 points is a $(k,2)$-arc. The conditions for which this same set now is a $(k,3)$-arc are somewhat relaxed and will be described in this section.

Theorem 7.1 *Let $a \in \mathbb{F}_q$, q odd. Let $S^*(a)$ denote the set of points of $\mathrm{PG}(2,q)$ with coordinates of the form $(a,\pm1,\pm1)$, $(\pm1,a,\pm1)$ or $(\pm1,\pm1,a)$, with independent choices of sign. Let $S^*(\infty)$ be the set of points with coordinates $(1,0,0)$, $(0,1,0)$ or $(0,0,1)$.*

The set $S^*(a)$ $(= S^*(-a))$ is a $(12,3)$-arc of $\mathrm{PG}(2,q)$ if and only if

$$a \notin \{0, \pm1, \pm\sqrt{-1}\}. \tag{7.1}$$

The set $S^*(a) \cup S^*(\infty)$ is a $(15,3)$-arc if and only if a satisfies (7.1).

The set $S^*(a) \cup S^*(0)$ is a $(18,3)$-arc if and only if a satisfies (7.1) and

$$a \neq \pm2, a^2 \pm a \pm 2 \neq 0. \tag{7.2}$$

The group S_4 acts as a group of automorphisms for each of these sets.

Proof : Note that $|S^*(a)| = 12$ if and only if $a \neq 0, \pm1$ or ∞ and that $|S^*(0)| = 6$.

The symmetric group of order 24 acts transitively on $S^*(a)$, $S^*(0)$ and $S^*(\infty)$ (cf. Section 6.2).

To prove that $S^*(a)$ is an arc we show that no quadruple of different points of $S^*(a)$ is collinear. Because S_4 is a transitive group of automorphisms, we may chose an arbitrary element of $S^*(a)$ as the first point of each quadruple, say

$P_0(a) = (1, 1, a)$.

We will also use a second type of symmetry to reduce the number of quadruples we need to consider: substituting $-a$ for a everywhere permutes the points of $S^*(a)$ and therefore $S^*(a) = S^*(-a)$. Hence, for what follows, all conditions we derive for a must also hold for $-a$.

Interchanging the first two coordinates leaves $P_0(a)$ invariant and the stabilizer of $P_0(a)$ splits $S^*(a) \setminus \{P_0(a)\}$ into a singleton orbit $\{P_1(a)\}$ and 5 pairs $\{P_i(a), P_i'(a)\}$, as follows:

$$\begin{array}{lcllcl}
P_1(a) & = & (-1,-1,a), & & & \\
P_2(a) & = & (1,-1,a), & P_2'(a) & = & (-1,1,a), \\
P_3(a) & = & (1,a,1), & P_3'(a) & = & (a,1,1), \\
P_4(a) & = & (-1,a,-1), & P_4'(a) & = & (a,-1,-1), \\
P_5(a) & = & (a,-1,1), & P_5'(a) & = & (-1,a,1), \\
P_6(a) & = & (a,1,-1), & P_6'(a) & = & (1,a,-1).
\end{array}$$

Hence, taking $P_1(a), \ldots, P_6(a)$ as representatives of these 6 orbits, it suffices to show that for each $i = 1, \ldots, 6$ the line $P_0(a)P_i(a)$ intersects $S^*(a)$ in at most three points.

In fact, it is not necessary to investigate all six of these cases. Note for instance that applying $(x, y, z) \to (y, x, -z)$ to $P_3(a)$ yields $P_5(-a)$ and applying the same transformation to $P_0(a)$ yields $P_0(-a)$. Hence $P_0(a)P_5(a)$ will intersect $S^*(a)$ in at most three points, if and only if $P_0(a)P_3(a)$ does so. The same relation exists between $P_0(a)P_6(a)$ and $P_0(a)P_4(a)$.

We may therefore restrict ourselves to the first four cases:

1. $P_0(a)P_1(a)$, with equation $f_1(x, y, z) = x - y = 0$,
2. $P_0(a)P_2(a)$, with equation $f_2(x, y, z) = ax - z = 0$,
3. $P_0(a)P_3(a)$, with equation $f_3(x, y, z) = (a + 1)x - y - z = 0$,
4. $P_0(a)P_4(a)$, with equation $f_4(x, y, z) = -(1 + a^2)x + (1 - a)y + (1 + a)z = 0$.

In the first part of Table 7.1 we list the values of $f_i(r)$ for each of the 12 points r of $S^*(a)$.

For $S^*(a)$ to be a $(k,3)$-arc, none of the colums for $f_1(r) \ldots f_4(r)$ may contain more than 3 zeroes for rows that correspond to $S^*(a)$. From the columns for $f_1(r)$ and $f_2(r)$ we find the conditions $2 \neq 0$, $a \neq 0$, $a \neq \pm 1$ and $a^2 \neq \pm 1$. $f_3(r)$ yields the extra condition that not both a^2+a+2 and a^2+a-2 can be zero. This only happens when $4 = 0$, which was already excluded bij $f_1(r)$. From $f_4(r)$, we know that at most one of $-a^3-a+2=0$, $-a^3-a-2=0$ and $a^2+3=0$ is allowed. When both $-a^3-a+2$ and $-a^3-a-2$ are zero, we again find $4=0$. When both $-a^3-a+2=0$ and $a^2+3=0$, we find $3a-a+2=0$ or $2a+2=0$, while when both $-a^3-a-2=0$ and $a^2+3=0$, we find $3a-a-2=0$ or $2a-2=0$.

Hence, when q is odd and a satisfies (7.1), no four different points of $S^*(a)$ lie on the same line, and we may conclude that $S^*(a)$ is indeed a $(12,3)$-arc.

Because $S^*(a)$ is a $(k,3)$-arc and $S^*(\infty)$ only contains three points, a line containing four points of $S^*(a) \cup S^*(\infty)$ must contain at least one point of $S^*(a)$ and one point of $S^*(\infty)$. By symmetry, we may again choose the element $P_0(a) = (1,1,a)$ of $S^*(a)$ as the first point of such a line. The stabilizer of $P_0(a)$ splits $S^*(\infty)$ into the singleton $\{T_1(0,0,1)\}$ and the pair $\{T_2(0,1,0), T_2'(1,0,0)\}$. Hence, it suffices to show that $P_0(a)T_1$ and $P_0(a)T_2$ intersect $S^*(a) \cup S^*(\infty)$ in at most three points. It is easily computed that $P_0(a)T_1 = P_0(a)P_1(a)$ and $P_0(a)T_2 = P_0(a)P_2(a)$ and hence again by inspecting the colums for $f_1(r)$ and $f_2(r)$ we see that no additional conditions are needed for $S^*(a) \cup S^*(\infty)$ to be a $(k,3)$-arc.

Finally, consider the set $S^*(a) \cup S^*(0)$. It is easily checked that the set $S^*(0)$ never contains more than three points on a line and when (7.1) is satisfied neither does $S^*(a)$. The set $S^*(0)$ has four trisecants and three bisecants. The trisecants have equations $x \pm y \pm z = 0$ with independent choices of sign, the bisecants are the lines with equations $x=0$, $y=0$ and $z=0$.

A line containing four points of $S^*(a) \cup S^*(0)$ is one of three types. First, we have the lines that are trisecants of $S^*(a)$ and contain one point of $S^*(0)$. To avoid such lines, we must be sure that no columns of Table 7.1 contain more

		$f_1(r)$	$f_2(r)$	$f_3(r)$	$f_4(r)$
		$x-y$	$ax-z$	$(a+1)x-y-z$	$-(1+a^2)x$ $+(1-a)y+(1+a)z$
$S^*(a)$	$(1,1,a)$	0	0	0	0
	$(-1,-1,a)$	0	$-2a$	$-2a$	$2a(1+a)$
	$(1,-1,a)$	2	0	2	$2(-1+a)$
	$(-1,1,a)$	-2	$-2a$	$-2(1+a)$	$2(a^2+1)$
	$(1,a,1)$	$1-a$	$-1+a$	0	$-2a(-1+a)$
	$(1,a,-1)$	$1-a$	$1+a$	2	$-2(a^2+1)$
	$(-1,a,-1)$	$-1-a$	$1-a$	$-2a$	0
	$(-1,a,1)$	$-1-a$	$-1-a$	$-2(1+a)$	$2(1+a)$
	$(a,1,1)$	$-1+a$	a^2-1	a^2+a-2	$-a^3-a+2$
	$(a,-1,-1)$	$1+a$	a^2+1	a^2+a+2	$-a^3-a-2$
	$(a,1,-1)$	$-1+a$	a^2+1	$a(1+a)$	$-a(a^2+3)$
	$(a,-1,1)$	$1+a$	a^2-1	$a(1+a)$	$-a(a^2-1)$
$S^*(0)$	$(1,1,0)$	0	a	a	$-a(1+a)$
	$(-1,1,0)$	-2	$-a$	$-2-a$	a^2-a+2
	$(1,0,1)$	1	$-1+a$	a	$a(1-a)$
	$(-1,0,1)$	-1	$-1-a$	$-2-a$	a^2+a+2
	$(0,1,1)$	-1	-1	-2	2
	$(0,-1,1)$	1	-1	0	$2a$
$S^*(\infty)$	$(1,0,0)$	1	a	$1+a$	$-a^2-1$
	$(0,1,0)$	-1	0	-1	$1-a$
	$(0,0,1)$	0	-1	-1	$1+a$

Table 7.1: Lists the values of $f_i(r)$ for each of the points in the left column (cf. proof of Theorem 7.1).

than three zeroes in rows corresponding to $S^*(a) \cup S^*(0)$. This yields the extra conditions $a \neq -2$, $a^2 \pm a + 2 \neq 0$ and $a^2 + a \pm 2 \neq 0$. Second, we have the lines that are bisecants of $S^*(a)$ and bisecants of $S^*(0)$. Such a line must be one of $x = 0$, $y = 0$ and $z = 0$, but none of the points $(a, \pm 1, \pm 1)$, $(\pm 1, a, \pm 1)$ or $(\pm 1, \pm 1, a)$ lies on such a line. Last, we have the lines that are trisecants of $S^*(0)$ and contain one point of $S^*(a)$. Because $\pm 1 \pm 1 \pm a \neq 0$, this case also never occurs. Hence, when (7.1) and (7.2) are satisfied, $S^*(a) \cup S^*(0)$ is a $(k,3)$-arc. ∎

As with $(k,2)$-arcs, in some cases we can add the set I of size 6 to $S^*(a)$:

Theorem 7.2 *Let $q = 1 \bmod 4$. Let $a, i \in \mathbb{F}_q$, such that $i^2 = -1$. Let $S^*(a)$ be defined as in Theorem 7.1. Let I denote the set of six points whose coordinates are permutations of $(1, i, 0)$. (I is a subset of the conic $C : x^2 + y^2 + z^2 = 0$.)*

Then $S^*(a) \cup I$ is an $(18,3)$-arc of $\mathrm{PG}(2,q)$ if and only if

$$a \notin \{0, \pm 1, \pm i, \pm i \pm 1, \pm 2i)\}. \tag{7.3}$$

Proof :

To prove this theorem, we can follow the proof of Theorem 6.3. For $S^*(a)$ to be a $(k,3)$-arc we now have the conditions (7.1). Also instead of no collinear triple, we can now have no collinear quadruples in $S^*(a) \cup I$. Therefore in Table 6.1, we cannot have more than three zeroes in each colum.

Apart from the conditions $a \notin \{0, \pm 1, \pm i\}$ of Theorem 7.1, we also find the following conditions: from the first colum $a \neq \pm i \pm 1$. Also no two of $ia^2 \pm ia + i \pm 1$ can be zero at the same time. However, this yields no new conditions. From the second colum, we find that $a \neq \pm i$ and $a \neq \pm 2i$. ∎

In Theorem 6.4, we proved that the set $S^*(1) \cup I$ is a $(k,2)$-arc if $i \neq \pm 2$. If we drop this condition, then $S^*(1) \cup I$ still remains a $(k,3)$-arc. Indeed, Table 6.3 will still contain at most 3 zeroes (cf. proof of Theorem 6.4).

Also note that the line $x = y$ always intersects $S^*(a) \cup S^*(0) \cup S^*(\infty)$ in four points (when $a \neq 0$), hence this set is never a $(k,3)$-arc. Also, the line $x = 0$ intersects $S^*(a) \cup S^*(0) \cup I$ and $S^*(a) \cup S^*(\infty) \cup I$ in four points, so these sets neither are $(k,3)$-arcs.

In Table 7.2 we present the values of a for which an arc of type $S^*(a), S^*(a) \cup S^*(\infty), S^*(a) \cup S^*(0)$ or $S^*(a) \cup I$ exists for all $q \leq 29$. If the arc exists, the table mentions whether the arc is complete or not (NC stands for not complete). If the set is not a $(k,3)$-arc, then the space is left blank.

