



Maximal arcs in finite field planes

P. A. Hoadley

October, 2003

Supervisors: S. G. Barwick, M. R. Brown

Thesis submitted as a requirement for the degree of Bachelor
of Mathematical and Computer Sciences (Honours) in the
School of Pure Mathematics

Contents

1	Introduction	1
2	Elementary projective geometry	3
2.1	History	3
2.2	Homogeneous co-ordinates	5
2.3	Projective space over a field	7
2.4	Affine space over a field	9
2.5	Incidence structures	9
3	Some structures in $PG(2, q)$ and $PG(3, q)$	11
3.1	Conics	11
3.2	Arcs	13
3.3	k -caps and Ovaloids	15
4	Maximal arcs in finite field planes	22
4.1	Some definitions and elementary results	22
4.2	Existence of maximal arcs	23
4.3	Trivial maximal arcs	25
5	Denniston maximal arcs	27
5.1	Some results from group theory	27
5.2	Quadratic polynomials in finite fields	30
5.3	Constructing the maximal arcs	31
5.4	Geometry of the Denniston arcs	33

6	Thas (1974) maximal arcs	35
6.1	Some preliminary definitions and results	35
6.2	Constructing the translation plane	43
6.3	Constructing the Thas (1974) maximal arcs	46
7	Mathon maximal arcs	50
7.1	Some definitions from field theory	50
7.2	Sets of conics	51
7.3	An example of the Mathon construction	61
8	Further constructions from sets of conics	63
9	Conclusion	67

List of Figures

2.1	Central projection	4
5.1	A Denniston maximal arc	34
6.1	A Thas (1974) maximal arc	47
6.2	Projection of a plane through a point	48

List of Tables

2.1	Names of subspaces of $PG(n, K)$	8
6.1	Counts of objects in $PG(3, q)$ and $PG(3, q^2)$	37

Abstract

A *maximal arc* is an interesting structure found in projective planes. This thesis will present the background material required to define and prove the existence of maximal arcs. Three constructions of non-trivial maximal arcs by different authors will be presented. Some of the recent literature on new constructions will be covered in overview.

Chapter 1

Introduction

A *maximal arc* is a set of points in a projective plane with certain distinguishing properties, and is a refinement of the more general concept of an *arc*. Maximal arcs have proved interesting over many years. It is straightforward to construct trivial examples of maximal arcs, but the question of the existence of non-trivial maximal arcs (which proved to be separate questions for projective planes of odd and even order) went unanswered for some time.

In this thesis, we will consider not only the general geometric properties of maximal arcs in finite field planes, but also three practical constructions from different authors published over three decades. Chapter 2 will introduce a small amount of background material in projective geometry. Only those topics central to the understanding of later chapters will be presented. Chapter 3 will consider in more detail some geometric structures in projective planes and spaces—again, primarily material which will be used in the constructions of later chapters. Chapter 4 will introduce maximal arcs, consider some of their properties, and present a brief historical overview of work by various authors.

The first of three non-trivial constructions will be presented in Chapter 5. This construction, due to Denniston in 1969 [9], proved the existence of non-trivial maximal arcs in field planes of even order. The construction relies on some results from group theory, a review of which will be given in

Section 5.1. Chapter 6 presents a construction due to Thas in 1974 [19].¹ It involves finding a maximal arc in a translation plane constructed by the method of Bruck and Bose [6]. A more recent construction due to Mathon in 2002 [18] is presented in Chapter 7. This approach, using sets of conics, has been extended to yield further new constructions. Several papers using this method are surveyed in Chapter 8.

There are other constructions yielding maximal arcs, including that of Thas in 1980 mentioned in the footnote below. This thesis will not describe all of them in detail, and will be confined predominantly to maximal arcs in finite field planes. The aim is to present an interesting mathematical and historical survey of work on existence results and known constructions of maximal arcs. Section 4.2 presents an outline of some important existence results that will not be covered in detail.

¹These arcs are commonly called Thas (1974) maximal arcs to distinguish them from a separate construction due to Thas published in 1980. The latter construction will not be considered in this thesis.

Chapter 2

Elementary projective geometry

Some familiarity with projective geometry will be assumed in this thesis. In this chapter we will review some of the more important introductory concepts which are used regularly throughout the remaining chapters. Section 2.1 will give a very brief overview of some of the history of projective geometry. Section 2.2 introduces *homogeneous co-ordinates* which will be used in some proofs in later chapters. We will introduce definitions of *projective spaces* (Section 2.3) and *affine spaces* (Section 2.4). Section 2.5 will define *incidence structures*.

2.1 History

For centuries, the only system of geometry was that described by Euclid in his ‘Elements’ (*circa* 300 BC). It displayed an ‘august procession of definitions, axioms, postulates and theorems deduced from them’ (see [17]). *Euclidean geometry* was accepted for over 2 000 years as describing and arising from the properties of space suggested by real physical experience. Indeed, the word *geometry* means ‘measurement of the Earth’.

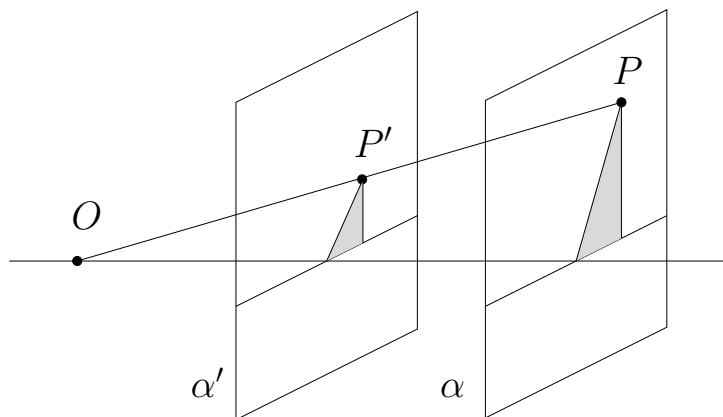
Non-Euclidean geometries began to arise during the nineteenth century

by extracting ideas of a simple nature from Euclidean geometry, especially those ideas that did not involve measurement of distance or angle (see [8] for more details). *Projective geometry*, in particular, arises from the study of those properties that are invariant under *central projection*.

Definition 2.1. Two figures in distinct planes are said to be derived from each other by *central projection* if corresponding points can be joined by concurrent lines, all passing through a fixed point O , the *centre of projection*.

An example of central projection is shown in Figure 2.1. Immediately we

Figure 2.1: Central projection



The point $P \in \alpha$ is projected onto the plane α' by finding the intersection P' of α' and the line joining P with the point O , the centre of projection. Note that, in general, there is no requirement that α and α' be parallel.

lose certain properties that we had in Euclidean geometry:

- measure (both linear and angular)
- parallelism
- perpendicularity
- distinction between conics.

However, we also retain some properties. Most importantly, we retain type (points remain points and lines remain lines) and incidence (whether a point lies on a line).

At this point, we can define the *extended Euclidean plane*, an example of a *projective plane*, in the following intuitive way.

Definition 2.2. Consider the Euclidean plane.

1. Call the set of all lines parallel to a given line in the Euclidean plane a *pencil* of parallel lines.
2. To each pencil of parallel lines, add an abstract entity called a *point at infinity*. Distinct pencils have distinct points at infinity.
3. The set of all points at infinity define the *line at infinity*, l_∞ .

The resulting structure is called the *extended Euclidean plane*, and is an example of a *projective plane*.

We will define a particular type of projective plane, the *field plane*, more rigorously in Section 2.3. We will also define more rigorously the properties of projective planes in Section 2.5. For now it will suffice to notice that in the construction of the extended Euclidean plane we have lost the property of parallelism: any two lines in a projective plane will meet at some point, even if only at the line at infinity.

2.2 Homogeneous co-ordinates

It is simple to demonstrate that normal Cartesian co-ordinates are inadequate to express the property of a projective plane that states that any two lines meet in a unique point. Let l and m be two distinct parallel lines with slope a such that

$$\begin{aligned}l &: y = ax + c \\m &: y = ax + c'.\end{aligned}$$

Clearly there exists no Cartesian point (x, y) to represent the point of intersection of l and m at the line at infinity, l_∞ .

Homogeneous co-ordinates arise when we consider a point as being determined by an ordered set of *three* numbers where only the ratios between those numbers are significant (see [17]). Now let

$$\begin{aligned} l : aX + bY + c &= 0 \\ m : a'X + b'Y + c' &= 0. \end{aligned}$$

Let P be the point of intersection, but now consider the co-ordinates (X, Y) of P as ratios where

$$X : Y : 1 = bc' - b'c : ca' - c'a : ab' - a'b.$$

Now we write

$$\begin{aligned} X = \frac{x}{z} &= \frac{kx}{kz} \\ Y = \frac{y}{z} &= \frac{ky}{kz} \quad k \neq 0, \end{aligned}$$

and see that any point (X, Y) is expressible in terms of three co-ordinates, $(x, y, z) \equiv (kx, ky, kz) \equiv k(x, y, z)$. As it stands, this holds only for non-parallel lines. We can easily extend the concept by allowing $z = 0$, hence $ab' - a'b = 0$ and then l and m are parallel. Notice that only the ratios are important, and we can derive only *two* independent ratios from a set of three co-ordinates. We exclude $(0, 0, 0)$ from being a possible point.

Our equations for the lines l and m now become homogeneous in the variables x, y, z :

$$\begin{aligned} l : ax + by + cz &= 0 \\ m : a'x + b'y + c'z &= 0, \end{aligned}$$

and the point of intersection is $P \equiv (bc' - b'c, ca' - c'a, ab' - a'b)$. In particular, though, because $-\frac{a}{b} = -\frac{a'}{b'}$, $P \equiv (bc' - b'c, ca' - c'a, 0)$. That $z = 0$ will always be the case for such a point at infinity, and hence l_∞ has equation $z = 0$.

We will use the familiar notation (x, y, z) to represent the point with those co-ordinates, but also denote the line l by $[a, b, c]$ where it holds that

$$ax + by + cz = 0.$$

It is straightforward to show that for two points $P_1 = (x_1, y_1, z_1)$ and $P_2 = (x_2, y_2, z_2)$, the unique line l passing through these points is given by the equation

$$\begin{vmatrix} x & y & z \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = 0.$$

Similarly, for two lines $l = [a_1, b_1, c_1]$ and $m = [a_2, b_2, c_2]$, the point of intersection is $(b_1c_2 - b_2c_1, c_1a_2 - c_2a_1, a_1b_2 - a_2b_1)$, as shown above. Finally, a line $l = [a, b, c]$ is incident with a point $P = (x, y, z)$ if and only if $ax + by + cz = 0$. These relations arise from the construction we will consider in Section 2.3 below.

Homogenous co-ordinates for points and lines in projective planes will be used in some proofs in later chapters.

2.3 Projective space over a field

We can define a projective plane, and more generally a projective space, using mappings from a vector space over a field. Firstly we will define the *n-dimensional projective space over a field K*.

Definition 2.3. Let $V = V(n + 1, q)$ be an $(n + 1)$ -dimensional vector space over a field K with zero element 0 . Consider the equivalence relation \mathcal{R} on the elements of $V - \{0\}$ where the equivalence classes are the one-dimensional subspaces of V with the zero deleted. (Thus if $X, Y \in V - \{0\}$, then $X \equiv Y \Leftrightarrow Y = tX$ for some $t \in K - \{0\}$.) Then the set of equivalence classes is the *n-dimensional projective space over K* and is denoted by $PG(n, K)$, or, when $K = GF(q)$, $PG(n, q)$. In the case of a plane, we call $PG(2, K)$ a *field plane*.

From here, we can define a series of structures inside a projective space.