Again, in some cases, S_4 is not the full automorphism group of $S^*(a)$. For instance, if $q \equiv 1 \pmod 3$ and $a^3 = 1$, $a \neq 1$, then $(x,y,z) \mapsto (x,ay,a^2z)$ extends the group of automorphisms of $S^*(a)$ to $S_4 \colon 3$.

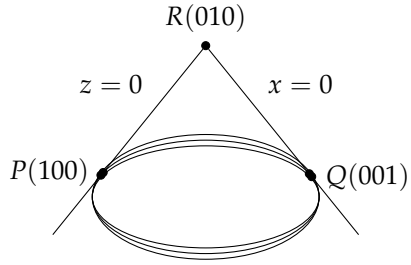
7.2 $(k,3)$-arcs from half conics

For $q = 11$ the table of the complete $(k,3)$-arcs lists 6 complete $(k,3)$-arcs with an automorphism group of type D_{10}. In this section we shall describe how to construct these arcs and show that this construction can be generalised to other (small) fields, yielding arcs having a cyclic group of order $\frac{q-1}{2}$ or a dihedral group D_{q-1} as a group of automorphisms.

Let q be odd. Let $D \in \mathbb{F}_q^*$. Denote by C_D the conic with equation $xz = Dy^2$. This conic belongs to the pencil of conics that are tangent to the lines $x = 0$ and $z = 0$ in the points P and Q with coordinates $(1,0,0)$ and $(0,0,1)$. These tangents intersect in the point R with coordinates $(0,1,0)$.

q	a	$S^*(a)$	$S^*(a) \cup S^*(\infty)$	$S^*(a) \cup S^*(0)$	$S^*(a) \cup I$
5	± 2	NC			
7	$\pm 2, \pm 3$	NC	NC		
9	$\pm\alpha, \pm\alpha^3$	NC	NC		
11	± 2	NC	NC		
	$\pm 4, \pm 5$	NC	complete		
	± 3	NC	NC	complete	
13	± 2	NC	NC		NC
	± 3	NC	NC	NC	NC
	± 4	NC	NC	NC	
	± 6	NC	NC	complete	
17	± 2	NC	NC		NC
	$\pm 3, \pm 5$	NC	NC	NC	
	$\pm 6, \pm 7, \pm 8$	NC	NC	NC	NC
19	± 2	NC	NC		
	$\pm 3, \pm 4, \pm 5, \pm 6,$ $\pm 7, \pm 8, \pm 9$	NC	NC	NC	
23	$\pm 2, \pm 9, \pm 10$	NC	NC		
	$\pm 3, \pm 4, \pm 5,$ $\pm 6, \pm 7, \pm 8 \pm 11$	NC	NC	NC	
25	$\pm\alpha, \pm\alpha^5$	NC	NC		NC
	$\pm\alpha^2, \pm\alpha^3, \pm\alpha^4, \pm\alpha^7,$ $\pm\alpha^8, \pm\alpha^9, \pm\alpha^{10}, \pm\alpha^{11}$	NC	NC	NC	NC
27	$\pm\alpha, \pm\alpha^2, \pm\alpha^3, \pm\alpha^4,$ $\pm\alpha^5 \pm \alpha^6, \pm\alpha^7, \pm\alpha^8,$ $\pm\alpha^9, \pm\alpha^{10}, \pm\alpha^{11}, \pm\alpha^{12}$	NC	NC	NC	
29	$\pm 2, \pm 7, \pm 8$	NC	NC		NC
	$\pm 13, \pm 11$	NC	NC	NC	
	$\pm 3, \pm 4, \pm 5, \pm 6,$ $\pm 9, \pm 10, \pm 14$	NC	NC	NC	NC

Table 7.2: Lists the values of a for which an arc of the types in the colums exists for all $q \leq 29$.



Except for P and Q, all points of C_D can be given coordinates of the form $(1, t, Dt^2)$ with $t \in \mathbb{F}_q^*$. We shall call t the *parameter* of the corresponding point of C_D.

Let C_D^+ denote the set of all points of C_D whose parameter is a non-zero square. Likewise, let C_D^- denote the set of all points of C_D with a parameter that is not a square. Note that $C_D = C_D^+ \cup C_D^- \cup \{P, Q\}$. The sets C_D^+ and C_D^- will be called *half conics*.

The sets C_D^+ and C_D^- are left invariant by a dihedral group of order $q-1$ generated by the projective transformations

$$\phi_1 : (x, y, z) \mapsto (x, \alpha^2 y, \alpha^4 z)$$

and

$$\begin{cases} \phi_2 : (x, y, z) \mapsto (z, y, x) & \text{if } D \text{ is a square,} \\ \phi_3 : (x, y, z) \mapsto (z, \alpha y, \alpha^2 x) & \text{if } D \text{ is a non-square.} \end{cases}$$

with α a generator of the multiplicative group of $\mathbb{F}_q$. The sets C_D^+ and C_D^- are interchanged by ϕ_2 if D is a non-square, and by ϕ_3 if D is a square. In terms of parameters t, the dihedral group is generated by $t \mapsto \alpha^2 t$ (ϕ_1) and $t \mapsto 1/Dt$ (ϕ_2) or $t \mapsto \alpha/Dt$ (ϕ_3).

Note that any transformation of the form $(x, y, z) \mapsto (x, y, kz)$ with $k \in \mathbb{F}_q^*$, maps C_D^+ onto C_{kD}^+. Also, the transformation $(x, y, z) \mapsto (x, \alpha y, \alpha^2 z)$ maps C_D^+ onto C_D^-.

As a consequence, when considering a number of half conics, without loss of generality we may take one of them to be C_1^+.

It turns out that for smaller values of q we can construct $(k,3)$-arcs by taking the union of three such half conics, yielding arcs of size $\frac{3}{2}(q-1)$. We have generated by computer all arcs of this form for $q \leq 79$. The results (up to equivalence) are listed in Table 7.3 (together with their automorphism group). We conjecture that for $q > 19$ no arcs of this type exist.

$q=5$		$q=11$		$q=13$	
$C_1^+ \cup C_1^- \cup C_2^+$	[120]	$C_1^+ \cup C_1^- \cup C_5^+$	D_{10}	$C_1^+ \cup C_1^- \cup C_7^+$	D_{12}
$C_1^+ \cup C_1^- \cup C_3^+$	D_4	$C_1^+ \cup C_1^- \cup C_7^+$	D_{10}	$C_1^+ \cup C_2^+ \cup C_4^+$	6
$q=7$		$C_1^+ \cup C_1^- \cup C_9^+$	D_{10}	$C_1^+ \cup C_2^+ \cup C_{11}^+$	6
$C_1^+ \cup C_1^- \cup C_2^+$	D_6	$C_1^+ \cup C_2^+ \cup C_3^+$	5	$C_1^+ \cup C_4^+ \cup C_6^+$	6
$C_1^+ \cup C_1^- \cup C_4^+$	D_6	$C_1^+ \cup C_2^+ \cup C_4^+$	5	$q=19$	
$C_1^+ \cup C_1^- \cup C_5^+$	D_6	$C_1^+ \cup C_2^+ \cup C_5^+$	5	$C_1^+ \cup C_7^+ \cup C_{11}^+$	[162]
$C_1^+ \cup C_1^- \cup C_6^+$	[54]	$C_1^+ \cup C_2^+ \cup C_{10}^+$	5	$C_1^+ \cup C_8^+ \cup C_{11}^+$	9
$C_1^+ \cup C_2^+ \cup C_3^+$	D_6	$C_1^+ \cup C_4^+ \cup C_5^+$	D_{10}		
$C_1^+ \cup C_2^+ \cup C_4^+$	[54]	$C_1^+ \cup C_4^+ \cup C_7^+$	5		
$C_1^+ \cup C_3^+ \cup C_2^-$	3^2	$C_1^+ \cup C_4^+ \cup C_9^+$	D_{10}		
$q=9$		$C_1^+ \cup C_8^+ \cup C_9^+$	5		
$C_1^+ \cup C_1^- \cup C_{-\alpha}^+$	S_4	$C_1^+ \cup C_2^+ \cup C_{10}^-$	5		
$C_1^+ \cup C_1^- \cup C_{-\alpha^3}^+$	S_4	$C_1^+ \cup C_4^+ \cup C_9^-$	D_{10}		
$C_1^+ \cup C_\alpha^+ \cup C_{\alpha^2}^+$	4				
$C_1^+ \cup C_\alpha^+ \cup C_{\alpha^3}^+$	$3:4$				
$C_1^+ \cup C_{\alpha^2}^+ \cup C_{-\alpha}^+$	4				
with $\alpha = 1+\sqrt{-1}$, i.e., $\alpha^2+\alpha=1$.					

Table 7.3: Complete list of arcs, up to equivalence, that consist of three 'half conics' (for $q \leq 79$)

The arcs of this type can be roughly divided into three kinds:

- those that contain two half conics with the same index D, i.e., almost the full conic C_D,
- those that use three half conics of the same sign,
- those that use half conics of two different signs, and never with the same index

The following lemma shows that those of the first and third kind will never be complete arcs

Lemma 7.3 *Let $D, E, F \in \mathbb{F}_q$, $D \neq E$. If $S = C_D^+ \cup C_E^+ \cup C_F^-$ is a $(k,3)$-arc, then so is $S \cup \{P, Q\}$.*

Proof : First note that no line through $Q(0,0,1)$ can already contain 3 points of S. If that were the case, then each of these points would have the same middle coordinate (assuming coordinates are normalized to have first coordinate equal to 1). But the middle coordinates of C_D^+ and C_E^+ are squares, while those of C_F^- are not.

By symmetry, also no line through $P(1,0,0)$ can already contain 3 points and finally, the line joining P and Q, i.e., the line with equation $y = 0$ does not intersect S. ∎

Lemma 7.4 *Let $q \equiv -1 \pmod 4$ (i.e., -1 is not a square). Let $D, E, F \in \mathbb{F}_q$, $D \neq E \neq F \neq D$. If $S = C_D^\pm \cup C_E^\pm \cup C_F^\pm$ (with independent choices of sign) is a $(k,3)$-arc, and $\{D, E, F\}$ contains at least one square and one non-square, then also $S \cup \{R\}$ is a $(k,3)$-arc.*

Proof : A line through $R(0,1,0)$ intersects S in points that have the same last coordinate. If -1 is not a square, then a half conic $C_D^\pm$ can contain at most one point with a given last coordinate, and that last coordinate will be a square if and only if D is a square. As D, E, F are not all squares or all non-squares, the line can not contain 3 points of S. ∎

From the proofs of these lemmas it follows that all three points P, Q, R can be added when the conditions of both lemmas are both satisfied.

The converse is not true: if neither lemma is satisfied this does not necessarily imply that an arc $S = C_D^{\pm} \cup C_E^{\pm} \cup C_F^{\pm}$ is complete. In fact we only find the following three complete arcs of size $\frac{3}{2}(q-1)$: in $\mathrm{PG}(2,11)$, $C_1^+ \cup C_4^+ \cup C_5^+$ and $C_1^+ \cup C_4^+ \cup C_9^+$ are complete. In $\mathrm{PG}(2,19)$ the set $C_1^+ \cup C_7^+ \cup C_{11}^+$ is complete.

There are two arcs of the second kind that merit special attention. For $q = 7$ and $q = 19$ the sets $C_1^+ \cup C_\omega^+ \cup C_{\omega^2}^+$ with $\omega^3 = 1$, $\omega \neq 1$ are $(k,3)$-arcs. These arcs admit an additional symmetry $(x,y,z) \mapsto (x,y,\omega z)$ that permute the three half conics. For $q = 7$, this arc is the set $C_1^+ \cup C_2^+ \cup C_4^+$. It is the set S_1 from Theorem 7.5 which is not complete. For $q = 19$, this arc is the set $C_1^+ \cup C_7^+ \cup C_{11}^+$ which is complete.

Note that the two arcs for $q = 9$ with S_4 as automorphism group are arcs of the type as described in Section 7.1 with $a = \alpha^3$ for $C_1^+ \cup C_1^- \cup C_{-\alpha}^+$ and $a = \alpha$ for $C_1^+ \cup C_1^- \cup C_{-\alpha^3}^+$.

For completeness we would like to point out that the complete $(13,3)$-arc with group D_{10} for $q = 11$, can be constructed by combining *two* half conics (C_1^+ and C_3^+) and the three points P, Q and R.

7.3 (k,3)-arcs from cubic curves

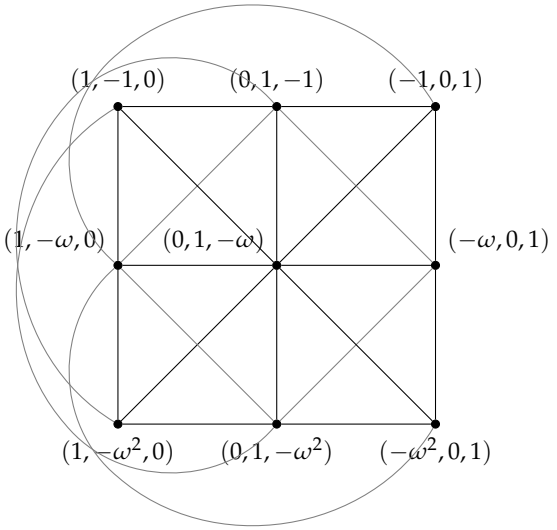
7.3.1 The Hessian configuration

Let $q \equiv 1 \pmod 3$. Then the field $\mathbb{F}_q$ contains an element $\omega \neq 1$ such that $\omega^3 = 1$ (and hence $\omega^2 + \omega + 1 = 0$).