Definition 2.4. Given an n -dimensional projective space $PG(n, K)$ over a field K :

1. A *point* is an element of $PG(n, K)$. Specifically, the equivalence class of the vector $X \in V - \{0\}$ (using the relation \mathcal{R} from Definition 2.3) is the point $\mathbf{P}(X)$.
2. For any $m \in \{-1, 0, 1, 2, \dots, n\}$, a subspace of dimension m , or an m -*space*, of $PG(n, K)$ is a set of points all of whose representing vectors form, together with the zero, a subspace of dimension $m + 1$ of $V = V(n + 1, q)$. This subspace is denoted Π_m . A subspace of dimension zero has already been defined as a point, and we make the further definitions given in Table 2.1 for other dimensions.

Table 2.1: Names of subspaces of $PG(n, K)$

m	Π_m
-1	ϕ
0	point
1	line
2	plane
3	3-space or solid
$n - r$	subspace of co-dimension r
$n - 2$	secundum
$n - 1$	hyperplane or prime

3. A *hyperplane* or *prime* is the set of points $\mathbf{P}(X)$ whose vectors $X = (x_0, \dots, x_n)$ satisfy a linear equation

$$u_0x_0 + u_1x_1 + \dots + u_nx_n = 0$$

with $U = (u_0, \dots, u_n) \in K^{(n+1)} - \{(0, \dots, 0)\}$. It can be denoted $\Pi(U)$.

From Definition 2.3 follows a *co-ordinate system* for the projective space $PG(n, K)$. If the equivalence class of X is the point $\mathbf{P}(X)$ then X is called a *co-ordinate vector* for $\mathbf{P}(X)$. Further, tX with $t \in K - \{(0, \dots, 0)\}$ is also a co-ordinate vector for $\mathbf{P}(X)$. This co-ordinate system is directly analogous to the system of homogeneous co-ordinates presented in Section 2.2. (For the remainder of this thesis, we will relax the notation for a point and use X for $\mathbf{P}(X)$.)

2.4 Affine space over a field

Definition 2.5. If H_∞ is any hyperplane in $PG(n, K)$ then

$$AG(n, K) = PG(n, K) - H_\infty$$

is an *affine space of dimension n over K* . As with $PG(n, K)$, if $K = GF(q)$, we write $AG(n, q)$.

The subspaces of $AG(n, K)$ are the subspaces of $PG(n, K)$ not contained in H_∞ , and with any points of H_∞ deleted in each case. We call H_∞ the *hyperplane at infinity of $AG(n, q)$* .

2.5 Incidence structures

In this section we will confine discussion to spaces of two dimensions, though the definitions generalise to higher dimensions.

Definition 2.6. An *incidence structure* is a triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ where \mathcal{P} is a set of points, \mathcal{L} is a set of lines and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$. Let $P \in \mathcal{P}$ and $l \in \mathcal{L}$. If $(P, l) \in \mathcal{I}$ then P is said to be *incident* with l , or l to be *incident* with P .

Definition 2.7. A set of points $\{P_1, \dots, P_n\} \subseteq \mathcal{P}$ is said to be *collinear* if there exists a line $l \in \mathcal{L}$ such that $P_i \in l$ for each $i \in 1, \dots, n$.

We can now define projective and affine planes in the conventional axiomatic way.

Definition 2.8. Let \mathcal{P} be an incidence structure with the following properties:

P1: Any two points are incident with exactly one line.

P2: Any two lines are incident with exactly one point.

P3: Each line is incident with at least three points.

P4: There exist at least three non-collinear points.

We call \mathcal{P} a *projective plane*.

Definition 2.9. Let \mathcal{A} be an incidence structure with the following properties:

A1: Any two distinct points lie on a unique line.

A2: Given any line l and any point P not incident with l , there exists a unique line m such that P is incident with m , and l and m are incident with no common point.

A3: There exist at least three non-collinear points.

We call \mathcal{A} an *affine plane*.

Starting with the next chapter, we will be considering structures in projective planes and spaces (in particular, in planes and spaces co-ordinatised by finite fields). In Chapters 5 and 6, we will be using affine planes in some proofs.

Chapter 3

Some structures in $PG(2, q)$ and $PG(3, q)$

In this chapter we will survey some basic structures in projective planes and projective 3-spaces. In Section 3.1 we consider *conics* in $PG(2, q)$. This leads on to Section 3.2 where we will look at *arcs* in projective planes. The results derived in that section will be used in Section 3.3 concerning *k-caps* and *ovaloids*. The main result will be Theorem 3.20 which will be used in the construction of a maximal arc due to Thas in Chapter 6.

3.1 Conics

Definition 3.1. A *conic* \mathcal{C} in $PG(2, q)$ is a set of points whose co-ordinates (x, y, z) satisfy a homogeneous equation of degree two:

$$\mathcal{C} : S(x, y, z) = ax^2 + by^2 + cz^2 + fyz + gzx + hxy = 0$$

where $a, \dots, h \in GF(q)$ and are not all zero.

Definition 3.2. A conic \mathcal{C} is *reducible* or *degenerate* if $S(x, y, z) = 0$ is reducible: if it factorises into two homogeneous linear factors over $GF(q)$ (or a field extension of $GF(q)$). Otherwise \mathcal{C} is called *irreducible* or *non-degenerate*.

We need some further definitions and results related to conics for later proofs, but space does not permit a full treatment here. (Further details on results stated without proof here can be found in [16].)

Theorem 3.1. *A line l meets a conic \mathcal{C} in $PG(2, q)$ in exactly two points (possibly coinciding, possibly in a field extension), or else lies wholly on \mathcal{C} .*

Definition 3.3. For a conic $\mathcal{C} \in PG(2, q)$, each line l in the plane is called

1. a *bisecant* if it meets \mathcal{C} in two distinct points,
2. a *tangent* if it meets \mathcal{C} in two coinciding points,
3. an *external line* if it meets \mathcal{C} in two points in a field extension, or
4. a *generator line* if it lies completely on \mathcal{C} .

The following two theorems will be used in Section 3.2.

Theorem 3.2. *Let \mathcal{C} be a conic in $PG(2, q)$, q even, where*

$$\mathcal{C} : ax^2 + by^2 + cz^2 + fyz + gzx + hxy = 0.$$

Then \mathcal{C} is degenerate if and only if $(f, g, h) = (0, 0, 0)$. Provided $(f, g, h) \neq (0, 0, 0)$, the following statements hold:

1. *There exists a unique tangent to \mathcal{C} through each point $P \neq (f, g, h)$.*
2. *All the tangents to \mathcal{C} pass through the point $N = (f, g, h)$. The point N is called the nucleus of the conic \mathcal{C} .*

Theorem 3.3. *Let \mathcal{C} be a non-degenerate conic in $PG(2, q)$.*

1. *If q is odd, \mathcal{C} contains $q + 1$ points, no three collinear.*
2. *If q is even, \mathcal{C} contains $q + 1$ points, no three collinear, and $\mathcal{C} \cup \{N\}$ is a set of $q + 2$ points, no three collinear, where N is the nucleus of \mathcal{C} .*

3.2 Arcs

Definition 3.4. A k -arc in $PG(2, q)$ is a set of k points, no three of which are collinear. A k -arc is *complete* if it is not contained in a $(k + 1)$ -arc.

We will denote the maximum value of k for which a k -arc exists as $m(2, q)$. Of course, each line of $PG(2, q)$ can intersect a k -arc \mathcal{K} in at most two points.

Definition 3.5. A line l that intersects a k -arc \mathcal{K} in i points is called an i -secant.

We will call a 2-secant a *bisecant*, a 1-secant a *tangent* and a 0-secant an *external line*. For P a point on a k -arc \mathcal{K} , let $t(P)$ denote the number of tangents to \mathcal{K} through P . For any point $Q \in PG(2, q) - \mathcal{K}$, let $\sigma_2(Q)$ be the number of bisecants and $\sigma_1(Q)$ the number of tangents to \mathcal{K} through Q . We can prove some simple but useful relations between these quantities.

Lemma 3.4. [16] *Let \mathcal{K} be a k -arc in $PG(2, q)$, let $P \in \mathcal{K}$ and let $Q \in PG(2, q) - \mathcal{K}$. Then the following two relations hold:*

1. $t(P) = q - k + 2$,
2. $\sigma_1(Q) + 2\sigma_2(Q) = k$.

Proof. As $P \in \mathcal{K}$, there are $k - 1$ bisecants to \mathcal{K} through P , and altogether $q + 1$ lines through P , so

$$\begin{aligned} t(P) &= (q + 1) - (k - 1) \\ &= q - k + 2. \end{aligned}$$

Every line l through Q is either an external line, a tangent or a bisecant to \mathcal{K} . The number of points k in \mathcal{K} is the sum of the number of tangents to \mathcal{K} through Q and twice the number of bisecants to \mathcal{K} through Q . Hence, $\sigma_1(Q) + 2\sigma_2(Q) = k$. \square

Corollary 3.5. [16] *Let \mathcal{K} be a $(q+1)$ -arc. There is a unique tangent through each point of \mathcal{K} , and so \mathcal{K} has $q + 1$ tangents.*

Proof. Let P be a point on \mathcal{K} . Since $k = q + 1$, $t(P) = q - (q + 1) + 2 = 1$. \square

Tangents to k -arcs turn out to be very useful. We can prove the following two further results about tangents.

Theorem 3.6. [16] *If q is even, the $(q + 1)$ tangent lines to a $(q + 1)$ -arc \mathcal{K} are concurrent in a point called the nucleus of \mathcal{K} .*

Proof. Let $P \notin \mathcal{K}$, so

$$\sigma_1(P) + 2\sigma_2(P) = k = q + 1.$$

Since q is even, $q + 1$ is odd, and so $\sigma_1(P)$ is odd. Hence there is at least one tangent line through P . Thus, if b is a bisecant of \mathcal{K} , then through every point of b there passes at least one tangent line. There are $q + 1$ points on b , and \mathcal{K} has $q + 1$ tangent lines, so, in fact, through every point $B \in b$ there passes exactly one tangent, so no two tangents can intersect on a bisecant. Now let P be the intersection of two tangents. Then P cannot be on any bisecant of \mathcal{K} , so $\sigma_2(P) = 0$, and hence $\sigma_1(P) = q + 1$. Hence the $q + 1$ tangents are concurrent at P . \square

Lemma 3.7. [16] *A $(q + 2)$ -arc \mathcal{K} has no tangents.*

Proof. Let $P \in \mathcal{K}$. Then $t(P) = q - k + 2 = 0$ by Lemma 3.4. \square

In some circumstances, it is possible to increase the size of a k -arc.

Corollary 3.8. [16] *If q is even, a $(q + 1)$ -arc \mathcal{K} is incomplete, and can be completed uniquely to a $(q + 2)$ -arc.*

Proof. \mathcal{K} has a nucleus N (by Theorem 3.6). Consider the set of $q + 2$ points $\mathcal{K}' = \mathcal{K} \cup N$. A line l not through N cannot be a tangent line to \mathcal{K} , and so meets \mathcal{K}' in two points of \mathcal{K} . Conversely, a line l through N must be a tangent line to \mathcal{K} , and so meets \mathcal{K}' in two points, namely a point of \mathcal{K} and N . So, every line meets \mathcal{K}' in two points, and $\mathcal{K} \cup N$ is a $(q + 2)$ -arc. The nucleus N is unique, so the completion is unique. \square

We are now in a position to determine the maximum value of k .

Theorem 3.9. [16] $m(2, q) = \begin{cases} q + 2 & \text{for } q \text{ even} \\ q + 1 & \text{for } q \text{ odd} \end{cases}$.

Proof. For any k -arc \mathcal{K} , $t(P) = q + 2 - k \geq 0$ (Lemma 3.4). Thus, $k \leq q + 2$, that is, $m(2, q) \leq q + 2$. We consider the cases of q odd and even separately.

- Suppose q is even. Let \mathcal{C} be a non-degenerate conic in $PG(2, q)$. The tangents to \mathcal{C} are concurrent at the nucleus N , so $\mathcal{C} \cup \{N\}$ is a $(q+2)$ -arc. Therefore, $m(2, q) = q + 2$ for q even.
- Suppose q is odd. Assume there exists a $(q + 2)$ -arc \mathcal{K} and let Q be a point such that $Q \in PG(2, q) - \mathcal{K}$. Since in this case, $t(P) = 0$ for all $P \in \mathcal{K}$, there exist no tangents to \mathcal{K} through Q . So,

$$\begin{aligned} 2\sigma_2(Q) &= q + 2 \\ q &= 2(\sigma_2(Q) - 1). \end{aligned}$$

This is a contradiction, since q is odd. Thus a $(q + 2)$ -arc can not exist in $PG(2, q)$, q odd, so $m(2, q) \leq q + 1$. Since a non-degenerate conic in $PG(2, q)$ is a $(q + 1)$ -arc (by Theorem 3.3), $m(2, q) = q + 1$ for q odd.

□

In the next section, we will begin by considering an object in 3-space analogous to the planar k -arc.

3.3 k -caps and Ovaloids

Definition 3.6. In $PG(3, q)$, a set \mathcal{K} of k points no three of which are collinear is called a k -cap. A k -cap is *complete* if it is not contained in a $(k + 1)$ -cap.

We can relate k -caps to k -arcs with a simple lemma, which we will significantly refine later in Theorem 3.20.

Lemma 3.10. [15] *Let \mathcal{K} be a k -cap, and let π be a plane of $PG(3, q)$. Then π meets \mathcal{K} in a set of points \mathcal{K}' which form an arc in π .*

Proof. Assume there exist three points in \mathcal{K}' which are collinear. Then there exist three points in \mathcal{K} which are collinear, which is a contradiction. Hence \mathcal{K}' is an arc in π . \square

We can easily find an upper bound for k if q is odd.

Lemma 3.11. [15] *In $PG(3, q)$, q odd, a k -cap \mathcal{K} satisfies $k \leq q^2 + 1$.*

Proof. Let P_1 and P_2 be two points on \mathcal{K} . Each plane through P_1P_2 meets \mathcal{K} in a k' -arc and so $k' \leq q + 1$ by Theorem 3.9. So, $k \leq 2 + (q + 1)(q - 1)$ where $(q + 1)$ is the number of planes around the line, and $(q - 1)$ is the maximum number of points in the k' -arc excluding P_1 and P_2 . So, $k \leq q^2 + 1$. \square

We can prove a similar result for q even, but to do this we need some further definitions. The first of these is very familiar.

Definition 3.7. A line l that intersects a k -cap \mathcal{K} in i points is called an i -secant.

Again, we will call a 2-secant a *bisecant*, a 1-secant a *tangent* and a 0-secant an *external line*. Let P be a point of a k -cap \mathcal{K} , and let $t(P)$ denote the number of tangents to \mathcal{K} through P . For any point $Q \in PG(3, q) - \mathcal{K}$, let $\sigma_2(Q)$ be the number of bisecants and $\sigma_1(Q)$ the number of tangents to \mathcal{K} through Q .

Lemma 3.12. [15] *Let \mathcal{K} be a k -cap in $PG(3, q)$, and let $P \in \mathcal{K}$, and $Q \in PG(3, q) - \mathcal{K}$. The following two relations hold:*

1. $t(P) + k = q^2 + q + 2$,
2. $\sigma_1(Q) + 2\sigma_2(Q) = k$.

Proof. There are $q^2 + q + 1$ lines through P , and $k - 1$ of these are bisecants, so the remainder are tangents. Hence,

$$\begin{aligned} t(P) &= q^2 + q + 1 - (k - 1) \\ t(P) + k &= q^2 + q + 2 \end{aligned}$$

The second relation was essentially proved in Lemma 3.4. \square

Our aim in this section is to prove a result about a particular type of k -cap. The following two theorems will give us a useful inequality relating k and the order, q , of the projective space.

Theorem 3.13. [15] *A k -cap \mathcal{K} in $PG(3, q)$, q even, has no tangents if and only if $q = 2$, $k = 8$, and \mathcal{K} is the complement of a plane.*

Proof. (\Rightarrow): Suppose that \mathcal{K} has no tangents, so $t(P) = 0$ for all $P \in \mathcal{K}$, and hence $k = q^2 + q + 2$ by Lemma 3.12. The number of bisecants of \mathcal{K} is:

$$\binom{q^2 + q + 2}{2} = \frac{(q^2 + q + 2)(q^2 + q + 1)}{2}$$

which is less than $(q^2 + 1)(q^2 + q + 1)$, the total number of lines in $PG(3, q)$. Hence there exists a line l external to \mathcal{K} . Because there are no tangent lines to \mathcal{K} , a plane through l is either skew to \mathcal{K} or meets \mathcal{K} in a k -arc \mathcal{K}' . As \mathcal{K}' has no tangents, \mathcal{K}' is a $(q + 2)$ -arc. So, $q + 2$ must divide $q^2 + q + 2$. Since $q^2 = (q - 2)(q + 2) + 4$, $q + 2$ divides 4. Therefore, $q = 2$ and $k = 2^2 + 2 + 2 = 8$. Finally, let $\mathcal{S} = PG(3, 2) - \mathcal{K}$. It follows that \mathcal{S} is a set of seven points such that if a line l has two of its points in \mathcal{S} , it has all three. So \mathcal{S} is a plane, and \mathcal{K} is the complement of a plane.

(\Leftarrow): Let \mathcal{K} be a complement of a plane \mathcal{S} in $PG(3, 2)$, so $\mathcal{S} = PG(3, 2) - \mathcal{K}$. Assume there exists a line l that is a tangent to \mathcal{K} . So one point P of l is incident with \mathcal{K} , and the remaining two points of l are incident with \mathcal{S} . This leads to a contradiction, since \mathcal{S} is a plane. So there exist no tangents to \mathcal{K} . \square

Theorem 3.14. [15] *If \mathcal{K} is a k -cap in $PG(3, q)$, q even, and $q > 2$, then $k \leq q^2 + 1$.*

Proof. Suppose $k > q^2 + 1$ (and $k < q^2 + q + 2$ by Lemma 3.12 and Theorem 3.13). We may assume \mathcal{K} is complete, since if not we complete \mathcal{K} to a k' -cap with $k' > q^2 + 1$. Let $P \in \mathcal{K}$, and let l be a tangent to \mathcal{K} through P (l exists by Theorem 3.13). Since a $(q + 2)$ -arc has no tangents (Lemma 3.7), any plane through l meets \mathcal{K} in at most $q + 1$ points. If all planes through l meet \mathcal{K} in at most q points, then $k \leq 1 + (q + 1)(q - 1)$ (since there are $q + 1$ planes through l meeting \mathcal{K} in at most $q - 1$ points other than P), hence $k \leq q^2$. But $k > q^2 + 1$, so there exists a plane π through l such that $\pi \cap \mathcal{K}$ is a $(q + 1)$ -arc. This arc has a nucleus N . If every line through N were an external line or a tangent to \mathcal{K} , then $\mathcal{K} \cup \{N\}$ would be a $(k + 1)$ -cap. Since \mathcal{K} is complete, there exists a bisecant b of \mathcal{K} through N , and b cannot lie in π (because every line joining N to a point on the $(q + 1)$ -arc $\pi \cap \mathcal{K}$ is a tangent). So the $q + 1$ planes through b all contain one of the $q + 1$ tangents in π through N . Therefore, no plane through b meets \mathcal{K} in a $(q + 2)$ -arc (Lemma 3.7). We can count the points of \mathcal{K} on the planes through b : $k \leq 2 + (q + 1)(q - 1)$ (since there are $q + 1$ planes through b meeting \mathcal{K} in at most $q - 1$ points other than the two points of the bisecant itself), hence $k \leq q^2 + 1$. This is a contradiction, so $k \leq q^2 + 1$. \square

We can now make a claim about the intersection of certain planes with a k -cap.

Corollary 3.15. [15] *Let \mathcal{K} be a $(q^2 + 1)$ -cap. Let b be a bisecant to \mathcal{K} . Then each plane through b meets \mathcal{K} in a $(q + 1)$ -arc.*

Proof. As in Theorem 3.14, we can count the points of \mathcal{K} in the planes through b . There are $q^2 + 1$ points in \mathcal{K} . Since $q^2 + 1 = 2 + (q + 1)(q - 1)$, the $q + 1$ planes through b each meet \mathcal{K} in *exactly* $q - 1$ points other than the two points of \mathcal{K} on the bisecant b . So each plane through b meets \mathcal{K} in $q + 1$ points which are necessarily a $(q + 1)$ -arc. \square

We now need some results about tangents to k -caps.

Lemma 3.16. [15] *Let \mathcal{K} be a $(q^2 + 1)$ -cap, and let $P \in \mathcal{K}$. Then there are $q + 1$ tangents through P .*

Proof. There are q^2 points in $\mathcal{K} - P$, so q^2 bisecants to \mathcal{K} through P . The remaining $q + 1$ lines through P are therefore tangents to \mathcal{K} . \square

We will denote the maximum value of k for which a k -cap exists in $PG(3, q)$ by $m_2(3, q)$.

Theorem 3.17. [15] *There exists a $(q^2 + 1)$ -cap in $PG(3, q)$, $q > 2$.*

Proof. An elliptic quadric is a $(q^2 + 1)$ -cap. (The details are omitted here, as we do not have room to consider quadrics. Instead, the reader is referred to [15] where quadrics in $PG(3, q)$ are defined, and where it is shown that an elliptic quadric in $PG(3, q)$ is a $(q^2 + 1)$ -cap.) \square

Theorem 3.18. [15] *Let \mathcal{K} be a k -cap in $PG(3, q)$. Then:*

1. $m_2(3, q) = q^2 + 1$ for $q > 2$;
2. $m_2(3, 2) = 8$.

Proof. We know $m_2(3, q) \leq q^2 + 1$ for q odd (Lemma 3.11) and $m_2(3, q) \leq q^2 + 1$ for q even and $q > 2$ (by Theorem 3.14). Since it can be shown that an elliptic quadric is a $(q^2 + 1)$ -cap (Theorem 3.17), $m_2(3, q) = q^2 + 1$ for $q > 2$, and $m_2(3, 2) = 8$ by Theorem 3.13. \square

For $q > 2$, a $(q^2 + 1)$ -cap in $PG(3, q)$ is called an *ovaloid* or an *ovoid*. (In higher dimensions, these objects are distinct, though we need only consider them in $PG(3, q)$ for the remainder of this thesis.)

Theorem 3.19. [15] *Let \mathcal{K} be an ovaloid in $PG(3, q)$, and let $P \in \mathcal{K}$. The $q + 1$ tangent lines to \mathcal{K} through P lie in a plane π . (We call π the tangent plane to \mathcal{K} at P , and note that $\pi \cap \mathcal{K} = \{P\}$.)*

Proof. Firstly consider the case where q is odd. Fix a point $P \in \mathcal{K}$. Let $Q \in \mathcal{K}$, $Q \neq P$, and let π be a plane through PQ . So, by Corollary 3.15, π is a plane through P that meets \mathcal{K} in a $(q + 1)$ -arc, and $Q \in \pi$. We will count incident pairs (Q, π) (such that $Q \in \mathcal{K} - P$ and π is a plane through P that meets \mathcal{K} in a $q + 1$ -arc) in two ways. Firstly, we count the pairs by

multiplying the number of points $Q \in \mathcal{K} - P$ by the number of planes through PQ , giving $q^2(q+1)$. Now let t be the number of planes π through P that meet \mathcal{K} in a $(q+1)$ -arc. We can obtain the number of pairs by multiplying t by the number of points of $\mathcal{K} - P$ in π , which gives tq . So,

$$\begin{aligned} q^2(q+1) &= tq \\ t &= \frac{q^2(q+1)}{q} \\ &= q(q+1) \\ &= q^2 + q. \end{aligned}$$

As the number of planes through P is $q^2 + q + 1$, the remaining plane π' meets \mathcal{K} in $\{P\}$, and the $q+1$ lines through P in π' are the $q+1$ tangent lines through P .