Consider the set $\mathcal{H}$ of the nine points with the following coordinates :

$$\begin{array}{ccc} (1,-1,0) & (0,1,-1) & (-1,0,1) \\ (1,-\omega,0) & (0,1,-\omega) & (-\omega,0,1) \\ (1,-\omega^2,0) & (0,1,-\omega^2) & (-\omega^2,0,1) \end{array}$$

The set $\mathcal{H}$ is called the *Hessian configuration* and has many interesting properties [1, 19]. It is a $(9,3)$-arc such that every point lies on exactly 4 trisecants and no bisecants. There are 12 trisecants in all. The configuration of points and trisecants represents an affine plane $\mathrm{AG}(2,3)$ embedded in $\mathrm{PG}(2,q)$. (Note that for $q=7$ this arc is complete and regular.)



$\mathcal{H}$ is the set of intersection points of the *Hesse pencil* of cubic curves generated by $xyz=0$ and $x^3+y^3+z^3=0$. In fact, $\mathcal{H}$ is the set of nine inflection points for each of the irreducible cubics in this pencil.

Every cubic curve in the Hesse pencil is left invariant by the group G_{18} (of order 18) that is generated by the permutations of the coordinates together

with the transformation $\sigma_\omega : (x,y,z) \mapsto (x,\omega y,\omega^2 z)$. For specific curves in the pencil the automorphism group can be larger. The group of projective transformations that leaves $\mathcal{H}$ itself invariant has order 216.

Let C_c denote the cubic of the Hessian pencil with equation $x^3+y^3+z^3+cxyz$, with $c \in \mathbb{F}_q$. C_c is irreducible (and non-singular) if and only if $c \neq -3, -3\omega, -3\omega^2$. In that case, the Abelian group associated with C_c (with one of its inflection points chosen as neutral element) has $\mathcal{H}$ as a subgroup. It follows that $|C_c|$ must be divisible by $|\mathcal{H}| = 9$. The following table lists the largest possible value of $|C_c|$ for finite fields not larger than 256.

q	$\max_c \lvert C_c\rvert$	q	$\max_c \lvert C_c\rvert$	q	$\max_c \lvert C_c\rvert$
4	9	64	81	157	180
7	9	67	81	163	189
13	18	73	90	169	189
16	18	79	90	181	207
19	27	97	117	193	216
25	36	103	117	199	225
31	36	109	126	211	234
37	45	121	144	223	252
43	54	127	144	229	252
49	63	139	162	241	270
61	72	151	171	256	288

For many fields these cubic curves C_c provide $(k,3)$-arcs of a reasonably large size. All listed sizes lie in the interval $[q+\sqrt{q}-1, q+2\sqrt{q}+1]$ and in some cases ($q = 4, 25, 64, 121, 256$) the upper bound (the Hasse bound) is even reached.

We shall be interested in the cubic curve C_1, i.e., the curve with equation $x^3+y^3+z^3+xyz = 0$. Consider the set $\mathcal{H}_1$ of the nine points with the following coordinates :

$$\begin{array}{ccc} (1,1,-1) & (1,-1,1) & (1,-1,-1) \\ (1,\omega,-\omega^2) & (1,-\omega,\omega^2) & (1,-\omega,-\omega^2) \\ (1,\omega^2,-\omega) & (1,-\omega^2,\omega) & (1,-\omega^2,-\omega) \end{array}$$

It is easily seen that each of these points belongs to the curve C_1.

Both $\mathcal{H}$ and $\mathcal{H}_1$ are orbits of G_{18}. The set $\hat{\mathcal{H}} \stackrel{\text{def}}{=} \mathcal{H} \cup \mathcal{H}_1$ is an $(18,3)$-arc. The tangent to the curve C_1 in a point of $\mathcal{H}_1$ intersects a point of $\mathcal{H}$. (For example, the line $x+y+2z=0$ is a tangent at $(1,1,-1)$ and intersects $\mathcal{H}$ in $(1,-1,0)$.) Apart from these 9 tangents (which are bisecants to the arc) all other lines connecting two points of $\mathcal{H}_1$ are trisecants.

As a consequence $\hat{\mathcal{H}}$ is a subgroup of the Abelian group of the curve C_1, and hence $|C_1|$ is a multiple of 18. Note that $\mathcal{H}$ is a subgroup of index 2 of $\hat{\mathcal{H}}$, and hence the corresponding coset $\mathcal{H}_1$ is necessarily a $(9,2)$-arc (which does not lie on a conic).

The $(9,2)$-arc $\mathcal{H}_1$ can be extended to a $(k,3)$-arc in other ways. Consider for example the set S_ω :

$$\begin{array}{ccc} (1,0,0) & (0,1,0) & (0,0,1) \\ (\omega^2,1,1) & (1,\omega^2,1) & (1,1,\omega^2) \end{array}$$

which consists of two orbits of G_{18}, each of size 3. It is easily seen that this set is a $(6,2)$-arc, and that the 15 bisecants have the following equations :

$$\begin{array}{ccc} x=0, & y=0, & z=0, \\ & & \\ x=y, & y=z, & z=x, \\ x=\omega y, & y=\omega z, & z=\omega x, \\ x=\omega^2 y, & y=\omega^2 z, & z=\omega^2 x, \end{array}$$

$$\omega x+y+z=0, \quad x+\omega y+z=0, \quad x+y+\omega z=0,$$

forming three orbits of G_{18} (of sizes 3, 9, 3). By considering one line in each orbit, it is easily seen that no bisecant of S_ω intersects $\mathcal{H}_1$ in more than one point. As both S_ω and $\mathcal{H}_1$ are $(k,2)$-arcs, this proves that $\mathcal{H}_1 \cup S_\omega$ is a $(15,3)$-arc.

There is another way to extend $\mathcal{H}_1$ to an arc with interesting properties. Consider the set $\mathcal{H}_1'$ obtained by extending $\mathcal{H}_1$ with the following orbit of G_{18} :

$$(1,1,1), \quad (1,\omega,\omega^2), \quad (1,\omega^2,\omega)$$

In other words, $\mathcal{H}_1'$ contains the 12 points with coordinates that are of the form $(\pm 1, \pm 1, \pm 1)$, $(\pm 1, \pm\omega, \pm\omega^2)$ or $(\pm 1, \pm\omega^2, \pm\omega)$. The symmetric group S_4 acts on $\mathcal{H}_1'$ by permuting the coordinates and allowing independent sign changes of the coordinates. Together with σ_ω this group extends to a group G_{72} of automorphisms of type $S_4 : 3$, of size 72.

In fact, applying the transformation $z \mapsto \omega z$ shows that $\mathcal{H}_1'$ is equivalent to $S^*(\omega)$ of Theorem 7.1 and therefore a $(12,3)$-arc (and even a $(12,2)$-arc provided the characteristic of the field is not 7).

By the same theorem it can be extended to a $(15,3)$-arc by adding the points $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$, still with G_{72} as a group of automorphisms, and to an $(18,3)$-arc provided the characteristic of the field is not 5 or 7. The latter arc no longer has σ_ω as an automorphism.

7.3.2 A (18,3)-arc with $G_S \approx 3_+^{1+2}$

Theorem 7.5 *Let $q \equiv 1 \pmod 3$. Let $\omega \in \mathbb{F}_q$, $\omega \neq 1$ such that $\omega^3 = 1$. Let $c \in \mathbb{F}_q$.*

Consider the sets S_1 and $S_2(c)$ of points with the following coordinates :

S_1			$S_2(c)$		
$(1,1,1)$	$(1,1,\omega)$	$(1,1,\omega^2)$	$(1,0,c)$	$(\omega,0,c)$	$(\omega^2,0,c)$
$(1,\omega,1)$	$(1,\omega,\omega)$	$(1,\omega,\omega^2)$	$(0,c,1)$	$(0,c,\omega)$	$(0,c,\omega^2)$
$(1,\omega^2,1)$	$(1,\omega^2,\omega)$	$(1,\omega^2,\omega^2)$	$(c,1,0)$	$(c,\omega,0)$	$(c,\omega^2,0)$

(7.4)

Then $S_1 \cup S_2(c)$ is an $(18,3)$-arc if and only if $c \neq 0$ and $c^3 \neq \pm 1$. The group $G_{27} \approx 3_+^{1+2}$ of size 27, generated by the elements

$$(x,y,z) \mapsto (x,\omega y,z), \quad (x,y,z) \mapsto (x,y,\omega z), \quad (x,y,z) \mapsto (y,z,x),$$

is a group of automorphisms of $S_1 \cup S_2(c)$.

Proof : Note that $|S_1| = |S_2(c)| = 9$, as $c \neq 0$.

First consider the case $c^3 = -1$, i.e., $c = -1$, $-\omega$ or $-\omega^2$. In that case $S_2(c)$ is precisely the Hesse configuration $\mathcal{H}$. Then the trisecant of $\mathcal{H}$ with equation $x + y + z = 0$ intersects S_1 in the additional points $(1, \omega, \omega^2)$ and $(1, \omega^2, \omega)$ and therefore $S_1 \cup S_2(c)$ is not an (18,3)-arc. Henceforth we shall assume that $c^3 \neq -1$.

It is easily verified that G_{27} leaves both S_1 and $S_2(c)$ invariant. If we extend G_{27} to G_{54} by the map which interchanges two coordinates, then G_{54} still leaves S_1 invariant, but not $S_2(c)$ (unless $c = 1$, ω or ω^2, i.e., $c^3 = 1$).

The stabilizer of $(1, 1, 1)$ in G_{54} consists of the 6 coordinate permutations and has three orbits on S_1. It is therefore easily seen that the lines connecting $(1, 1, 1)$ with any other point of S_1 have equations

$$x = y, \quad x + \omega y + \omega^2 z = 0$$

or an equation obtained from these by permuting x, y, z.

It follows that S_1 is a $(9, 3)$-arc in which every point lies on three trisecants (the orbit of G_{54} of the first equation above) and two bisecants (the orbit of the second equation). It also follows that if $c^3 \neq 1$ then no point of $S_2(c)$ lies on a trisecant of S_1. Likewise, if $c^3 \neq -1$, then no point of $S_2(c)$ lies on a bisecant of S_1.

As a consequence, any line which intersects $S_1 \cup S_2(c)$ in more than three points, must intersect $S_2(c)$ in more than two points. To determine these lines, consider the stabilizer of $(1, 0, c)$ in G_{27}. It consists of the 3 transformations that multiply the y-coordinate by either 1, ω or ω^2 and has 5 orbits on $S_2(c)$. The lines connecting $(1, 0, c)$ with any other point of $S_2(c)$ have equations

$$y = 0, \quad cx + \frac{1}{c}y - z = 0, \quad cx - c^2 y - z = 0,$$

or equations derived from these by multiplying the coefficient of y by ω or ω^2.

If $c^3 = -1, -\omega$ or $-\omega^2$, i.e., if $c^9 = -1$, then some of these lines will coincide and each point will then lie on 4 trisecants of $S_2(c)$. The case $c^3 = -1$ was

already excluded. If $c^3 = -\omega$ or $-\omega^2$, then it is easily verified that all 18 points of $S_1 \cup S_2(c)$ lie on the (irreducible) cubic with equation $x^3 - c^3y^3 + c^6z^3$, making it an $(18,3)$-arc.

If $c^9 \neq -1$, then the only line through $(1,0,c)$ which intersects $S_2(c)$ in more than two points is the line with equation $y = 0$. Clearly this line does not contain a point of S_1, hence again $S_1 \cup S_2(c)$ is an $(18,3)$-arc. ∎

The set S_1 consists precisely of the nine intersection points of the pencil of cubics generated by $x^3 = y^3$ and $y^3 = z^3$. In this pencil, consider the three cubics C, C', C'' with equations

$$\begin{aligned} C &: c^3(x^3 - y^3) = z^3 - y^3 \\ C' &: c^3(z^3 - x^3) = y^3 - x^3, \\ C'' &: c^3(y^3 - z^3) = x^3 - z^3. \end{aligned}$$

Note that these cubics coincide if and only if $c^6 - c^3 + 1 = 0$ and then all points of $S_1 \cup S_2(c)$ belong to that cubic. Otherwise, each of the cubics C, C', C'' intersects $S_2(c)$ in precisely three points, corresponding to the three rows in (7.4).