Now consider the case where q is even. Let P be a point in \mathcal{K} and l a tangent line to \mathcal{K} through P . As in the proof of Theorem 3.14, there exists a plane π' through l meeting \mathcal{K} in a $(q+1)$ -arc with nucleus N . So there are $q+1$ tangents through N in π' . Since $|\mathcal{K}| = q^2 + 1$, \mathcal{K} is complete, and so there exists a bisecant b to \mathcal{K} through N . Each plane β through b meets \mathcal{K} in a $(q+1)$ -arc by Corollary 3.15.

We now show that every tangent to \mathcal{K} through N is in π' . Let the $q+1$ planes about b be $\beta_1, \dots, \beta_{q+1}$. The intersection $\beta_i \cap \mathcal{K}$ is a $(q+1)$ -arc, so a point $Q \in \beta_i$ which is not on the arc either lies on one tangent or on $q+1$ tangents by Theorem 3.6. But Q lies on the bisecant b , so Q cannot be the nucleus. Therefore, Q lies on one tangent, t_i , and $t_i \neq t_j$ for $i \neq j$. Since every line through N lies in one of the β_i , the number of tangent lines through N is $q+1$, and these all lie in π' , as N is the nucleus of $\pi' \cap \mathcal{K}$. This also means that if a plane α through l other than π' contains a point P' of \mathcal{K} other than P , then PP' is a bisecant and so $\alpha \cap \mathcal{K}$ is a $(q+1)$ -arc. Notice that $q^2 + 1 = q(q) + 1$, where there are q points in $(\alpha \cap \mathcal{K}) - P$, and q such planes through l , leaving a single plane through l which must meet \mathcal{K} in just the point P . This plane must contain all of the $q+1$ tangent lines through P . Hence there is a unique plane through P that meets \mathcal{K} in one point. \square

The final theorem makes a general claim about the intersection of planes and ovaloids in $PG(3, q)$. We will use this result in the Thas (1974) construction in Chapter 6.

Theorem 3.20. [15] *Let \mathcal{K} be a $(q^2 + 1)$ -cap (an ovaloid) in $PG(3, q)$. Then every plane of $PG(3, q)$ is either a tangent plane, or meets \mathcal{K} in a $(q + 1)$ -arc.*

Proof. By Theorem 3.19, there are $q^2 + 1$ tangent planes to \mathcal{K} . Let π be a plane in $PG(3, q)$. If $|\pi \cap \mathcal{K}| \geq 2$ then $|\pi \cap \mathcal{K}| = q + 1$ by Corollary 3.15. We can define such a plane by choosing three points on \mathcal{K} , but once defined, any three points on the resulting $(q + 1)$ -arc will result in the same plane. So, the number of such planes meeting \mathcal{K} in a $(q + 1)$ -arc is given by

$$\frac{\binom{q^2+1}{3}}{\binom{q+1}{3}} = q(q^2 + 1).$$

Finally, the number of external planes is given by subtracting the number of tangent planes and the number of planes meeting \mathcal{K} in a $(q + 1)$ -arc from the total number of planes in $PG(3, q)$:

$$\begin{aligned} \text{Number of external planes} &= (q^3 + q^2 + q + 1) - (q^2 + 1) - (q^3 + q) \\ &= 0. \end{aligned}$$

Therefore, every plane of $PG(3, q)$ is either a tangent plane, or meets \mathcal{K} in a $(q + 1)$ -arc. \square

Chapter 4

Maximal arcs in finite field planes

In this chapter, we finally meet the *maximal arc*. Section 4.1 gives some elementary results. In Section 4.2 we look at the existence of maximal arcs. The trivial maximal arcs are considered in Section 4.3.

4.1 Some definitions and elementary results

In this section we introduce the $\{k; n\}$ -arc and the *maximal arc*. Some results are presented involving both structures.

Definition 4.1. A $\{k; n\}$ -arc \mathcal{K} of a finite projective plane π of order q is a set of k points of π such that some line of π meets \mathcal{K} in n points, but no line meets \mathcal{K} in more than n points.

So a $\{k; n\}$ -arc is a set of k points in π where no $n + 1$ points are collinear.

Definition 4.2. A line l that meets a $\{k; n\}$ -arc in m points is called an *m-secant*. In the particular cases where $m = 0, 1$ or 2 , l is called an *external line*, a *tangent* and a *bisecant* respectively.

Lemma 4.1. [16] *Let \mathcal{K} be a $\{k; n\}$ -arc in a projective plane π of order q . If \mathcal{K} has an m -secant, then $k \leq q(n - 1) + m$.*

Proof. Let $P \in \mathcal{K}$ be on an m -secant. Then there are q lines other than the m -secant through P , each of which meet \mathcal{K} in at most $n - 1$ points. Hence $k \leq q(n - 1) + m$. \square

Corollary 4.2. [16] *Let \mathcal{K} be a $\{k; n\}$ -arc in a projective plane π of order q . Then $k \leq q(n - 1) + n$.*

Proof. If a line l is an m -secant, then $m \leq n$. Now $k \leq q(n - 1) + n$ by Lemma 4.1. \square

We have, then, a maximum value for k , and this leads us to the definition of a *maximal arc*.

Definition 4.3. If \mathcal{K} is a $\{k; n\}$ -arc in a projective plane π and $k = q(n - 1) + n$, then \mathcal{K} is called a *maximal arc*.

Lemma 4.3. [11] *Let \mathcal{K} be a maximal $\{k; n\}$ -arc in a projective plane π of order q . Then every line l in π meets \mathcal{K} in either zero or n points.*

Proof. Suppose l meets \mathcal{K} in m points where $1 \leq m < n$. Let $P \in \mathcal{K}$ be a point incident with l . Then, other than l , there are q lines through P , each meeting \mathcal{K} in at most $n - 1$ points other than P (since \mathcal{K} is a $\{k; n\}$ -arc). Hence $k \leq m + q(n - 1) < q(n - 1) + n$. Therefore, \mathcal{K} is not a maximal arc. This is a contradiction, so every line l in π meets \mathcal{K} in either zero or n points. \square

So, equivalent to Definition 4.3, a maximal $\{k; n\}$ -arc \mathcal{K} is a subset of points of π such that every line $l \in \pi$ meets \mathcal{K} in zero or n points.

4.2 Existence of maximal arcs

An obvious question is ‘for what values of n do maximal arcs exist in a projective plane of order q ?’ In this section, we will first derive a necessary condition for the existence of a maximal arc and then look at when this is also sufficient.

Definition 4.4. Let π be a projective plane. The *dual* π' of π is the incidence structure whose points are the lines of π and whose lines are the points of π . The incidence relation is the same in π' as in π .

It can be shown easily that the dual of a projective plane is a projective plane.

Lemma 4.4. [11] *If \mathcal{K} is a maximal $\{q(n-1) + n; n\}$ -arc in a projective plane π of order q and $n < q$ then the set of lines external to \mathcal{K} is a maximal $\{q(q-n+1)/n; q/n\}$ -arc in the dual plane π' .*

Proof. Let \mathcal{K}' be the set of points in π' corresponding to the lines in π that are external to \mathcal{K} . It will be shown that every line in π' meets \mathcal{K}' in either zero or q/n points.

Let P_1 be a point on \mathcal{K} . Therefore, every line incident with P_1 is an n -secant to \mathcal{K} . It follows that the line p_1 in π' corresponding to P_1 is not incident with \mathcal{K}' , since no external line to \mathcal{K} in π can meet P_1 .

Let P_2 be a point not on \mathcal{K} . Every line incident with P_2 is either external to \mathcal{K} or an n -secant to \mathcal{K} . There are

$$\frac{|\mathcal{K}|}{n} = \frac{q}{n}(n-1) + 1$$

lines in π through P_2 secant to \mathcal{K} . Therefore, there are

$$q + 1 - \left(\frac{q}{n}(n-1) + 1 \right) = \frac{q}{n} \tag{4.1}$$

lines in π through P_2 external to \mathcal{K} . So the line $p_2 \in \pi'$ corresponding to P_2 meets \mathcal{K}' in q/n points. Therefore the set of lines in π external to \mathcal{K} is a maximal $\{q(q-n+1)/n; q/n\}$ -arc \mathcal{K}' in the dual plane π' . \square

We will call the set of lines external to a maximal arc \mathcal{K} the *dual* of \mathcal{K} .

Corollary 4.5. [11] *Let \mathcal{K} be a maximal $\{q(n-1) + n; n\}$ -arc in a projective plane π of order q . Then n divides q .*

Proof. By Lemma 4.4, there exists a maximal $\{q(q-n+1)/n; q/n\}$ -arc \mathcal{K}' in the dual plane π' of π . Now q/n must be an integer, so n divides q . \square

So a necessary condition for the existence of a maximal $\{k; n\}$ -arc in a projective plane of order q is that n divides q (and this was originally proved by Barlotti [4] in 1955), but is it sufficient? It turns out that the answer is no: in 1961, Cossu [7] proved that there exists no $\{21; 3\}$ -arc in $PG(2, 9)$. Thas generalised this result in 1975.

Theorem 4.6. [20] *In $PG(2, q)$, $q = 3^h$ and $h > 1$, there are no $\{2q + 3; 3\}$ -arcs and no $\{q(q - 2)/3; q/3\}$ -arcs.*

Ball, Blokhuis and Mazzocca settled the general case for q odd in 1997.

Theorem 4.7. [3] *In $PG(2, q)$, and given $1 < n < q$, there are no $\{qn - q + n; n\}$ -arcs with q odd.*

The proof uses polynomial techniques. Ball and Blokhuis presented a simplified proof (also based on polynomials) in 1998 [2].

Denniston [9] gave a construction in 1969 that proves the existence of maximal arcs in $PG(2, 2^h)$ for any $n = 2^m$, where $m = 0, \dots, h$. That is, n divides q is a sufficient condition in projective planes of even order. This construction is examined in Chapter 5.

4.3 Trivial maximal arcs

The following constructions are known as *trivial* maximal arcs.

Lemma 4.8. [16][20] *Let \mathcal{K} be a maximal $\{k; n\}$ -arc in the projective plane $\pi = PG(2, q)$.*

1. *If $n = q + 1$ then $\mathcal{K} = \pi$.*
2. *If $n = q$ then $\mathcal{K} = AG(2, q) = \pi - l$ for some line l .*
3. *If $n = 1$ then \mathcal{K} is a single point.*

Proof.

1. Since \mathcal{K} is a maximal arc, Lemma 4.1 implies that every line is either an n -secant or an external line of \mathcal{K} . Since $n = q + 1$, there exists a $(q + 1)$ -secant l_0 . Every line in π meets l_0 in a point of \mathcal{K} , hence every line is a $(q + 1)$ -secant so $\mathcal{K} = \pi$.
2. Since $n = q$, by Equation 4.1 (in Lemma 4.4) there is one external line l to \mathcal{K} in π . Hence $\mathcal{K} = AG(2, q) = \pi - l$.
3. Since $k = q(1 - 1) + 1 = 1$, \mathcal{K} is a single point.

□

Note that for $n = 2$, a maximal arc \mathcal{K} is simply a k -arc, a structure we considered in Section 3.2. Some more interesting, non-trivial constructions are presented in Chapter 5 (due to Denniston), Chapter 6 (due to Thas) and Chapter 7 (due to Mathon).

Chapter 5

Denniston maximal arcs

This chapter considers a construction due to Denniston [9]. This work solved the spectral problem for non-trivial maximal arcs in $PG(2, q)$, q even. Prior to Denniston, it was known that the condition that n divides q was necessary for the existence of a maximal arc. Denniston's construction shows that a maximal arc exists for all n dividing q , q even—the condition is also sufficient. Before looking at the construction, we will review some very basic results from group theory.

5.1 Some results from group theory

Definition 5.1. Let G and H be groups. A *homomorphism* from G to H is a function $\phi : G \rightarrow H$ such that, for all $a, b \in G$

$$\phi(ab) = \phi(a)\phi(b).$$

We can summarise the properties of a homomorphism with the following lemma.

Lemma 5.1. [10] *Let G and H be groups, $g \in G$, and $\phi : G \rightarrow H$ a homomorphism.*

1. $\phi(e_G) = e_H$, where e_G and e_H are the identity elements of the respective groups.

2. $\phi(g^{-1}) = (\phi(g))^{-1}$.
3. The image of ϕ is the set $\phi(G) = \{\phi(g) | g \in G\}$. Then $\phi(G)$ is a subgroup of H .
4. The kernel of ϕ is the set $\ker \phi = \{g \in G | \phi(g) = e_H\}$. Then $\ker \phi$ is a normal subgroup of H .

Proof. We prove each of the claims in turn:

1. Consider $\phi(g) = \phi(e_G g) = \phi(e_G)\phi(g)$. So $\phi(e_G) = e_H$.
2. Consider $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H$. So $\phi(g)^{-1} = \phi(g^{-1})$.
3. Let $g_1, g_2 \in G$. Consider $\phi(g_1)\phi(g_2)^{-1} = \phi(g_1g_2^{-1}) \in \phi(G)$. So the image of ϕ is closed under the group operation and taking inverses, and is hence a subgroup of H .
4. Let $g_1, g_2 \in \ker \phi$. So, $\phi(g_1) = \phi(g_2) = e_H$. Then,

$$\begin{aligned} \phi(g_1g_2^{-1}) &= \phi(g_1)\phi(g_2)^{-1} \\ &= e_H e_H^{-1} \\ &= e_H. \end{aligned}$$

So, $g_1g_2^{-1} \in \ker \phi$ and $\ker \phi < G$. Now let $g \in \ker \phi$, and $x \in G$. We show that $xgx^{-1} \in \ker \phi$.

$$\begin{aligned} \phi(xgx^{-1}) &= \phi(x)\phi(g)\phi(x)^{-1} \\ &= \phi(x)e_H\phi(x)^{-1} \\ &= e_H. \end{aligned}$$

So, $xgx^{-1} \in \ker \phi$, and hence $\ker \phi \triangleleft G$.

□

Definition 5.2. Let N and G be groups with $N \triangleleft G$. Consider the set

$$\frac{G}{N} = \{gN | g \in G\}$$

of all left cosets of N in G . Define a binary operation on G/N :

$$gNhN = (gh)N.$$

Then (without proof here—see [10]), G/N is a group, specifically the *factor group* of G by N .

The operation of multiplying cosets is well-defined, but, again, we will not prove it here. These selected results have been recalled only to introduce the following theorem.

Theorem 5.2 (Homomorphism Theorem). [10] *Let $\phi : G \rightarrow H$ be a homomorphism between groups G and H . Then the groups $G/\ker \phi$ and $\phi(G)$ are isomorphic.*

Proof. Let $K = \ker \phi \triangleleft G$. So G/K is a group. We have a one-to-one correspondence:

$$\begin{aligned} \frac{G}{K} &\longleftrightarrow \phi(G) \\ xK &\longleftrightarrow \phi(x) \\ yK &\longleftrightarrow \phi(y) \end{aligned}$$

and

$$xKyK = xyK \longleftrightarrow \phi(xy) = \phi(x)\phi(y).$$

Hence, G/K is isomorphic to $\phi(G)$. □

Definition 5.3. A group G is *elementary abelian* if $G = \Pi_{i=1}^n \mathbb{Z}_p$ for some $n \in \mathbb{N}$ and p a prime.

Finally, we introduce a particular type of homomorphism.

Definition 5.4. Let G be a group. A homomorphism from G to G is called an *endomorphism* of G .

5.2 Quadratic polynomials in finite fields

Denniston's construction begins by considering the finite field $GF(2^r)$.

Lemma 5.3. [9] *Let $F = GF(2^r)$, and let A be its additive group. The map*

$$\phi : F \longrightarrow F$$

where

$$x \longmapsto ax^2 + c \quad (a \neq 0)$$

is a bijection of F .

Proof. Let $\phi' : F \longrightarrow F$ be the map $x \longmapsto x^2$. Then ϕ' is the Frobenius automorphism, since the characteristic of F is two. It follows that ϕ is an injective mapping of F onto itself. \square

Now let $a \neq 0$ and $b \neq 0$. Consider the following two mappings:

$$f : x \longmapsto ax^2 + bx + c$$

$$f_0 : x \longmapsto ax^2 + bx.$$

Notice that f_0 is an endomorphism of A , since

$$\begin{aligned} f_0(x + y) &= a(x + y)^2 + b(x + y) \\ &= (ax^2 + bx) + (ay^2 + by) \\ &= f_0(x) + f_0(y). \end{aligned}$$

Lemma 5.4. [9] *The range $f_0(A)$ is a subgroup of index two in A .*

Proof. By inspection, the kernel of f_0 is $\{0, b/a\} \cong \mathbb{Z}_2$. So, by Theorem 5.2, the range $f_0(A)$ is isomorphic to A/\mathbb{Z}_2 , and thus $f_0(A)$ is a subgroup of index two in A . \square

Finally, we define an irreducible quadratic form over a finite field, an object that will be the starting point for the construction in the next section.

Definition 5.5. An *irreducible quadratic form* $\phi(x, y)$ over $GF(q)$ is a polynomial over $GF(q)$ of the form

$$\phi(x, y) = ax^2 + hxy + by^2$$

which cannot be expressed as the product of two linear polynomials.

5.3 Constructing the maximal arcs

With the preliminary work in the section above, the actual construction is straightforward.

Let n and q be two powers of two with $n \leq q$. Let A be the additive group of $GF(q)$. Firstly, choose an irreducible quadratic form over $GF(q)$:

$$\phi(x, y) = ax^2 + hxy + by^2.$$

Choose a subgroup H of order n of the group A . We can always do this because A is an elementary abelian group, and thus the direct product of prime order subgroups, in this case \mathbb{Z}_2 . If $q = 2^h$, we can write A as a h -tuple where each element corresponds to an occurrence of \mathbb{Z}_2 . If $n = 2^r$ we then choose any r co-ordinates in the h -tuple to construct a subgroup of order n .

Next we need to define *non-homogeneous co-ordinates*. Recall $PG(2, q) = \{(x, y, z) | x, y, z \in GF(q), \text{ not all zero, and } (x, y, z) \equiv \rho(x, y, z) \text{ where } \rho \in GF(q) - \{0\}\}$. We let the line at infinity, l_∞ , be the line $z = 0$. We then give non-homogeneous co-ordinates to the affine plane $PG(2, q) - l_\infty$ as follows. Since $PG(2, q) - l_\infty = \{(x, y, z) | z \neq 0\}$, we can write $PG(2, q) - l_\infty = \{(x, y, 1)\}$ as homogeneous co-ordinates, or $\{(x, y) | x, y \in GF(q)\}$. We call the latter *non-homogeneous co-ordinates*. So, choose a system of non-homogeneous co-ordinates in $PG(2, q)$, and let

$$\mathcal{K} = \{(x, y) | \phi(x, y) \in H\}.$$

Theorem 5.5. [9] *The structure \mathcal{K} , as described above, is a maximal arc.*

Proof. We will consider three lines in turn:

1. The line at infinity, l_∞ , is external to \mathcal{K} since \mathcal{K} has been expressed in non-homogeneous co-ordinates, and thus lie within the affine part of the projective plane.
2. Let g be a line, other than l_∞ , and suppose firstly that g passes through the origin $(0, 0)$. So g has equation $y = mx$ or $x = 0$. We substitute each of these into $\phi(x, y)$ in turn, giving

$$\begin{aligned}\phi(x, y) &= ax^2 + hx(mx) + b(mx)^2 \\ &= ax^2 + hmx^2 + bm^2x^2 \\ &= (a + hm + bm^2)x^2\end{aligned}$$

and

$$\phi(x, y) = by^2,$$

respectively. Let G be the set of values of $\phi(x, y)$ at the affine points of g . Then G is the set of values of the expressions $a'x^2$ or $a'y^2$ (for $a' = a + hm + bm^2$ and $a' = b$), respectively. Suppose $a' = 0$. Then $\phi(x, y) = 0$ for values of (x, y) other than $(0, 0)$. But $\phi(x, y)$ is irreducible, so we have a contradiction. Therefore a' will never be zero. Then, every element of $GF(q)$ belongs to G , and occurs at just one point of g , by Lemma 5.3. Since n of these elements belong to H , it follows that g meets \mathcal{K} in exactly n points.

3. Now suppose g does not pass through the origin. We know that G is the set of values of a quadratic, obtained by substituting $y = mx + c$, or $x = c$ into $\phi(x, y)$. By Lemma 5.4, we know that the range of a quadratic is either a subgroup of index two in A , or the second coset of that subgroup. Since g does not pass through the origin, the value 0 does not belong to G . It follows that G is, in A , the complement of a subgroup (G' , say) of index two. It also follows that each element of G occurs at just two points of g .

Consider A as a vector space of dimension h over $GF(2)$, and recall $n = 2^r$. So G' is a subspace of A of dimension $h-1$, that is, a hyperplane in A . Similarly, H is a subspace of A of dimension r . We are interested in $G \cap H$, but will first consider $G' \cap H$. Since G' is a hyperplane, either

- (a) H is wholly contained in G' , or
- (b) H intersects G' in a space of dimension $r - 1$.

Because G and G' are complements, the first case implies H and G are disjoint. In the second case, $G' \cap H$ is a space of dimension $r - 1$ over $GF(2)$, and thus has

$$2^{r-1} = \frac{2^r}{2} = \frac{n}{2}$$

points. The complement G , in this case, also contains $\frac{n}{2}$ points. Finally, then, g and \mathcal{K} are either disjoint or have n common points.

So, every line in $PG(2, q)$ intersects \mathcal{K} in zero or n points. Therefore \mathcal{K} is a maximal arc. □

5.4 Geometry of the Denniston arcs

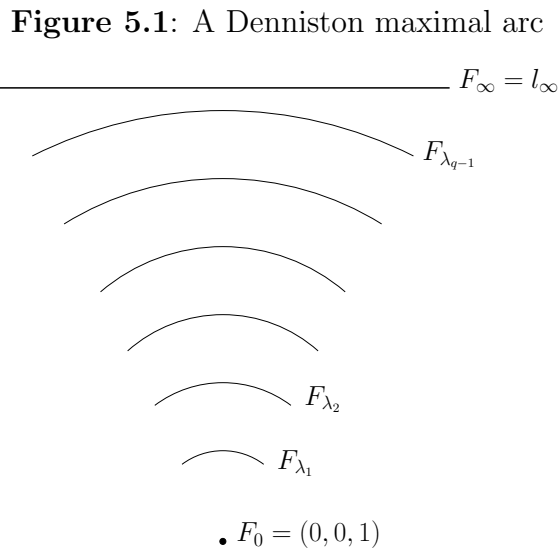
Denniston arcs have a nice geometric representation. In this section, let $PG(2, q)$ be co-ordinatised by homogeneous co-ordinates over $GF(q)$. So the points of $PG(2, q)$ are represented by $\langle(x, y, z)\rangle$, $x, y, z \in GF(q)$ and $(x, y, z) \neq (0, 0, 0)$, and the lines of $PG(2, q)$ by $\langle[a, b, c]\rangle$, $a, b, c \in GF(q)$ and $[a, b, c] \neq [0, 0, 0]$. A point and a line are incident if $(x, y, z) \cdot [a, b, c] = 0$.