7.4 Special (k,3)-arcs for $q = 7$

In PG$(2,7)$, the two arcs of size 11 with automorphism group S_3 consist of three 'half' conics (as defined in Section 7.2) and two extra points. Using the notations of that section, these arcs are

$$\begin{aligned} S_{11} &= C_1^+ \cup C_1^- \cup C_4^+ \cup \{P, Q\}, \\ S'_{11} &= C_1^+ \cup C_2^+ \cup C_3^+ \cup \{P, R\}. \end{aligned}$$

Also, adding the points P, Q and R to the last arc in Table 7.3 for $q = 7$ yields a complete arc:

$$S_{12} = C_1^+ \cup C_3^+ \cup C_2^- \cup \{P, Q, R\}.$$

The automorphism group of this arc is 3^2.

The unique complete arc of size 9 in PG$(2,7)$ corresponds to the Hessian configuration described in Section 7.3.1.

7.5 Special (k,3)-arcs for $q = 8$

In what follows let α denote a primitive generating element of $\mathbb{F}_8$ which satisfies $\alpha^3 + \alpha^2 + 1 = 0$. The Frobenius automorphism σ of the field corresponds to $k \mapsto k^2$.

The complete arc of size 11 with $\Gamma_S \approx 2A_4$ and $G_S \approx 2^3$

In PG$(2,8)$, there is a unique complete arc of size 11 consisting of 8 points on a conic and three collinear points not on that conic. If we take this conic $\mathcal{C}$ to have equation $y^2 = xz$, then the arc points on the conic have coordinates $(1, t, t^2)$ with $t \in \mathbb{F}_8$. The three other arc points lie on the line ℓ with equation $x = 0$. This line is tangent to $\mathcal{C}$ in the point with coordinates $(0,0,1)$ which is not an arc point. Each triple of points on ℓ (not containing $(0,0,1)$) can be added to the set of arc points of the conic. However, only for 7 of these triples the arc is complete and these 7 arcs all turn out to be equivalent. Their group G_S is isomorphic to 2^3 and consist of the 8 elements

$$\phi_u : (x\ y\ z) \quad \mapsto \quad (x\ y\ z) \begin{pmatrix} 1 & u & u^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad u \in \mathbb{F}_q.$$

Adding the frobenius automorphism σ and its square σ^2 yields the automorphism group Γ_S which is isomorphic to $2A_4$.

The two complete arcs of size 15 with $\Gamma_S \approx 3A_4$ and $G_S \approx A_4$

Consider the set T of the following twelve points:

$$\begin{array}{cccc} (1,\alpha^4,\alpha) & (\alpha^2,\alpha,1) & (\alpha^4,\alpha^2,\alpha) & (\alpha,1,\alpha^4) \\ (1,\alpha,\alpha^2) & (\alpha^4,\alpha^2,1) & (\alpha,\alpha^4,\alpha^2) & (\alpha^2,1,\alpha) \\ (1,\alpha^2,\alpha^4) & (\alpha,\alpha^4,1) & (\alpha^2,\alpha,\alpha^4) & (\alpha^4,1,\alpha^2) \end{array}$$

In PG$(2,8)$ there are 24 points not lying on a line of the subplane PG$(2,2)$. The set T contains 12 of these points. We find three ways to split up these 12 points into two conical subsets. The equations of the corresponding conics are given below.

$$\begin{array}{cc} y^2 = xz & y^2 + z^2 = xz \\ x^2 = xz + yz & x^2 + z^2 = xz + yz \\ x^2 + y^2 = yz & x^2 + y^2 + z^2 = yz \end{array}$$

Also consider the following three sets of points of the line $z = 0$:

$$\begin{array}{ccc} T_1 & T_2 & T_3 \\ (1,0,0) & (1,\alpha,0) & (\alpha,1,0) \\ (0,1,0) & (1,\alpha^2,0) & (\alpha^2,1,0) \\ (1,1,0) & (1,\alpha^4,0) & (\alpha^4,1,0) \end{array}$$

The three points of the set T_1 lie in the respective intersections of the three conic pairs given above.

We find that the sets $T \cup T_1$ and $T \cup T_2$ are non-equivalent complete $(15,3)$-arcs. The set $T \cup T_3$ is however not an arc.

The three sets all have the alternating group on 4 elements A_4 as automorphism group. It can be generated by

$$\phi_1 : (x,y,z) \mapsto (x+y,x,z)$$

of order 3 and

$$\phi_2 : (x,y,z) \mapsto (x+z,y,z)$$

$$\phi_2' : (x, y, z) \mapsto (x, y + z, z)$$

of order 2. Note that the group A_4 is a subgroup of the stabilizer of the line $z = 0$ in $\mathrm{PGL}(3, 2)$. Adding the Frobenius automorphism yields the automorphism group $\Gamma_S \approx 3A_4$.

These arcs were already discovered by Bierbrauer [3].

7.6 Special (k,3)-arcs for $q = 9$

In what follows let α denote a primitive generating element of $\mathbb{F}_9$ which satisfies $\alpha^2 + \alpha - 1 = 0$. The Frobenius automorphism σ of the field corresponds to $k \mapsto k^3$.

The unique complete arc of size 14 with $\Gamma_S \approx G_S \approx 4$

In $\mathrm{PG}(2, 9)$, none of the arcs consisting of three 'half' conics as defined in Section 7.2 are complete. Using the same notations, we find that adding the points P and R to the sets yield the following two complete arcs:

$$\begin{aligned} S_{14} &= C_1^+ \cup C_\alpha^+ \cup C_{\alpha^2}^+ \cup \{P, R\}, \\ S_{14}' &= C_1^+ \cup C_{-\alpha}^+ \cup C_{\alpha^2}^+ \cup \{P, R\}. \end{aligned}$$

These arcs are PGL-inequivalent, but PΓL-equivalent and have a cylic automorphism group of order 4.

The unique complete arc of size 15 with $\Gamma_S \approx G_S \approx D_{10}$

In $\mathrm{PG}(2, 9)$, there is a unique complete arc having the dihedral group of order 10 as a group of automorphisms. It consists of all points of a conic C_1, together with half of the points of a second conic C_2. If C_1 has equation $y^2 = xz$, then

C_2 has equation $x^2 + y^2 - \alpha^2 z^2 + \alpha xz$. The points occur in three orbits of size 5 under the action of the automorphism group:

$$\begin{array}{ccccc} (1,\alpha,\alpha^2) & (1,\alpha^2,-1) & (1,0,0) & (1,-\alpha^2,-1) & (1,-\alpha,\alpha^2) \\ (1,1,1) & (1,-\alpha^3,-\alpha^2) & (0,0,1) & (1,\alpha^3,-\alpha^2) & (1,-1,1) \\ (1,\alpha^2,0) & (1,1,\alpha^3) & (1,0,\alpha^6) & (1,-1,\alpha^3) & (1,-\alpha^2,0) \end{array}$$

D_{10} is generated by

$$\phi_1 : (x\ y\ z) \quad \mapsto \quad (x\ -y\ z)$$

and

$$\phi_2 : (x\ y\ z) \quad \mapsto \quad (x\ y\ z) \begin{pmatrix} \alpha^3 & \alpha & -\alpha^3 \\ -1 & 1 & -1 \\ -1 & 1 & \alpha^3 \end{pmatrix}.$$

Note that $\phi_2^{\phi_1} = \phi_2^{-1}$.

The unique complete arc of size 12 with $\Gamma_S \approx 3^2 : Q_8$ and $G_S \approx 3^2 : 4$ and the unique complete arc of size 12 with $\Gamma_S \approx 3^2 : D_{12}$ and $G_S \approx 3^2 : 6$

In $\mathrm{PG}(2,9)$, the nine points

$$\begin{array}{ccc} (1,0,1) & (0,1,1) & (1,1,-1) \\ (1,-1,1) & (0,0,1) & (-1,1,1) \\ (1,1,1) & (0,1,-1) & (1,0,-1) \end{array} \tag{7.5}$$

together with the points $(1,-1,0)$, $(0,1,0)$, $(1,0,0)$ and $(1,1,0)$ on the line $z = 0$ form a projective subplane $\mathrm{PG}(2,3)$. The other six points on the line $z = 0$ are the points $(1,t,0)$ with $t \in \{\alpha, \alpha^2, \alpha^3, \alpha^5, \alpha^6, \alpha^7\}$. The union of any three of these six points together with the nine points of (7.5) is a $(k,3)$-arc that always turns out to be complete. Among these arcs we find two orbits.

The first orbit consists of 12 isomorphic arcs having $\Gamma_S \approx 3^2 : Q_8$ and $G_S \approx 3^2 : 4$ as group of automorphisms. A representative S of this orbit consists of the points of (7.5) and the three points $(1,\alpha,0)$, $(1,\alpha^5,0)$ and $(1,\alpha^7,0)$.

The second orbit consists of 8 isomorphic arcs with $\Gamma_S \approx 3^2 : D_{12}$ and $G_S \approx 3^2 : 6$. A representative S' of this orbit consists of the points of (7.5) and the three points $(1, \alpha, 0)$, $(1, \alpha^6, 0)$ and $(1, \alpha^7, 0)$.

The group 3^2 can be generated by the following linear transformations:

$$\begin{aligned}\phi_{\pm 1} &: (x, y, z) \mapsto \quad (x \pm z, y, z),\\ \phi_{\pm 2} &: (x, y, z) \mapsto \quad (x, y \pm z, z),\\ \phi_{\pm 3} &: (x, y, z) \mapsto (x \pm z, y \pm z, z),\end{aligned}$$

The group $G_S \approx 3^2 : 4$ of the arc S is then obtained by adding the element

$$i : (x, y, z) \mapsto (-x + y, x + y, z)$$

of order 4. The group Q_8 can be generated by the following elements:

$$\begin{aligned}\pm 1 &: (x, y, z) \mapsto \quad (x, y, \pm z),\\ \pm i &: (x, y, z) \mapsto \quad (-x + y, x + y, \pm z),\\ \pm j &: (x, y, z) \mapsto \quad (-y^3, x^3, \pm z),\\ \pm k &: (x, y, z) \mapsto (-x^3 - y^3, -x^3 + y^3, \pm z^3)\end{aligned}$$

such that $i^2 = j^2 = k^2 = ijk = -1$. Note that the subgroup 3^2 is left invariant under conjugation by Q_8 and therefore Γ_S is of type $3^2 : Q_8$.

The group $G_{S'} \approx 3^2 : 6$ can be generated by the elements $\phi_{\pm 1}, \phi_{\pm 2}, \phi_{\pm 3}$ together with

$$\psi_6 : (x, y, z) \mapsto (-x, x - y, z).$$

of order 6. The group D_{12} can be generated by ψ_6 and

$$\psi_2 : (x, y, z) \mapsto (x^3, -y^3, z^3)$$

of order 2 with $\psi_6^{\psi_2} = \psi_6^{-1}$. Note that the subgroup 3^2 is left invariant under conjugation by D_{12} and therefore Γ_S is of type $3^2 : D_{12}$.

The unique complete arc of size 16 with $\Gamma_S \approx (3:4):2$ and $G_S \approx 3:4$

The points of this arc are the 16 rational points of a non-singular irreducible cubic curve with equation $yz^2 + \alpha^2 y^3 + x^3 - xy^2 = 0$. This cubic is of type (ii)b, as classified in [19, Theorem 11.54] and is the cubic with the largest number of points in PG$(2,9)$. The automorphism group G_S of this arc is isomorphic to the semi-direct product $3:4$ and can be generated by

$$\phi_1 : (x,y,z) \mapsto (x+y,y,z)$$

and

$$\phi_2 : (x,y,z) \mapsto (x-\alpha^2 y, -y, \alpha^2 z).$$

Note that $\phi_1^3 = \phi_2^4 = 1$ and $\phi_1^{\phi_2} = \phi_1^{-1}$. To obtain Γ_S we need to add the automorphism

$$\phi_3 : (x,y,z) \mapsto (x^3, -y^3, \alpha^2 z^3)$$

of order 2. We have $\phi_1^{\phi_3} = \phi_1$ and $\phi_2^{\phi_3} = \phi_2^2$.

7.7 Special (k,3)-arcs for $q = 11$

The unique complete arc of size 19 with $G_S \approx 19:3$

There is a unique complete arc of size 19 with $G_S \approx 19:3$ which can be constructed as an orbit of the 19th power of a Singer cycle (cf. Section 6.1).

Note that this arc is regular: through each point there are 0 bisecants, and hence 9 trisecants and 3 unisecants.

The 2 complete arcs of size 21 with $G_S \approx 7:3$

These two arcs each consists of the union of three orbits of size 7 of the 19th power of a Singer cycle (cf. Section6.1). The automorphism group of both arcs

is the group $7:3$.

Note that again the arcs are regular: in both cases each point of the arc lies on 9 trisecants, and hence 2 bisecants and 1 unisecant.