We can now represent the quadratic form $\phi(x, y)$ in Section 5.3 as a set of conics in $PG(2, q)$ as follows:

$$F_\lambda : ax^2 + hxy + by^2 + \lambda z^2 = 0, \quad \lambda \in GF(q) \cup \{\infty\}.$$

Then F_0 is the point $(0, 0, 1)$ and F_∞ is the repeated line $z^2 = 0$. Recall that we have previously called $z = 0$ the line at infinity, l_∞ . Every other conic in this set is non-degenerate and has nucleus $(0, 0, h) \equiv (0, 0, 1)$. Furthermore,

the set forms a partition of $PG(2, q)$ (see [11] for more details), and the field $GF(q)$ parameterises the family of conics. Figure 5.1 shows a graphical representation of the family in the projective plane.



The curves F_i represent the family of conics in this particular construction. All maximal arcs from this family of conics contain the point F_0 . To form the maximal arc, we choose an appropriate subset of $n - 1$ of the remaining F_i .

Forming a Denniston maximal arc involves choosing a subgroup H of the additive group of the field $GF(q)$. This corresponds to choosing F_0 and a subset of $n - 1$ conics from the F_{λ_i} (see Figure 5.1). The arc \mathcal{K} is then the union of the points in those conics. Note that a Denniston maximal arc always contains the point $F_0 = (0, 0, 1)$.

Chapter 6

Thas (1974) maximal arcs

In this chapter we look at an interesting way to construct maximal arcs due to Thas [19]. Firstly, we will briefly consider some definitions that will be useful in the following sections. In Section 6.2 we introduce the Bruck-Bose construction described in [6]. Their construction provides a representation of a particular kind of projective plane called a *translation plane* which will be defined below. It is in the latter structure that we will construct a maximal arc.

6.1 Some preliminary definitions and results

Definition 6.1. A projective plane π is a *translation plane* if there is a line l in π such that the group of elations of π with axis l is transitive on the points of $\pi - l$ (see [11] and [16] for definitions of these terms). The line l is called a *translation line* of π .

Definition 6.2. A *spread* \mathcal{S} of $PG(n, q)$ by r -spaces is a set of r -spaces which partitions $PG(n, q)$. \mathcal{S} is often called an *r -spread*, and when $r = 1$ this is abbreviated to a *spread*.

We can show that there exists a spread in $PG(3, q)$. This was originally proved in [6], but we supply a different proof here. To construct a spread in $PG(3, q)$, we embed $PG(3, q)$ in $PG(3, q^2)$ as follows. Points in $PG(3, q^2)$

have homogeneous co-ordinates (x_0, x_1, x_2, x_3) , $x_i \in GF(q^2)$ and x_i not all zero, such that $\rho(x_0, x_1, x_2, x_3) \equiv (x_0, x_1, x_2, x_3)$ for all $\rho \in GF(q^2) = \{0\}$.

Definition 6.3. We can obtain $PG(3, q)$ by restricting these co-ordinates so that $x_i \in GF(q)$. In this way we say that $PG(3, q)$ can be *naturally embedded* in $PG(3, q^2)$. $PG(3, q)$ is called a *Baer subspace* of $PG(3, q^2)$.

Definition 6.4. Let α be a plane in $PG(3, q)$ where α is the set of points (x_0, x_1, x_2, x_3) , $x_i \in GF(q)$, that satisfies the equation

$$a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3 = 0,$$

where $a_i \in GF(q)$. We can *expand* α to be a plane of $PG(3, q^2)$ by allowing the x_i to be elements of $GF(q^2)$. The expanded plane is then called a *plane of $PG(3, q)$* .

Note that a plane in $PG(3, q^2)$ must meet $PG(3, q)$ in a subspace (either a plane, a line, a point or ϕ). So a *plane of $PG(3, q)$* , as defined here, is a plane of $PG(3, q^2)$ that meets $PG(3, q)$ in a plane.

We will count some of the objects and their relations in $PG(3, q)$ for use shortly. Extending this to counts for $PG(3, q^2)$ is straightforward, and both are summarised in Table 6.1. Firstly, $PG(3, q)$ contains $q^3 + q^2 + q + 1$ points by virtue of being a projective 3-space, and hence $q^3 + q^2 + q + 1$ planes by the principle of duality. There are $q + 1$ points on a line of $PG(3, q)$, since a line is a 1-dimensional subspace. Hence there are $q + 1$ planes through a line by duality. There are $q^2 + q + 1$ points in a plane of $PG(3, q)$, since a plane is a 2-dimensional subspace, so, by duality again, there are $q^2 + q + 1$ planes through a point. The number of lines in a plane in $PG(3, q)$ is the number of lines in a 2-dimensional subspace: we know that by duality in such a space, the number of lines is $q^2 + q + 1$. Then, by duality in $PG(3, q)$, we have $q^2 + q + 1$ lines through a point. Finally, we count the number of lines by

counting tuples (P, l) of points P on lines l in two different ways:

$$\begin{aligned} \text{total points} \times \text{lines on a point} &= \text{total lines} \times \text{points on a line} \\ \frac{(q^3 + q^2 + q + 1)(q^2 + q + 1)}{q + 1} &= \text{total lines} \\ \text{total lines} &= q^4 + q^3 + 2q^2 + q + 1. \end{aligned}$$

Obviously, these results can be extended to $PG(3, q^2)$ by substituting q^2 for q in each case.

Table 6.1: Counts of objects in $PG(3, q)$ and $PG(3, q^2)$

Object	$PG(3, q)$	$PG(3, q^2)$
points	$q^3 + q^2 + q + 1$	$q^6 + q^4 + q^2 + 1$
lines	$q^4 + q^3 + 2q^2 + q + 1$	$q^8 + q^6 + 2q^4 + q^2 + 1$
planes	$q^3 + q^2 + q + 1$	$q^6 + q^4 + q^2 + 1$
points on a line	$q + 1$	$q^2 + 1$
points on a plane	$q^2 + q + 1$	$q^4 + q^2 + 1$
lines on a point	$q^2 + q + 1$	$q^4 + q^2 + 1$
lines on a plane	$q^2 + q + 1$	$q^4 + q^2 + 1$
planes on a point	$q^2 + q + 1$	$q^4 + q^2 + 1$
planes on a line	$q + 1$	$q^2 + 1$

Next we will show how a line of $PG(3, q^2)$ can meet the Baer subspace $PG(3, q)$.

Lemma 6.1. *If a line l of $PG(3, q^2)$ intersects $PG(3, q)$ in two points then l intersects $PG(3, q)$ in $q + 1$ points.*

Proof. Let l be a line in $PG(3, q^2)$. Suppose l intersects $PG(3, q)$ in two points, P and Q . Then PQ is a line in $PG(3, q)$ and $|PQ| = q + 1$. So l intersects $PG(3, q)$ in $q + 1$ points. \square

Corollary 6.2. *A line of $PG(3, q^2)$ meets $PG(3, q)$ in 0, 1 or $q + 1$ points.*

Proof. A line l of $PG(3, q^2)$ can meet $PG(3, q)$ in at most $q + 1$ points. If l meets $PG(3, q)$ in more than one point, it meets $PG(3, q)$ in $q + 1$ points by Lemma 6.1. So l can only meet $PG(3, q)$ in 0, 1 or $q + 1$ points. \square

Definition 6.5. Let l be a line of $PG(3, q^2)$. We will call l a *line of $PG(3, q)$* if $|l \cap PG(3, q)| = q + 1$.

Now we will count the number of lines of $PG(3, q^2)$ which meet $PG(3, q)$ in $q + 1$, 1 and 0 points respectively.

Lemma 6.3. *In $PG(3, q^2)$, there are:*

1. $q^4 + q^3 + 2q^2 + q + 1$ lines meeting $PG(3, q)$ in $q + 1$ points,
2. $q^7 + q^6 + q^5 - q^3 - q^2 - q$ lines meeting $PG(3, q)$ in 1 point, and
3. $q^8 - q^7 - q^5 + q^4$ lines meeting $PG(3, q)$ in 0 points.

Proof.

1. There are $q^4 + q^3 + 2q^2 + q + 1$ lines in $PG(3, q)$. Each of these can be extended to a line in $PG(3, q^2)$, so there are $q^4 + q^3 + 2q^2 + q + 1$ lines in $PG(3, q^2)$ meeting $PG(3, q)$ in $q + 1$ points.
2. Consider a point $P \in PG(3, q)$. As a point of $PG(3, q)$, there are $q^2 + q + 1$ lines of $PG(3, q)$ through P . As a point of $PG(3, q^2)$, there are $q^4 + q^2 + 1$ lines of $PG(3, q^2)$ through P . So there are

$$q^4 + q^2 + 1 - (q^2 + q + 1) = q^4 - q$$

lines in $PG(3, q^2)$ meeting $PG(3, q)$ in just the point P . We have $q^3 + q^2 + q + 1$ such points P , so there are

$$(q^4 - q)(q^3 + q^2 + q + 1) = q^7 + q^6 + q^5 - q^3 - q^2 - q$$

lines in $PG(3, q^2)$ meeting $PG(3, q)$ in 1 point.

3. There are a total of $q^8 + q^6 + 2q^4 + q^2 + 1$ lines in $PG(3, q^2)$. The number of lines not meeting $PG(3, q)$ in 1 or $q + 1$ points is

$$\begin{aligned} & (q^8 + q^6 + 2q^4 + q^2 + 1) - (q^7 + q^6 + q^5 - q^3 - q^2 - q) - \\ & (q^4 + q^3 + 2q^2 + q + 1) \\ = & q^8 - q^7 - q^5 + q^4. \end{aligned}$$

So the number of lines in $PG(3, q^2)$ meeting $PG(3, q)$ in 0 points is $q^8 - q^7 - q^5 + q^4$.

□

We will now consider planes in $PG(3, q)$.

Definition 6.6. Let π be a plane of order q^2 . A subplane β of π of order q is called a *Baer subplane*.

We need a preliminary result about Baer subplanes.

Lemma 6.4. *Let π be a plane of order q^2 and let β be a Baer subplane of π . Any line in π meets β in one or $q + 1$ points.*

Proof. Consider a point P in $\pi - \beta$. Suppose P lies on the extension of two lines a and b of β into π . Then a and b restricted to β do not intersect in β , which is a contradiction since β is a projective plane. Thus P lies on at most 1 line of β extended into π . Suppose P lies on no such lines. Then the line joining P to every point in β is a distinct line in π . Thus there exist $q^2 + q + 1$ lines in π through P , but this is a contradiction, since π is a projective plane of order q . Therefore P lies on exactly one line of β extended into π .

Now let a be the single line of β containing P . This accounts for $q + 1$ points of β . The lines joining the remaining q^2 points of β and P contain only one point in β . So we have these q^2 lines and a passing through P . This is precisely the number of lines passing through P , since π is a projective plane of order q^2 . Therefore any line in π meets β in one or $q + 1$ points. □

We will now prove some results about lines in planes of $PG(3, q)$.

Lemma 6.5. *Let l be a line that is disjoint from $PG(3, q)$. Then l lies in no plane of $PG(3, q)$.*

Proof. Suppose l lies in a plane α of $PG(3, q)$ and let α' be α restricted to $PG(3, q)$. Then $\alpha \cong PG(2, q^2)$, and α' is a Baer subplane of α . Every line in a plane meets a Baer subplane in 1 or $q + 1$ points, by Lemma 6.4. Hence we have a contradiction since l is disjoint from $PG(3, q)$. Therefore l lies in no plane of $PG(3, q)$. \square

Definition 6.7. Let l be a line of $PG(3, q^2)$ that meets $PG(3, q)$ in a unique point. We call l a *1-secant* of $PG(3, q)$.

Lemma 6.6. *Let l be a 1-secant of $PG(3, q)$. Then l cannot be contained in two distinct planes of $PG(3, q)$.*

Proof. Suppose l is contained in two distinct planes, α and β , of $PG(3, q)$. In a 3-space, two planes can only intersect in a line or a plane, so $l = \alpha \cap \beta$. But $\alpha \cap \beta$ restricted to $PG(3, q)$ is a line in $PG(3, q)$, so $|l \cap PG(3, q)| > 1$. This is a contradiction since l is a 1-secant. Therefore, l cannot be contained in two distinct planes of $PG(3, q)$. \square

Consider a plane α of $PG(3, q)$. Note that $\alpha \cong PG(2, q^2)$. We can count the total number of 1-secants in this expanded plane. Let P be a point of α . In $PG(2, q^2)$, there are $q^2 + 1$ lines through P , but $q + 1$ of these lines correspond to lines in $PG(2, q)$ through P . So there are $q^2 - q$ 1-secants in α through P . There are $q^2 + q + 1$ such points P , so there are

$$(q^2 + q + 1)(q^2 - q) = q^4 - q$$

1-secants in the expanded plane. Then, there are $q^3 + q^2 + q + 1$ such expanded planes, giving $(q^4 - q)(q^3 + q^2 + q + 1) = q^7 + q^6 + q^5 - q^3 - q^2 - q$ 1-secants lying in expanded planes. Hence, we can prove the following Lemma.

Lemma 6.7. *Let l be a 1-secant of $PG(3, q)$. Then l lies in a unique plane of $PG(3, q)$.*

Proof. There are $q^7 + q^6 + q^5 - q^3 - q^2 - q$ lines in $PG(3, q^2)$ meeting $PG(3, q)$ in one point, by Lemma 6.3. We have precisely this number of 1-secants lying in planes of $PG(3, q)$, and by Lemma 6.6, l cannot lie in two distinct planes. Therefore, l lies in a unique plane of $PG(3, q)$. \square

We need some further results involving lines in both spaces.

Lemma 6.8. *Let l_1 and l_2 be distinct lines of $PG(3, q)$ that intersect in a point P . Then P is a point of $PG(3, q)$.*

Proof. Let $\alpha = l_1 \oplus l_2$ be the plane spanned by the lines l_1 and l_2 . The plane α is a plane of $PG(3, q)$. Suppose $P \in PG(3, q^2) - PG(3, q)$. Then, as lines restricted to $PG(3, q)$, l_1 and l_2 do not intersect. This is a contradiction since α is a projective plane. Therefore P is a point of $PG(3, q)$. \square

On every line of $PG(3, q)$ there are $q + 1$ points in $PG(3, q)$ and hence $q^2 + 1 - (q + 1) = q^2 - q$ points not in $PG(3, q)$. There are $q^4 + q^3 + 2q^2 + q + 1$ lines in $PG(3, q)$, so in total there are

$$(q^4 + q^3 + 2q^2 + q + 1)(q^2 - q) = q^6 + q^4 - q^3 - q$$

points of $PG(3, q^2) - PG(3, q)$ on lines of $PG(3, q)$. Hence we have the following result.

Lemma 6.9. *Let P be a point of $PG(3, q^2) - PG(3, q)$. P is incident with exactly one line of $PG(3, q)$.*

Proof. There are $q^6 + q^4 + q^2 + 1$ points in $PG(3, q^2)$ and $q^3 + q^2 + q + 1$ points in $PG(3, q)$, hence $q^6 + q^4 - q^3 - q$ points in $PG(3, q^2) - PG(3, q)$. This is precisely the number of points in $PG(3, q^2) - PG(3, q)$ on lines of $PG(3, q)$. Therefore P is incident with exactly one line of $PG(3, q)$. \square

Lemma 6.10. *Let P be a point of $PG(3, q^2) - PG(3, q)$. P is incident with $q^3 + q^2$ 1-secants of $PG(3, q)$ and $q^4 - q^3$ lines which are disjoint from $PG(3, q)$.*

Proof. P lies on exactly one line of $PG(3, q)$ by Lemma 6.9. On this line are $q + 1$ points in $PG(3, q)$. Joining P to the remaining $q^3 + q^2$ points in $PG(3, q)$ gives all of the 1-secants through P . There are $q^4 + q^2 + 1$ lines of $PG(3, q^2)$ through P . Since one of those lines is a line of $PG(3, q)$, and $q^3 + q^2$ are 1-secants,

$$q^4 + q^2 + 1 - 1 - (q^3 + q^2) = q^4 - q^3$$

lines through P are disjoint from $PG(3, q)$. □

Finally we can construct a spread in $PG(3, q)$.

Lemma 6.11. *Let m be a line in $PG(3, q^2)$ such that m is disjoint from $PG(3, q)$. Let \mathcal{S} be the collection of $q^2 + 1$ lines of $PG(3, q)$ incident with m (one through each point of m). Then \mathcal{S} is a spread of $PG(3, q)$.*

Proof. We will show that the lines in \mathcal{S} are mutually skew and that each point in $PG(3, q)$ is incident with a unique line in \mathcal{S} .

1. Suppose there exist distinct lines $a, b \in \mathcal{S}$ such that $a \cap b = \{P\}$. By Lemma 6.8, $P \in PG(3, q)$. Let $A = a \cap m$ and $B = b \cap m$ be the points of intersection of a and b with m . Then A, B and P span a plane, α , and α is a plane of $PG(3, q)$ since $a, b \in PG(3, q)$. So m is contained in a plane of $PG(3, q)$. This is a contradiction by Lemma 6.5. Therefore the lines in \mathcal{S} are mutually skew.
2. There are $q^2 + 1$ lines in \mathcal{S} . Each of these lines restricted to $PG(3, q)$ contains $q + 1$ points, so there are $(q^2 + 1)(q + 1) = q^3 + q^2 + q + 1$ points in $PG(3, q)$ on the lines of \mathcal{S} . This is precisely the number of points in $PG(3, q)$, so each point in $PG(3, q)$ is incident with a unique line in \mathcal{S} .

□

The spread \mathcal{S} is known as the *regular* spread of $PG(3, q)$.

6.2 Constructing the translation plane

Let H be a fixed, 3-dimensional subspace of $PG(4, q)$. So $H \cong PG(3, q)$, and H is a hyperplane of $PG(4, q)$. Let \mathcal{S} be a spread of H . Construct an incidence structure $\bar{\pi} = \bar{\pi}(\mathcal{S})$ as follows:

- The points of $\bar{\pi}$ are the points of $PG(4, q) - H$.
- The lines of $\bar{\pi}$ are the planes of $PG(4, q)$ that intersect H in an element of \mathcal{S} .
- The incidence relation of $\bar{\pi}$ is that induced by incidence in $PG(4, q)$.

We can prove that the plane $\bar{\pi} = \bar{\pi}(\mathcal{S})$ is an affine plane.

Lemma 6.12. [6] *The incidence structure $\bar{\pi} = \bar{\pi}(\mathcal{S})$ is an affine plane.*

Proof. We will show that $\bar{\pi}$ satisfies the properties of an affine plane.

1. Let X, Y be two points of $\bar{\pi}$, so $X, Y \in PG(4, q) - H$. There exists a unique line $l \in PG(4, q)$ through X and Y . Now l is not in H , therefore l meets H in a point. This point lies on exactly one element s of the spread \mathcal{S} . Then the lines l and s span a unique plane in $PG(4, q) - H$ that contains X and Y . This plane is incident with the spread element s , so there exists a unique line in $\bar{\pi}$ passing through the points X and Y .
2. Let a, b be two distinct lines of $\bar{\pi}$ (so a and b are planes in $PG(4, q)$). Consider the case where a and b contain the same member s of \mathcal{S} , and assume a and b have some common point $P \in \bar{\pi}$. The span of s and P is a unique plane, thus a and b coincide: a contradiction. So a and b can have no point of $\bar{\pi}$ in common. Now consider the case where a and b contain different elements s_1 and s_2 of \mathcal{S} . s_1 and s_2 are skew, and so span the 3-space H . Additionally, a has at least one point outside of

H , so a and b must span a 4-space. By the Dimension Theorem,

$$\begin{aligned}\dim a \cap b &= \dim a + \dim b - \dim a \oplus b \\ &= 2 + 2 - 4 \\ &= 0.\end{aligned}$$

So in $PG(4, q)$, $a \cap b$ is a point, and this point is not in H . Therefore, in $\bar{\pi}$, $a \cap b$ is zero or one points. So two distinct lines of $\bar{\pi}$ meet in zero or one points.

3. Let X be a point of $\bar{\pi}$ and a a line of $\bar{\pi}$ not through X . Let s be the element of \mathcal{S} coincident with a . Let $b = X \oplus s$, so b is a line of $\bar{\pi}$ through X . As above, a and b have no point of $\bar{\pi}$ in common. Any other line $c \in \bar{\pi}$ containing X but distinct from b will contain some other element $s' \in \mathcal{S}$. So a and c contain no common point in H , but since they are 2-dimensional subspaces of $PG(4, q)$, they share at least one common point. Therefore, b is the unique line of $\bar{\pi}$ through X parallel to a .

□

The affine plane $\bar{\pi} = \bar{\pi}(\mathcal{S})$ can be uniquely completed to a projective plane, π . Each member $s \in \mathcal{S}$ corresponds to a set of parallel lines in π , namely those lines that correspond to planes of $PG(4, q)$ meeting H in s . So we adjoin each s to $\bar{\pi}$ as a *point at infinity*. Further, we adjoin the spread \mathcal{S} itself to $\bar{\pi}$ as a *line at infinity*, l_∞ . The resulting incidence structure π is a projective plane.

Lemma 6.13. [6] *The incidence structure π obtained by adjoining the spread \mathcal{S} to the affine plane $\bar{\pi} = \bar{\pi}(\mathcal{S})$ (in the manner described above) is a projective plane.*

Proof. We will show the π satisfies the properties of a projective plane.

1. Let X, Y be two distinct points in π .

- (a) Suppose $X, Y \in PG(4, q) - H$. By Lemma 6.12, there exists a unique line of π joining X and Y .
 - (b) Suppose $X \in PG(4, q) - H$ and Y corresponds to a line $s \in \mathcal{S}$ (or vice versa). Then the span of X and Y in $PG(4, q)$ is a plane passing through an element of \mathcal{S} , namely s . So, again, there exists a unique line of π joining X and Y .
 - (c) Suppose $X, Y \in \mathcal{S}$. Then X and Y both lie on l_∞ , and, again, there exists a unique line of π joining X and Y .
2. Let a, b be two distinct lines in π . We can now use the same argument as in Lemma 6.12 (with the exception that a and b containing the same member s of \mathcal{S} implies they *do* have a point in π in common, namely s) to show that a and b meet in a unique point.
3. Let l be a line in π . Then l contains

$$(q^2 + q + 1) - (q + 1) + 1 = q^2 + 1$$

points (where $(q^2 + q + 1)$ points are by virtue of l being a plane in $PG(4, q) - H$, we subtract $(q + 1)$ points being the line $s \in \mathcal{S}$ incident with l and then add the point at infinity s). So, every line l in π contains at least three points.