The complete arcs with $G_S \approx S_4$

When applying Theorem 7.1 to $q = 11$, we find that $S^*(a) \cup S^*(\infty)$ is an arc for all values of a, except for the values 0 and ± 1 (as -1 is non-square in $\mathbb{F}_{11}$). This arc is only complete for 4 of these values, i.e. when $a = \pm 4$ or $a = \pm 5$. (Note that $S^*(a) = S^*(-a)$.) This results in two inequivalent complete arcs of size 15 both having S_4 as automorphism group. These arcs are regular: each point lies on 6 trisecants, 2 bisecants and 4 unisecants.

Also according to Theorem 7.1, the values $a = \pm 3$ are the only ones for which $S^*(a) \cup S^*(0)$ is an arc in $\mathrm{PG}(2, 11)$. This arc is complete and has again S_4 as automorphism group. In this case, the set $S^*(a)$ is a complete $(k, 2)$-arc. The twelve points of $S^*(a)$ each lie on 5 trisecants, 7 bisecants and 0 unisecants. The six points of $S^*(0)$ each lie on 7 trisecants, 3 bisecants and 2 unisecants.

The complete arcs with $G_S \approx D_{10}$

As mentioned in Section 7.2, $\mathrm{PG}(2, 11)$ contains six complete arcs up to isomorphism that have the dihedral group of order 10 as group of automorphisms.

When using the same notations as in Section 7.2, we find the following com-

plete $(k,3)$-arcs up to isomorphism:

$$\begin{aligned}
S_{13} &= C_1^+ \cup C_3^+ \cup \{P,Q,R\} \\
S_{15} &= C_1^+ \cup C_4^+ \cup C_9^+ \\
S'_{15} &= C_1^+ \cup C_4^+ \cup C_5^+ \\
S_{17} &= C_1^+ \cup C_1^- \cup C_9^+ \cup \{P,Q\} \\
S'_{17} &= C_1^+ \cup C_1^- \cup C_5^+ \cup \{P,Q\} \\
S''_{17} &= C_1^+ \cup C_4^+ \cup C_9^- \cup \{P,Q\}
\end{aligned}$$

Because all indices that appear are squares in $\mathbb{F}_{11}$, the group D_{12} is generated by the transformations ϕ_1 and ϕ_2 as defined in Section 7.2.

The complete arcs with $G_S \approx 5$

There are 6 complete arcs in PG$(2,11)$ with a cyclic automorphism group of order 5. Each of these contain 3 'half' conics as defined in Section 7.2. These arcs are the following (using the same notations):

$$\begin{aligned}
S_{17} &= C_1^+ \cup C_2^+ \cup C_3^+ \cup \{P,R\} \\
S'_{17} &= C_1^+ \cup C_2^+ \cup C_4^+ \cup \{P,R\} \\
S''_{17} &= C_1^+ \cup C_2^+ \cup C_{10}^+ \cup \{P,R\} \\
S''_{17} &= C_1^+ \cup C_4^+ \cup C_7^+ \cup \{P,R\} \\
S'''_{17} &= C_1^+ \cup C_8^+ \cup C_9^+ \cup \{P,R\} \\
S_{18} &= C_1^+ \cup C_2^+ \cup C_{10}^- \cup \{P,Q,R\}
\end{aligned}$$

7.8 Special (k,3)-arcs for $q = 13$

The unique complete arc of size 18 with $G_S \approx S_4$

Applying Theorem 7.1 to $q = 13$ yields the values $a = \pm 3, \pm 4, \pm 6$ for which $S^*(a) \cup S^*(0)$ is an arc. Only for $a = \pm 6$ this arc turns out to be complete and has S_4 as automorphism group.

This arc is regular: each point lies on 7 trisecants, 3 bisecants and 4 unisecants.

The complete arcs of size 21 with $G_S \approx D_{12}$

PG$(2, 13)$ contains two complete arcs having the dihedral group of order 12 as group of automorphisms. Both arcs consist of the same three 'half' conics as defined in Section 7.2, together with three points. Using the same notations we find

$$\begin{aligned} S &= C_1^+ \cup C_1^- \cup C_7^+ \cup \{P, Q, R\} \\ S' &= C_1^+ \cup C_1^- \cup C_7^+ \cup \{(1,0,7), (1,0,8), (1,0,9)\} \end{aligned}$$

Because 7 is a non-square in $\mathbb{F}_{13}$, the group D_{12} is generated by ϕ_1 and ϕ_3 as defined in Section 7.2.

The complete arcs of size 20 with $G_S \approx 6$

The arcs constructed in Section 7.2 can be completed in many ways. Adding the points $P(1,0,0)$ and $R(0,1,0)$ to each one of the arcs yields three complete and one incomplete arc. The incomplete arc is the one discussed above to which the point $Q(0,0,1)$ can be added as well. The other three arcs are the

following (using the notations of Section 7.2:

$$\begin{aligned} S_{20} &= C_1^+ \cup C_2^+ \cup C_4^+ \cup \{P,R\} \\ S'_{20} &= C_1^+ \cup C_2^+ \cup C_{11}^+ \cup \{P,R\} \\ S''_{20} &= C_1^+ \cup C_4^+ \cup C_6^+ \cup \{P,R\}. \end{aligned}$$

These three arcs all have a cyclic automorphism group of order 6.

Arcs related to the Hessian configuration

Because $13 \equiv 1 \pmod 3$, the arcs defined in Section 7.3.1 exist in $\mathrm{PG}(2,13)$. The set $\hat{\mathcal{H}} = \mathcal{H} \cup \mathcal{H}_1$ is a complete $(18,3)$-arc for $q = 13$. Its group of automorphisms has size 36: it can be obtained by extending G_{18} with the following generator, of order 4 :

$$(x\ y\ z) \mapsto (x\ y\ z) \begin{pmatrix} 1 & 1 & 9 \\ 9 & 1 & 1 \\ 9 & 3 & 9 \end{pmatrix}$$

The $(15,3)$-arc $\mathcal{H}_1 \cup S_\omega$ also is complete for $q = 13$ and has the same group of automorphisms of size 36 as $\hat{\mathcal{H}}$.

The unique complete arc of size 18 with $G_S \approx 3_+^{1+2}$

For $q = 13$ and $c = -2$, the $(18,3)$-arc $S_1 \cup S_2(-2)$ as defined in Section 7.3.2 is complete with 3_+^{1+2} as group of automorphisms.

Cubic curves of size 21

The largest size of a cubic curve in $\mathrm{PG}(2,13)$ turns out to be 21, with two examples up to isomorphism.

The first example corresponds to the following equation

$$xy(x+y) = -6z^3.$$

This is an irreducible cubic curve with three inflection points (coordinates: (1,0,0), (0,1,0), (1,-1,0)) and three inflectional tangents that are concurrent ($x = 0$, $y = 0$ and $x + y = 0$, intersecting in $(0,0,1)$.)

The automorphism group G of this curve has size 18, is of type $3S_3$ and is generated by the permutations of x, y and $-x-y$ and the cyclic element $z \mapsto 3z$ (with $3^3 = 1$).

Apart from the three inflection points, the curve has 18 additional points, which form an orbit of G. The points are those whose coordinates (x, y, z) satisfy $\{x, y, -x-y\} = \{1, 2, -3\}$ and $z^3 = 1$.

The points $P_0, \ldots, P_{20}$ of this curve can be numbered in a way that reflects the Abelian group of the curve (which is cyclic of order 21) :

$$\begin{array}{llllll} P_0: & (1,0,0) & P_7: & (0,1,0) & P_{14}: & (1,-1,0) \\ P_1: & (1,2,1) & P_8: & (2,-3,1) & P_{15}: & (-3,1,1) \\ P_2: & (6,4,1) & P_9: & (4,3,1) & P_{16}: & (3,6,1) \\ P_3: & (5,-4,1) & P_{10}: & (-4,-1,1) & P_{17}: & (-1,5,1) \\ P_4: & (-4,5,1) & P_{11}: & (5,-1,1) & P_{18}: & (-1,-4,1) \\ P_5: & (4,6,1) & P_{12}: & (6,3,1) & P_{19}: & (3,4,1) \\ P_6: & (2,1,1) & P_{13}: & (1,-3,1) & P_{20}: & (-3,2,1) \end{array} \tag{7.6}$$

P_i, P_j, P_k are collinear if and only if $i + j + k \equiv 0 \pmod{21}$.

The automorphism group G can also be easily expressed in terms of this point numbering: the cyclic permutation $(x, y, z) \mapsto (y, -x-y, z)$ is equivalent to $P_i \mapsto P_{i+7}$, $P_i \mapsto P_{-i}$ interchanges x and $-x-y$, and $P_i \mapsto P_{4i}$ corresponds to $z \mapsto 3z$ (each time with index aritmetic modulo 21).

The automorphism group has two orbits of size 3 in the plane. A first orbit consists of the inflection points P_0 ,P_7 and P_{14}, the second orbit corresponds to the points with coordinates $(1,1,0)$, $(-2,1,0)$ and $(1,-2,0)$. Both orbits lie on the line with equation $z = 0$.

These six points have an important property: every line through these points, except the line $z = 0$, intersects the orbit of 18 non-inflection points in at most two points.

For the first orbit this is an immediate consequence of the fact that all 21 points lie on an irreducible cubic curve. For the second orbit, consider the representative point $(1,1,0)$. From (7.6) we compute the values of $(y-x)/z$ for each point P_i that is not an inflection point.

P_i	P_1	P_2	P_3	P_4	P_5	P_6
$(y-x)/z$	1	-2	4	-4	2	-1
P_i	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}
$(y-x)/z$	-5	-1	3	-6	-3	-4
P_i	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}
$(y-x)/z$	4	3	6	-3	1	5

The number of times a specific value k occurs in this table, is equal to the number of intersection points with the line $x - y + kz = 0$ through $(1,1,0)$. For $k = \pm 2, \pm 5, \pm 6$ there is one intersection point, for $k = \pm 1, \pm 3, \pm 4$ there are two, but never three. This proves our claim.

From this we conclude that adding any three of these six points to the 18 non-inflection points of the cubic yields a (21,3)-arc, giving a total of 6 non-equivalent (21,3)-arcs for $q = 13$. These arcs turn out to be complete. Only two of them have G as group of automorphisms. (The others have a cyclic automorphism group of order 3 or 6.)

The second example of a cubic curve of size 21 corresponds to the curve C_{21} with equation

$$x^2y + y^2z + 4z^2x = 0.$$

This cubic has no inflection points. Its automorphism group is the group 3^2 of size 9 and is generated by the transformations

$$(x,y,z) \mapsto (x,3y,9z), \quad (x,y,z) \mapsto (y,4z,x).$$

The group has one orbit of size 3, with points $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$, and 20 orbits of size 9 (on the points of $\mathrm{PG}(2,13)$). The cubic C_{21} consists of

the orbit of size 3 and two orbits of size 9, with representatives $(1,-1,-2)$ and $(1,-1,5)$. It is a complete $(21,3)$-arc.

Finally, it turns out that the same group leaves invariant a different (21,3)-arc which does not lie on a cubic. It consists of the orbit of size 3 together with the two orbits of size 9 with representatives $(1,1,2)$ and $(1,1,6)$.

Regular arcs for $q = 13$

From Section 5.5 we know that $\mathrm{PG}(2,13)$ contains several $(k,3)$-arcs that are regular. We shall only discuss those of size 21.

The first (21,3)-arc of this type has automorphism group of type S_3. Each point lies on 8 trisecants (and 4 bisecants and 2 unisecants). The points of this arc can be given by the following coordinates

$$\begin{array}{cccccc} (1,-1,3) & (1,3,-1) & (-1,1,3) & (-1,3,1) & (3,1,-1) & (3,-1,1) \\ & (0,1,1) & (1,0,1) & (1,1,0) & & \\ & (1,1,4) & (1,4,1) & (4,1,1) & & \\ (1,2,5) & (1,5,2) & (2,1,5) & (2,5,1) & (5,1,2) & (5,2,1) \\ & (1,0,0) & (0,1,0) & (0,0,1) & & \end{array} \tag{7.7}$$

The group S_3 acts by permuting the coordinates. The first three rows of (7.7) form a (12,2)-arc consisting of all points of the conic $2(x^2+y^2+z^2) = (x+y+z)^2$ except those on the line $x+y+z=0$, i.e., $(1,3,9)$ and $(1,9,3)$.

The second regular $(21,3)$-arc has a cyclic automorphism group of size 3. Each point lies on 9 trisecants, 2 bisecants and 3 unisecants. The points of this arc can be given by the following coordinates.

$$\begin{array}{ccccccc} (1,0,0) & (1,2,2) & (1,0,2) & (1,2,4) & (1,-2,-4) & (1,4,3) & (1,5,3) \\ (0,0,1) & (2,-5,1) & (0,-5,1) & (2,3,1) & (-2,-3,1) & (4,-1,1) & (5,-1,1) \\ (0,1,0) & (-5,4,2) & (-5,4,0) & (3,4,2) & (-3,4,-2) & (-1,4,4) & (-1,4,5) \end{array} \tag{7.8}$$

The automorphism group is generated by the transformation $(x,y,z) \mapsto (y,4z,x)$ which we encountered before, and cyclically permutes the rows of (7.8).

The third and fourth $(21,3)$-arc of this type are the two arcs discussed in the following section.

The unique regular complete arc of size 21 with $G_S \approx D_{14}$

For $q = 13$, there is one complete arc having the dihedral group of order 14 as automorphism group. Let C_1 be the conic with equation $x^2 + z^2 + 6xy + 6yz + 11xz = 0$ and C_2 the conic with equation $xz = y^2$. Then the arc consists of all points of C_1 together with the points of C_2 with coordinates $(1, t, t^2)$ with t one of the elements in the following list:

$$5, 2, 3, 1, 9, 7, 8 \tag{7.9}$$

The points of C_1 have the following coordinates:

$$(1,5,2), (1,1,5), (1,2,0), (0,1,0), (0,1,7), (1,8,8), (1,9,7) \tag{7.10}$$

$$(1,5,9), (1,8,11), (1,1,4), (1,0,1), (1,10,10), (1,9,6), (1,2,3) \tag{7.11}$$

The automorphism group can be generated by

$$\phi_1 : (x, y, z) \mapsto (z, 12y + 10z, x + 6y + 9z)$$

of order 7 and

$$\phi_2 : (x, y, z) \mapsto (z, y, x)$$

of order 2. For the arc points on C_2 ϕ_1 corresponds to $t \mapsto 12/t + 10$ and ϕ_2 to $t \mapsto 1/t$. The order of the points listed in (7.9), (7.10) and (7.11) corresponds to consecutive applications of ϕ_1. This order is reversed by ϕ_2. We have $\phi_1^{\phi_2} = \phi_1^{-1}$.

8

Generation of $(k, 2)$-arcs from conical subsets

In this chapter we describe a second algorithm that generates all complete $(k, 2)$-arcs in $\mathrm{PG}(2, q)$ up to equivalence. As in Chapter 4, this algorithm makes use of the principle of canonical augmentation. However, generation is now started from conical subsets instead of from single points. Although this algorithm seemed promising, it did not give us new results as it runs too slow to even reach $q = 27$. However, it reproduces our results for all $q \leq 25$ and hence confirms the correctness of our programs.

8.1 Isomorph-free generation from conical subsets

In order to verify the results of the generation of $(k, 2)$-arcs described in the previous chapters, we developped an algorithm that is totally independent to that of Chapter 4. Not only did we want to reproduce our results, we also hoped to find the classification of all complete $(k, 2)$-arcs in $\mathrm{PG}(2, 31)$.

8.1.1 Canonical augmentation

Where the algorithm for generating arcs in Chapter 4 starts from a singleton S and adds points to S at each step of the recursion, this algorithm starts the generation from the largest conical subsets of the resulting arcs. Note that each subset of size five of an arc is a conical subset since a conic is determined by five points. Hence, the set of conical subsets to start the generation from can be restricted to only those of size at least five.

Let $\mathcal{E}$ denote the set of all subsets of size at least 5 of all conics of $\mathrm{PG}(2, q)$. Then we denote with $\mathcal{E}(\mathcal{S})$ the set of all conical subsets of size at least five of a $(k, 2)$-arc S. Note that $\mathcal{E}(\mathcal{S}) \subseteq \mathcal{E}$ for every $(k, 2)$-arc S.

The idea is to first generate all possible subsets of conics of size at least 5 up to equivalence. Then, for each such set T we recursively add points to it in all possible ways until a complete arc S is obtained, which has T as a conical subset.

To ensure uniqueness up to equivalence, only those arcs S are retained for which the original conical subset T is *maximal* among all conical subsets of S, according to some specific ordering. This ordering is derived from a more general ordering on all equivalence classes of subsets of conics in the plane, and shall be explained in more detail later. Note that maximality of T is defined only up to the action of the stabilizergroup G_S of S. In other words, if T is maximal, and $g \in G_S$, then also T^g is maximal. The G_S-orbit of all 'maximal' conical subsets of S shall be denoted by $F(S)$. A precise definition of F will be given in section 8.1.4. To make the algorithm work, the function

F must satisfy the following properties:

1. For all S, $S \subseteq V$, $|S| \geq 5$, we have $F(S) \neq \emptyset$, $F(S) \subseteq \mathcal{E}(\mathcal{S})$,
2. For all S, $S \subseteq V$, $|S| \geq 5$, we have $F(S) \in G_S \backslash\backslash \mathcal{E}(\mathcal{S})$,
3. For all S, $S \subseteq V$, $g \in G$, we have $F(S^g) = F(S)^g$.

Note that property 2 and 3 are analogous to the required properties of the function F in Section 4.1.1.

8.1.2 The algorithm

Consider the following algorithm.

Algorithm 3 Generation From Conical Subsets

Output: $\mathcal{A}_{\text{out}} \subseteq G \backslash\backslash 2^V$
1: $\mathcal{A}_{\text{out}} = \emptyset$
2: **for all** $\mathcal{O} \in G \backslash\backslash \mathcal{E}$ **do**
3: Choose $T \in \mathcal{O}$ ❶
4: $\mathcal{B} = \emptyset$
5: **for all** complete arcs $S \in 2^V$ such that $T \subseteq S$ **do**
6: **if** $T \in F(S)$ **then**
7: Add S^G to $\mathcal{B}$ ❷
8: **end if**
9: **end for**
10: Add $\mathcal{B}$ to $\mathcal{A}_{\text{out}}$
11: **end for**

Note that it is very similar to that of Chapter 4. Again, $\mathcal{B}$ is a true set. It may happen that the same orbit is added more than once to $\mathcal{B}$ in ❷. To decide whether two arcs belong to the same orbit of G in ❷, one can use any canonical form for $(k, 2)$-arcs. We used the same canonical form as defined in Section 4.3.

For the algorithm to be well-defined, the set $\mathcal{E}$ must be group invariant for the group G, which is indeed the case. Also, the resulting set $\mathcal{A}_{\text{out}}$ must be independent of the choice of the orbit representative made at statement ❶. This is true because if we choose another set $T' \in \mathcal{O}$, then, due to the third property of F, for each arc S with $T \in F(S)$ we find an arc S' with $T' \in F(S')$ such that S and S' are part of the same orbit S^G of G .

Analogously to the proofs of Lemma 4.5 and 4.6, one can prove that the result of Algorithm 3 is the set $\mathcal{A}_{\text{out}}$ of all G-orbits of complete $(k,2)$-arcs of size at least 5 and that every orbit S^G is added to at most one $\mathcal{B}$ in ❷ and hence is added to $\mathcal{A}_{\text{out}}$ at most once.

8.1.3 The line canonical form of a conical subset

To be able to define an ordering on conical subsets in $\mathrm{PG}(2,q)$, we define some kind of a canonical form for conical subsets. As all conics are equivalent under the action of $G = \mathrm{PGL}(3,q)$ and can be identified with the projective line $\mathrm{PG}(1,q)$, with every conical subset we may associate a subset of $\mathrm{PG}(1,q)$. For that reason, we first define a canonical form for subsets L of the projective line.

We fix an ordering on the points of the line and extend this to a lexical ordering of subsets of points of equal size. We define the canonical form $\mathrm{can}(L)$ of a subset L of $\mathrm{PG}(1,q)$ to be the smallest subset in the orbit L^H, $H = \mathrm{PGL}(2,q)$ with respect to this lexical ordering.

We now define the *line canonical form* $\mathrm{lcan}(T)$ of a conical subset T to be the canonical form of the corresponding subset L on the projective line.

Although the line canonical form of a conical subset T is not part of the orbit T^G, $G = \mathrm{PGL}(3,q)$, it is an invariant for G of this conical subset and it satisfies the second property of a canonical form (cf. Section 4.2.2): two conical subsets having the same line canonical form are part of the same orbit in $G\backslash\backslash\mathcal{E}$ and conversely.

We define the following ordering on subsets of the projective line: we first order them according to size and in case of equal size, we order them lexically according to their canonical form. The elements of $G\backslash\backslash\mathcal{E}$ can then be ordered lexically according to their line canonical form.

8.1.4 The function F

The function F used in the algorithm has to determine whether a given conical subset of an arc is *maximal* or not.

To define a function F we cannot directly use the line canonical form of conical subsets. The line canonical form is an invariant of the group G, while we need $F(S)$ to be an orbit of G_S. Therefore, we denote a set of all conical subsets of S having the same line canonical form as a *quasi-orbit* of G_S on $\mathcal{E}(\mathcal{S})$. Each quasi-orbit then is the union of orbits of G_S on $\mathcal{E}(\mathcal{S})$. Note that every singleton quasi-orbit of G_S is of course a true orbit of G_S.

Let $F'(S) = \{T_1, \ldots, T_m\}$ be the quasi-orbit of all conical subsets T_i of the arc S whose line canonical forms are maximal among all conical subsets of S (in the sense that their size is largest and in case of equal size their line canonical form is lexically largest). (Note that $T_1, \ldots, T_m$ all have the same line canonical form.) We can now define the function F as follows:

1. If $F'(S)$ is a singleton, then $F(S) = F'(S)$.
2. Otherwise, if $h \in G$ such that $S^h = \text{can}(S)$, then we define $F(S)$ to be the orbit $T_l^{G_S}$, where T_l^h is lexically smallest among all images T_i^h of all $T_i \in F'(S), i = 1, \ldots, m$. (If $F'(S)$ is exactly one orbit of G_S, then $F(S) = F'(S)$.)

Note that with these definitions, the funtion F satisfies the needed properties for Algorithm 3. To prove this we first need the following lemma:

Lemma 8.1 *For all $S \subseteq V$, $g \in G$, we have $F'(S)^g = F'(S^g)$.*

Proof : The line canonical form of a conical subset is an invariant for the group G. Hence, the set of all conical subsets of S with maximal line canonical form will not change under the action of an element $g \in G$ ∎

Proposition 8.2 *Let $F(S)$ be defined as above. Then,*

1. *For all S, $S \subseteq V$, $|S| \geq 5$, we have $F(S) \neq \emptyset$, $F(S) \subseteq \mathcal{E}(\mathcal{S})$,*
2. *For all S, $S \subseteq V$, $|S| \geq 5$, $F(S)$ is an orbit of G_S on S;*
3. *For all S, $S \subseteq V$, $g \in G$, we have $F(S^g) = F(S)^g$.*

Proof : 1. This follows immediately from the definitions of F' and F.

2. By definition, $F'(S)$ is the union of orbits of $G_S \backslash\backslash \mathcal{E}(\mathcal{S})$, so in the first case $F(S)$ is indeed a single orbit of $G_S \backslash\backslash \mathcal{E}(\mathcal{S})$. In the second case, F(S) is of the from $T_l^{G_S}$ which is a G_S-orbit of T_l and $T_l \in \mathcal{E}(\mathcal{S})$, so here F(S) is also a single orbit of $G_S \backslash\backslash \mathcal{E}(\mathcal{S})$.

3. Because of Lemma 8.1, either both $F'(S)$ and $F'(S^g)$ are singletons or neither. Hence $F(s)$ and $F(S^g)$ either both satisfy the conditions of the first part of the definition of F, or neither do.

In the first case, when $F'(S)$ and $F'(S^g)$ are singletons, the proof follows immediately.

In the second case, S and S^g are part of the same orbit of G and hence have the same canonical form $\mathrm{can}(S) = \mathrm{can}(S^g)$. So, if $S^h = \mathrm{can}(S)$ for some $h \in G$, then $\mathrm{can}(S^g) = (S^g)^{g^{-1}h}$. Because of Lemma 8.1, $F'(S)^h = F'(S^h) = F'(\mathrm{can}(S))$ and $F'(S^g)^{g^{-1}h} = F'(S^h) = F'(\mathrm{can}(S))$.

Assume T is lexically smallest among all conical subsets of $F'(\text{can}(S))$. Then $F(S) = T^{h^{-1}G_S}$ and $F(S^g) = T^{(g^{-1}h)^{-1}G_{Sg}} = T^{h^{-1}gG_S^g}$ using $G_{Sg} = (G_S)^g$. As $F(S)^g = (T^{h^{-1}G_S})^g = T^{h^{-1}gG_S^g}$, we find $F(S)^g = F(S^g)$. ∎

8.2 Improvements

In practice, to generate the complete arcs S in line 5 of Algorithm 3 we use a recursive algorithm adding one point at each step of the recursion. To avoid generating the same arcs from the same set T several times, we number the points of the plane and only add a point to an arc S if its number is larger then the points in $S \setminus T$. (See line 10 and 24 in GENERATE of Algorithm 4.)

Algorithm 4 Generation From Conical Subsets

Output: $\mathcal{A}_{\text{out}} \subseteq G\backslash\backslash 2^V$
1: $\mathcal{A}_{\text{out}} = \emptyset$
2: **for all** $\mathcal{O} \in G\backslash\backslash\mathcal{E}$ **do**
3: Choose $T \in \mathcal{O}$ ❶
4: $\mathcal{B} = \emptyset$
5: GENERATE $(0, \mathcal{B}, T)$
6: Add $\mathcal{B}$ to $\mathcal{A}_{\text{out}}$
7: **end for**

The definition of the function F can help us improve the speed of the algorithm. Indeed, a complete arc S will only be kept if the original conical subset T from which the generation was started, is an element of $F(S)$. From the definition of F, we know that such a conical subset is maximal in size among all conical subsets of the resulting arc T. Hence, when we find a conical subset that is larger than the starting one during generation, then the further generation from the current arc is stopped. An analogous procedure can be followed when during generation a conical subset is met that has equal size but has a larger line canonical form than the conical subset T from which the generation was started. (See line 17 in GENERATE of Algorithm 4.)

However, in the first steps of the recursion, we do not need to compute all

Algorithm 4 Generation From Conical Subsets (continued)

```
 8: procedure GENERATE(start, B, T)
 9:     S ← T
10:     for i ← start to q^2 + q + 1 do
11:         if s_i ∉ S then
12:             S ← S ∪ {s_i}
13:             larger ← false
14:             if |S| ≥ 2|T| − 4 then
15:                 T ← all conical subsets of S containing s_i
16:                 for all conical subsets T' in T do
17:                     if |T'| > |T| or (|T'| = |T| and lcan(T') > lcan(T)) then
18:                         larger ← true
19:                         go to 23
20:                     end if
21:                 end for
22:             end if
23:             if not(larger) then
24:                 GENERATE (i + 1, B, S)
25:             end if
26:         end if
27:     end for
28: end procedure
```

conical subsets of the current arc S: if $|S| < 2|T| - 4$ with T the conical subset from which the generation was started, then each conical subset of size at least $|T|$ of S must contain at least 5 points of T and hence is equal to T as a conic is uniquely determined by 5 points. Hence, the arc S cannot contain conical subsets that are greater than T with respect to the ordering of conical subsets as defined in Section 8.1.3. (See line 14 in GENERATE of Algorithm 4.)

Also when computing all conical subsets of S, we only need to compute those ones containing the last added point s_i. Indeed, a conical subset not containing s_i and greater then T would already have stopped the generation in a previous step of the recursion. (See line 15 in GENERATE of Algorithm 4.)

8.3 Remarks

Generation of the set $\mathcal{E}$

In Algorithm 3, only one conical subset in each orbit $\mathcal{O}$ of $G\backslash\backslash\mathcal{E}$ is needed. Hence, in practice we do not need to generate the full set $\mathcal{E}$ of conical subsets: only one representative for each orbit in $\mathcal{E}$ is sufficient. As all conics are equivalent under the action of $G = \mathrm{PGL}(2, q)$ and can be identified with the projective line, we can even restrict ourselves to the orbits of the projective line.

To generate all subsets of $\mathrm{PG}(1, q)$ up to equivalence, we use essentially the same algorithms as those of Chapter 4 but with a trivial predicate P and the following definition of F.

> $F(S) \stackrel{\text{def}}{=} e^{hG_S}$ where $h \in G$ is such that $S = \mathrm{can}(S)^h$ and e is the smallest point in $\mathrm{can}(S)$,

where "the smallest point" is the smallest point in the ordering as chosen in Section 8.1.3 to define the canonical form of a line subset.

Mapping the points with coordinates $(1, t)$ of PG$(1, q)$ onto the points with coordinates $(1, t, t^2)$ in PG$(2, q)$ then yields the conical subsets corresponding with the generated line subsets.

Some more improvements

Apart from the ones described above, we added some further improvements which are not included in the pseudocode in Algorithm 4:

During generation, we want the original set T to stay maximal among all conical subsets. Hence, when a conical subset T' of equal size is found, we ensure that no other point of the corresponding conic of T' will be added to the arc in a next step of the recursion. For this, we keep track of these so called "forbidden" points at each level of the recursion.

Another an improvement is the following: we order the set of the line canoncical forms and give the conical subsets a *canonical index* corresponding to this ordering. During the algorithm, we keep track of these indices instead of the line canonical form of the conical subsets itselfs. In this way, we need less memory space and comparing indices is faster than comparing conical subsets. We also compute the list of possible *child indices* of each conical subset. A child index of a conical subset T is the canonical index of a set $T \cup p, p \in C$ in which C is the conic corresponding to the conical subset. This allows us in advance to forbid points that would yield and arc with a conical subset that is equal in size but larger in line canonical form.

Results

As explained in Section 8.2, we tried to make the basic Algorithm 3 more efficient in order to improve speed. With those adaptations, we managed to compute the complete arcs in PG$(2, q)$, $q \leq 25$. However, for $q > 25$ our program is too slow. Yet, the results for $q \leq 25$ are exactly the same as our results described Section 5 and hence this program confirms the correctness of our previous program.

Nederlandstalige samenvatting

In dit werk hebben we ons toegespitst op het vinden van alle complete $(k,2)$- en $(k,3)$-bogen in Desarguesiaanse projectieve vlakken $\mathrm{PG}(2,q)$ op equivalentie na.

We herhalen kort enkele definities.

Een (k,n)-*boog* S in $\mathrm{PG}(2,q)$ is een verzameling van k punten in het vlak zodat minstens één rechte van het vlak S snijdt in n punten, maar zodat geen enkele rechte de verzameling S snijdt in meer dan n punten. Een (k,n)-boog is *compleet* als en slechts als deze niet bevat is in een $(k+1,n)$-boog. In het geval van $(k,3)$-bogen laten we vaak stilzwijgend de eis vallen dat minstens één rechte 3 punten van de boog moet bevatten (vooral in Hoofdstuk 4 waar het algoritme wordt besproken). Dit betekent dat we een $(k,2)$-boog soms als een speciaal geval van een $(k,3)$-boog beschouwen. Bij complete $(k,3)$-bogen vormt dit geen probleem aangezien een $(k,2)$-boog nooit een complete $(k,3)$-boog kan zijn.

In deze tekst verwijst de term "boog" altijd naar een $(k,2)$- of $(k,3)$-boog. Uit de context zal altijd blijken welke van de twee bedoeld wordt.

In het eerste hoofdstuk hebben we ons geconcentreerd op $(k,2)$-bogen met grote conische deelverzamelingen. Een *conische deelverzameling* van een $(k,2)$-boog S is elke deelverzameling T van S van de vorm $T = S \cap C$, waarbij C een kegelsnede in het vlak is.

Als q oneven is, dan kan een boog hoogstens $q+1$ punten bevatten. In dat

geval valt de boog samen met de verzameling punten van een kegelsnede C. Zo'n boog bestaat altijd en het ligt dus voor de hand om na te gaan wat de volgende mogelijke grootte is van een complete boog in $\mathrm{PG}(2,q)$. Door het verwijderen van enkele punten van een kegelsnede C bekomt met een boog die niet meer compleet is. Als men nu een voldoende aantal punten verwijdert, dan is het mogelijk om de bekomen verzameling uit te breiden met punten die niet op de kegelsnede C liggen totdat men een complete boog bekomt. Als alle punten die niet op de kegelsnede liggen extern zijn ten opzichte van C, dan kan de boog hoogstens $(q+3)/2$ punten van de kegelsnede bevatten. Als minstens 1 boogpunt intern is ten opzichte van C, dan is de grootte van de doorsnede hoogstens $(q+1)/2$. Voor vele waarden van q behoren deze bogen tot de grootste bogen die gekend zijn. Het zijn deze types bogen die we verder onderzocht hebben. We bespreken de bogen met een conische deelverzameling van maximale grootte en 1 extra punt. Ook hebben we een complete classificatie opgesteld voor de bogen met een conische deelverzameling van maximale grootte en 2 extra punten. Hierbij zijn drie gevallen mogelijk: 2 interne punten, 2 externe punten en de combinatie van 1 intern en 1 extern punt. Deze bogen worden respectievelijk bogen van het *type I met excess* 2, bogen van het *type E met excess* 2 en bogen van het *type M met excess* 2 genoemd. Deze bogen zijn niet noodzakelijk compleet. Er zijn echter slechts weinig bogen van deze types gekend die meer dan twee extra punten bevatten. De theoretische classificatie van de bogen van deze types vormen de basis van een snel computerprogramma dat zoekt naar bogen met meer dan twee extra punten. De classificatie en de resultaten van het computerprogramma worden beschreven in Hoofdstuk 3

Voor het vinden van alle complete $(k,2)$- en $(k,3)$-bogen in Desarguesiaanse projectieve vlakken $\mathrm{PG}(2,q)$ hebben we specifieke algoritmes opgesteld. Voor het implementeren van deze algoritmes gebruiken we de programmeertaal Java.

We zijn gestart met het implementeren van de standaardtechniek voor het genereren van complete bogen. Deze methode gebruikt een backtracking-algoritme dat recursief elke $(k+1)$-boog S' genereert uit een k-boog S zodat $S \subseteq S'$. Om te voorkomen dat elke boog meer dan één keer gegenereerd wordt, worden de punten van het vlak genummerd en wordt een punt s alleen toegevoegd aan S als zijn volgnummer groter is dan deze van alle punten

in S. Equivalente bogen worden telkens nadat alle bogen van een bepaalde grootte zijn gevonden, uitgefilterd. Dit algoritme werkt correct maar levert maar resultaten binnen een aanvaardbare tijd als $q \leq 19$. We zijn dan ook op zoek gegaan naar andere en betere algoritmen om k-bogen te genereren.

Een eerste algoritme, dat besproken wordt in Hoofdstuk 4, maakt gebruik van *canonical augmentation*, een techniek voor isomorfvrije generatie ontworpen door B. McKay. Deze algemene techniek hebben we aangepast aan het specifieke geval van het genereren van deelverzamelingen S in projectieve vlakken die voldoen aan een bepaalde eigenschap $P(S)$ waarbij P groepsinvariant en erfelijk is. In onze implementaties van het algoritme beschouwen we voor $P(S)$ het predicaat "S is een $(k,2)$-boog van $\mathrm{PG}(2,q)$" of "S is een $(k,2)$- of $(k,3)$-boog van $\mathrm{PG}(2,q)$", afhankelijk van het feit of we complete $(k,2)$- of $(k,3)$-bogen wensen te genereren. Het algoritme zelf werkt ook voor andere predicaten.

Het basisidee van het algoritme is het gebruik van een functie F die aan twee eigenschappen voldoet. De functie moet een speciale baan bepalen in de verzameling van alle banen van de stabilisatorgroep van de boog S op de punten van S. Bovendien moet de functie F groepsinvariant zijn. Het algoritme werkt dan als volgt: hebben we een boog S van grootte k, dan worden daaruit bogen van grootte $k+1$ gegenereerd door alle overige punten s van het vlak te proberen toe te voegen. Is de nieuwe verzameling $S' = S \cup \{s\}$ ook een boog, dan behouden we deze boog enkel en alleen als het laatst toegevoegde punt s behoort tot de speciale baan $F(S')$ van de nieuwe boog. Om de snelheid van ons programma op te drijven, hebben we zorgvuldig gebruik gemaakt van een speciale functie die invariant is voor de punten van de boog. Het is een functie I_S die aan elk punt van de boog S een geheel getal $I_S(p)$ hecht zodanig dat $I_S(p) = I_S(p')$ als p en p' in dezelfde baan zitten van de statibilisatorgroep van de boog.

Van dit eerste algoritme hebben we twee varianten: de eerste variant maakt telkens gebruik van de stabilisatorgroep van de boog S die we verkrijgen in de loop van het algoritme. De tweede variant gebruikt deze stabilisatorgroep niet, maar vereist extra controles om er zeker van te zijn dat nooit twee isomorfe bogen gegenereerd worden. Beide varianten zijn geprogrammeerd en leveren dezelfde resultaten op. Ze reproduceren alle eerdere, door anderen

gevonden resultaten. Bovendien zijn we er met dit algoritme als eerste in geslaagd om alle complete $(k,2)$-bogen van $\mathrm{PG}(2,25)$, $\mathrm{PG}(2,27)$ en $\mathrm{PG}(2,29)$ en alle complete $(k,3)$-bogen van $\mathrm{PG}(2,11)$ en $\mathrm{PG}(2,13)$ te vinden. Deze resultaten worden voorgesteld aan de hand van tabellen in Hoofdstuk 5.

De meeste bogen met een algemeen gekende contructie hebben een interessante (en vaak ook grote) stabilisatorgroep. Daarom bepaalden we de stabilisatorgroep voor elk van de complete bogen. We bestudeerden een aantal van de bogen met grotere stabilisatorgroep in de hoop die bogen op een elegantere manier te kunnen beschrijven dan enkel aan de hand van een opsomming van de coördinaten van de punten in de boog. In sommige gevallen kunnen bogen ook beschreven worden als speciale deelverzamelingen van kubische krommen of van de unie van twee kegelsneden. Daarom hebben we voor elke $(k,2)$-boog het type van de algebraïsche kromme met de laagste graad bepaald waarop de boog ligt. Voor de $(k,3)$-bogen maakten we een lijst van de bogen die regulier zijn in de zin dat elk punt van de boog op een zelfde aantal trisecanten van de boog ligt.

Bij het bestuderen van de bogen vonden we een aantal algemene constructies van bogen die ook werken voor grotere waarden van q. We vonden constructies van $(k,2)$- en $(k,3)$-bogen die alle gestabiliseerd worden door de symmetrische group S_4 en we vonden constructies van bogen met de alternerende groep A_5 als stabilisatorgroep. Ook beschrijven we bogen bestaande uit de unie van drie halve kegelsnedes en bogen die opgebouwd worden uit deelverzamelingen van kubische krommen. Deze algemene constructies worden beschreven in het begin van Hoofdstuk 6 en Hoofdstuk 7. In het tweede deel van deze hoofdstukken worden voor elke q telkens de bogen uit deze constructies opgesomd en wordt een geometrische beschrijving gegeven van een aantal bijkomende bogen met een grotere stabilisatorgroep.

Een tweede algoritme voor het vinden van alle $(k,2)$-bogen gaat op een totaal andere manier te werk en is gebaseerd op het idee van een conische deelverzameling. Het idee bestaat erin eerst alle mogelijke deelverzamelingen van kegelsnedes van grootte minstens 5 (op equivalentie na) te genereren. Daarna worden aan elke verzameling T recursief punten toegevoegd totdat een complete boog S die T als conische deelverzameling bezit, bereikt is. Om uniciteit op equivalentie na te garanderen, worden bogen enkel en alleen be-

houden als de conische deelverzameling T van waaruit de boog opgebouwd werd, *maximaal* is onder alle conische deelverzamelingen van S. Om het begrip *maximaal* te kunnen definiëren, werd een vaste totale ordening op de equivalentieklassen van deelverzamelingen van kegelsnedes ingevoerd. Dit algoritme wordt besproken in Hoofdstuk 8. Een implementatie van dit algoritme heeft geen resultaten opgeleverd voor grotere waarden van q, het reproduceert wel de eerder gevonden resultaten voor $q \leq 25$.

Dankwoord

Tijdens mijn laatste jaar als student, had ik er nooit over nagedacht om als doctoraatsstudent of assistent aan de ugent te beginnen. Toen op onze proclamatie bleek dat de vakgroep nog dringend op zoek was naar een assistent, waren het Klaas en mijn ouders die me ervan overtuigden om de job aan te nemen. Nu zes jaar later ben ik er blijkbaar toch in geslaagd om een doctoraat af te werken. Dit slagen heb ik aan heel wat mensen te danken.

De persoon die het grootste woordje van dank verdient is vast en zeker mijn promotor. Kris, je hebt uren geduld met mij gehad om heel wat zaken tot herhalens toe in detail uit te leggen en om mij telkens opnieuw door de groepentheorie heen te sleuren. Vele malen stond ik aan je deur met de vraag of ik stoorde, waarop dan steevast het antwoord "Neen, kom maar binnen!" volgde. Ik nam dan al snel een uur van je tijd in beslag, zonder dat je er een probleem van maakte. Ook toen ik vaak opnieuw dezelfde vele java-bugs maakte in onze programma's bleef je rustig en liet je mij alles op het gemak uitzoeken.

Toen ik het in bepaalde periodes op vlak van onderzoek niet meer zo goed zag zitten, was het de aanwezigheid van heel wat mensen die ervoor zorgden dat ik hier toch gebleven ben.

Eerst en vooral wil ik Nele bedanken. Niet alleen vergezelde je mij zo'n 9 jaar geleden in de ziekenwagen en zorgde je zo voor de eerste ontmoeting tussen mijn papa en vriend (waarvoor dankjewel, zo hoefde ik dit zelf niet te doen), je zorgde er ook voor dat mijn studies en doctoraat ook in moeilijke periodes plezant bleven. Bedankt voor de vele uitleg als student en voor de vele babbeltjes, bureaubezoekjes, uitstapjes... Jammer dat je er de laatste 2 jaar

niet meer bij was!

Een andere reden die het leven op de S9 zo aangenaam maakte, was natuurlijk de sfeer op onze bureau. Meermaals waren we er stiekem van overtuigd dat we de tofste bureau van de vakgroep hadden! Patrica, Veerle en Bart zorgden ervoor dat ik me vanaf dag 1 op mijn gemak voelde. Maar ook de veranderingen met Bert, Jan, Gilles en Cathérine zorgden ervoor dat het werken op onze bureau plezant bleef. Een grote dankjewel allemaal! De vele praatjes zorgden voor een plezante afwisseling met het werk!

Ook de rest van de vakgroep verdient een woordje van dank. Niet alleen de toffe sfeer en de vele cafetaria- en bureaubabbels zorgden ervoor dat het plezant werken was in de S9. Ook de vele spelletjesavonden, filmavondjes (vooral de kostuumdrama's dan!), zomeractiviteiten, cultuurchequesuitstapjes...waren een toffe afwisseling!

Naast de collega's zijn er natuurlijk nog heel wat andere mensen die het zeker verdienen om hier vermeld te worden. Heel wat familie en vrienden waren dikwijls geïnteresseerd in "wat er daar nu toch allemaal nog te onderzoeken valt". Ik probeerde het jullie af en toe uit te leggen, maar ik weet niet of ik hier altijd in geslaagd ben. Toch bedankt voor de interesse!

Mama en papa, een dikke merci voor jullie zorg en de mogelijkheden en steun die jullie me tot nu toe gegegeven hebben. Niet alleen de morele steun, maar ook de vele potjes eten en de goeie zorg voor June hielpen mij om mijn doctoraat vol te houden. Dit laatste geldt zeker ook voor Bernard en Griet. Samen met Hanne en Sara zorgden jullie allen er dikwijls voor dat June toch op tijd kon opgepikt worden als ik weer eens mijn trein had gemist en later thuis zou zijn. Sofie en Sara, merci om mijn zusjes te zijn. Ik weet dat jullie altijd zullen klaarstaan voor mij.

Klaas, bedankt voor je grote steun en geduld. Je zorgde ervoor dat ik aan dit doctoraat begon en je vele hulp thuis zorgde ervoor dat ik het ondanks de grote afstand en de vele lange dagen toch ben blijven volhouden. Je weet me op te beuren in lastige periodes en zorgt supergoed voor ons klein Juneke. Merci!

Juneke, jij en je lachjes zorgen ervoor dat het na een werkdag steeds plezant is om thuis te komen!

Heide Sticker
Mei 2012

Bibliography

[1] M. Artebani and I. Dolgachev. The Hesse pencil of plane cubic curves. *L'Enseign. Math.*, 55:235–273, 2009.

[2] S. Ball and J. W. P. Hirschfeld. Bounds on (n, r)-arcs and their application to linear codes. *Finite Fields Appl.*, 11:326–336, 2005.

[3] J. Bierbrauer. The maximal size of a 3-arc in $\mathrm{PG}(2, 8)$. *J. Combin. Math. Combin. Comput.*, 45:145–161, 2003.

[4] E. Boros and T. Szőnyi. On the sharpness of a theorem of B. Segre. *Combinatorica*, 14:111–114, 1994.

[5] G. Brinkmann and B. D. McKay. Posets on up to 16 points. *Electron. J. Combin.*, 19:147–179, 2002.

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

[7] J. M. Chao and H. Kaneta. Classical arcs in $\mathrm{PG}(r, q)$ for $23 \leq q \leq 29$. *Discrete Math.*, 226:377–385, 2001.

[8] B. Cherowitzo. Bill Cherowitzo's Hyperoval Page, 1999. `http://math.ucdenver.edu/~wcherowi/research/hyperoval/hypero.html`.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford, Clarendon Press, 1985.

[10] K. Coolsaet and H. Sticker. A full classification of the complete k-arcs in $\mathrm{PG}(2, 23)$ and $\mathrm{PG}(2, 25)$. *J. Comb. Des.*, 17(6):459–477, 2009.

[11] K. Coolsaet and H. Sticker. Arcs with Large Conical Subsets. *Electron. J. Combin.*, 17:#R112, 2010.

[12] K. Coolsaet and H. Sticker. The complete k-arcs of $\mathrm{PG}(2,27)$ and $\mathrm{PG}(2,29)$. *J. Comb. Des.*, 19(2):111–130, 2011.

[13] K. Coolsaet and H. Sticker. The complete $(k,3)$-arcs of $\mathrm{PG}(2,q)$, $q \leq 13$. *J. Comb. Des.*, 20(2):89–111, 2012.

[14] 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.*, 94:31–58, 2009.

[15] G. Faina and F. Pambianco. On the spectrum of the values k for which a complete k-cap in $\mathrm{PG}(n,q)$ exists. *J. Geom.*, 62:84–98, 1998.

[16] J. C. Fisher, J. W. P Hirschfeld, and J. A. Thas. Complete arcs in planes of square order. *Annals Discrete Math.*, 30:243–250, 1986.

[17] M. Giulietti. Small complete caps in $\mathrm{PG}(2,q)$, for q an odd square. *J. Geom.*, 69:110–116, 2000.

[18] M. Giulietti. On plane arcs contained in cubic curves. *Finite Fields Appl.*, 8:69–90, 2002.

[19] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford, Clarendon Press, second edition, 1998.

[20] J. W. P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. *Finite Geometries, Proceedings*, 3:201–246, 2001.

[21] P. Kaski and P. R. J. Östergård. *Classification Algorithms for Codes and Designs*. Springer, Heidelberg, 2006.

[22] B. C. Kestenband. Unital intersections in finite projective planes. *Geom. Dedicata*, 11:107–117, 1981.

[23] G. Korchmáros. Osservazioni sui risultati di b. segre relativi ai k-archi completi contenenti $k-1$ punti di una conica. *Atti Accad. Naz. Lincei Rend.*, 56:541–549, 1974.

[24] G. Korchmáros and A. Sonnino. Complete arcs arising from conics. *Discrete Math.*, 267:181–187, 2003.

[25] 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.*, 18:25–47, 2010.

[26] G. Kéri. Types of superregular matrices and the number of n-arcs and complete n-arcs in $\mathrm{PG}(r,q)$. *J. Comb. Des.*, 14:363–390, 2006.

[27] S. Levy. *The eightfold way: the beauty of Klein's quartic curve*. Cambridge, Cambridge University Press, 1999.

[28] L. Lunelli and M. Sce. *k-archi completi nei piani proiettivi desarguesiani di rango 8 e 16*. Politecnico di Milano, Centro di calcoli numerici, 1958.

[29] S. Marcugini, A. Milani, and F. Pambianco. Maximal $(n,3)$-arcs in $PG(2,11)$. *Discrete Math.*, 208/209:421–426, 1999.

[30] S. Marcugini, A. Milani, and F. Pambianco. Classification of the $[n,3,n-3]_q$ codes over GF(7) GF(8) and GF(9). *Ars Combinatorica*, 61:263–269, 2001.

[31] S. Marcugini, A. Milani, and F. Pambianco. Minimal complete arcs in $\mathrm{PG}(2,q)$, $q \leq 29$. *J. of Combin. Math. Combin. Comput.*, 47:19–29, 2003.

[32] S. Marcugini, A. Milani, and F. Pambianco. Classification of the $(n,3)$-arcs in $\mathrm{PG}(2,7)$. *J. Geom.*, 80:179–184, 2004.

[33] S. Marcugini, A. Milani, and F. Pambianco. Maximal $(n,3)$-arcs in $PG(2,13)$. *Discrete Math.*, 294:139–145, 2005.

[34] S. Marcugini, A. Milani, and F. Pambianco. Complete arcs in $\mathrm{PG}(2,25)$: The spectrum of sizes and the classification of the smallest complete arcs. *Discrete Math.*, 307:739–747, 2007.

[35] B. D. McKay. Isomorph-free exhaustive generation. *J. Algorithms*, 26:306–324, 1998.

[36] P. R. J. Östergård and O. Pottonen. The perfect binary one-error-correcting codes of length 15: Part i classification. *IEEE Transactions on Information Theory*, 55(10):4657–4660, 2009.

[37] G. Pellegrino. Sur les k-arcs complets des plans de galois d'ordre impair. *Ann. Discrete Math.*, 18:667–694, 1983.

[38] 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):273–308, 1993.

[39] L. Lombardo Radice. Sul problema dei k-archi completi di $s_{2,q}$. *Boll. Un. Mat. Ital.*, 1:178–181, 1956.

[40] L. Storme and H. Van Maldeghem. Cyclic arcs in $\mathrm{PG}(2,q)$. *J. Algebraic Combinatorics*, 3(1):113–128, 1994.

[41] T. Szőnyi. Small complete arcs in galois planes. *Geom. Dedicata*, 18:161–172, 1985.

[42] J. F. Voloch. On the completeness of certain plane arcs. *European J. Combin*, 8:453–456, 1987.

[43] J. F. Voloch. On the completeness of certain plane arcs ii. *European J. Combin*, 11:491–496, 1990.