4. There clearly exists at least three non-collinear points.

□

Corollary 6.14. *The projective plane π has order q^2 .*

Proof. Let q' be the order of π , and let l be a line in π . Then l contains $q' + 1$ points (since π is a projective plane), but l contains $q^2 + 1$ points by Lemma 6.13. So, $q' + 1 = q^2 + 1$, and hence $q' = q^2$. □

Bruck and Bose showed that the projective plane π is a translation plane. Further, they considered a more general form of the construction: a $(2t - 1)$ -dimensional subspace of a $2t$ -dimensional projective space, giving a translation plane of order q^t (see [6]). This construction was earlier performed

algebraically in the vector space setting by André [1]. In the next section we will examine how a maximal arc can be constructed in the translation plane π .

6.3 Constructing the Thas (1974) maximal arcs

We can now construct a maximal arc in the following way.

Theorem 6.15. [19] *Let the 3-space $PG(3, q)$ be embedded as a hyperplane H in the 4-space $PG(4, q)$. Consider an ovoid \mathcal{O} and a spread \mathcal{S} of H such that each line of \mathcal{S} has exactly one point in common with \mathcal{O} . Now let X be a point of $PG(4, q) - H$. Let \mathcal{K} be the set of points of $PG(4, q) - H$ which are collinear with X and a point of \mathcal{O} (see Figure 6.1). Then \mathcal{K} is a maximal $\{q^3 - q^2 + q; q\}$ -arc in the translation plane π defined by the spread \mathcal{S} .*

Proof. Firstly we will determine the number of points in \mathcal{K} . The number of lines in \mathcal{S} is equal to the number of points in H divided by the number of points on a line:

$$\frac{q^3 + q^2 + q + 1}{q + 1} = q^2 + 1.$$

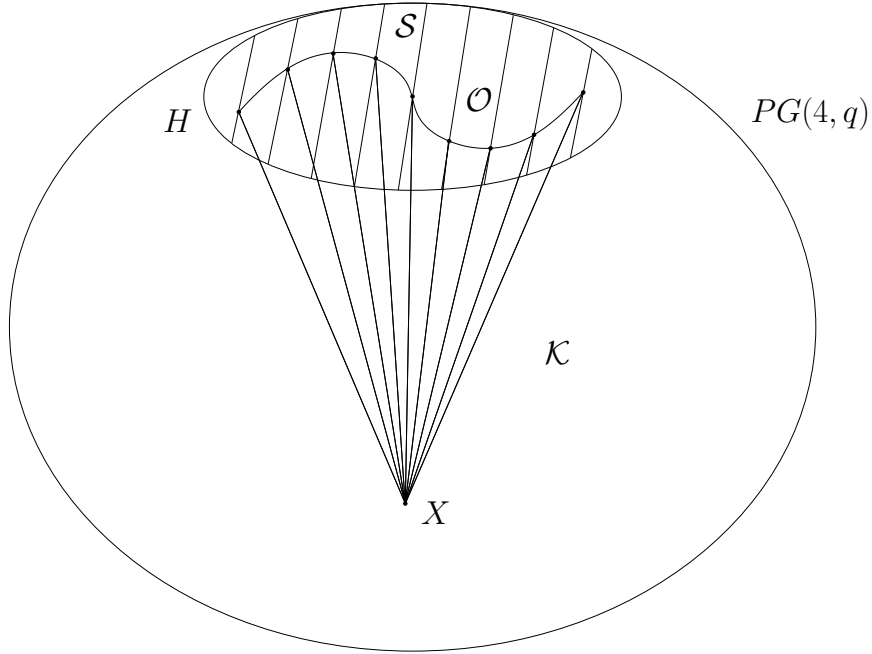
Each line $s_i \in \mathcal{S}$, $i = 1, \dots, q^2 + 1$, is incident with a point O_i of \mathcal{O} , and it is the $q^2 + 1$ lines $O_i X$ whose points (with the exception of O_i itself) that comprise \mathcal{K} . So, excluding O_i and without overcounting X , the number of points in \mathcal{K} is:

$$\begin{aligned} (q^2 + 1)(q - 1) + 1 &= q^3 - q^2 + q - 1 + 1 \\ &= q^3 - q^2 + q. \end{aligned}$$

Now, let l be a line of π , not the line at infinity, l_∞ (since l_∞ has no points in common with \mathcal{K}). We then consider the two cases:

1. Suppose $X \in l$. Then, in $PG(4, q)$, l corresponds to a plane α , and $\alpha \cap H$ is a line $s \in \mathcal{S}$. The line s contains a unique point $O \in \mathcal{O}$.

Figure 6.1: A Thas (1974) maximal arc

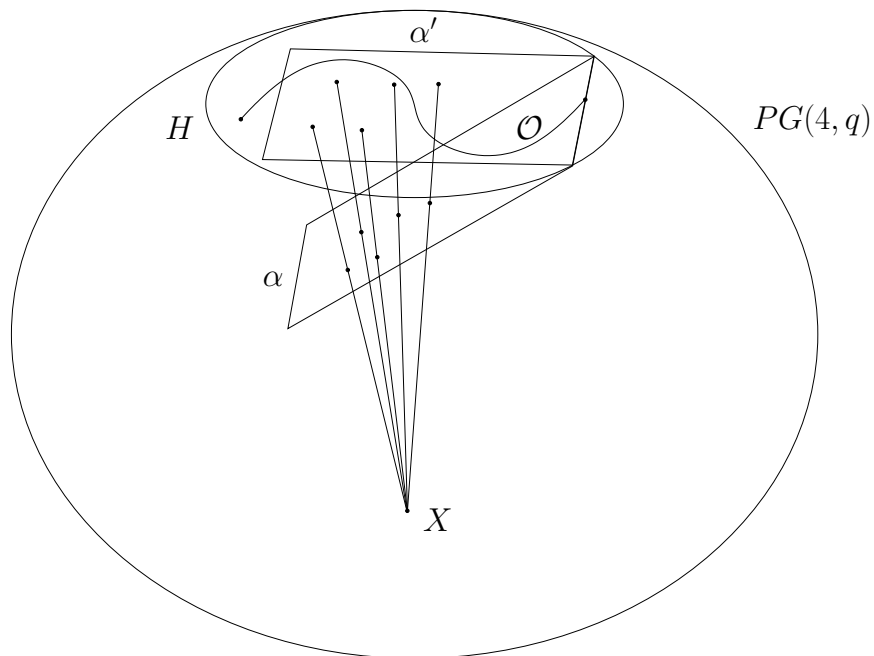


The hyperplane $H = PG(3, q)$ is embedded in $PG(4, q)$. Each line of the spread \mathcal{S} has exactly one point in common with the ovoid \mathcal{O} . Let X be a point in $PG(4, q)$ not in H . Then \mathcal{K} is the Thas (1974) maximal arc.

Hence α meets \mathcal{K} in the q points in $PG(4, q) - H$ lying on the line joining X and O . Further, for each point $O_i \in \mathcal{O}$, by construction, $\alpha \cap O_i X = \{X\}$ or $O_i X$ for $i = 1, \dots, q^2 + 1$, so α contains no other points of \mathcal{K} . Therefore, l meets \mathcal{K} in q points.

2. Suppose $X \notin l$. Consider the projection through X of the plane α in $PG(4, q)$ representing l onto H . We construct this projection by passing lines in $PG(4, q)$ from X through every point Q_i in α and finding their intersection with H . (Figure 6.2 demonstrates the idea using five lines from X through α .) Now, let $\mathcal{W} = X \oplus \alpha$ be the space spanned by these lines and the plane α . Since \mathcal{W} and H are both subspaces of $PG(4, q)$, they can together span a space of at most dimension 4. The dimension of both \mathcal{W} and H is 3, so together \mathcal{W} and H must span a

Figure 6.2: Projection of a plane through a point



Five of the projection lines from X through the plane α are shown. The set of projection lines form the plane α' by their intersection with H .

space of at least dimension 3. So, by the Dimension Theorem, we have:

$$\begin{aligned} \dim \mathcal{W} \cap H &= \dim \mathcal{W} + \dim H - \dim \mathcal{W} \oplus H \\ &= 3 + 3 - 4 \quad \text{or} \quad 3 + 3 - 3 \\ &= 2 \quad \text{or} \quad 3. \end{aligned}$$

For $\dim \mathcal{W} \cap H = 3$, we would need $X \in H$. Since $X \notin H$, $\dim \mathcal{W} \cap H = 2$. So the projection through X of the plane α representing l onto H is then a plane α' in H . The intersection of α' with \mathcal{O} will contain 1 or $q + 1$ points (Theorem 3.20). In the first case, l is external to \mathcal{K} because the point of intersection $O = \alpha \cap H \cap \mathcal{O} \in \mathcal{O}$ is not in \mathcal{K} . In the second case, one of the points in $\alpha' \cap \mathcal{O}$ is also in the plane α . The remaining q points in $\alpha' \cap \mathcal{O}$ are on projection lines from X through α . There are q such projection lines, and hence q such intersections, so l

meets \mathcal{K} in q points.

So every line l in π meets \mathcal{K} in 0 or q points. Therefore \mathcal{K} is a maximal arc. \square

Finally, we should ask whether an appropriate ovoid and spread actually exist.

Theorem 6.16. [19] *In $PG(3, q)$, q even, there exist an ovoid \mathcal{O} and a spread \mathcal{S} of $PG(3, q)$ such that each line of \mathcal{S} has exactly one point in common with \mathcal{O} .*

Theorem 6.17. [5] *In $PG(3, q)$, q odd, there exists no such ovoid and spread.*

The immediate consequence of these two theorems is that Thas maximal arcs exist only in the case where q is even.

Chapter 7

Mathon maximal arcs

In this chapter we will look at a relatively recent construction of maximal arcs due to Mathon [18]. The construction relies heavily on certain sets of conics in field planes, and we will cover the theory in Section 7.2. Section 7.3 gives the basis of an example of constructing a Mathon maximal arc.

7.1 Some definitions from field theory

Let $F = GF(q)$ be a finite field, where $q = p^h$ for p a prime.

Definition 7.1. An *automorphism* σ of F is a permutation of F such that

$$\sigma(x + y) = \sigma(x) + \sigma(y), \quad \sigma(xy) = \sigma(x)\sigma(y)$$

for all $x, y \in F$.

The set of automorphisms of F forms a group, denoted $\text{Aut}(F)$. This group is isomorphic to \mathbb{Z}_h , and is generated by the *Frobenius automorphism* ϕ , where $\phi(x) = x^p$ for $x \in GF(q)$.

Let $L = GF(q)$ and $K = GF(p)$ be fields where $q = p^h$.

Definition 7.2. The trace $\text{Tr}_{L/K} : L \rightarrow L$ is given by

$$\text{Tr}_{L/K}(t) = \sum_{\sigma \in \text{Aut}(L)} \sigma(t) = t + t^p + t^{p^2} + \cdots + t^{p^{h-1}}.$$

The image of $\text{Tr}_{L/K}$ is K . The trace has the following properties:

1. $\text{Tr}_{L/K}(\alpha + \beta) = \text{Tr}_{L/K}(\alpha) + \text{Tr}_{L/K}(\beta)$ for all $\alpha, \beta \in L$.
2. $\text{Tr}_{L/K}(x\alpha) = x \text{Tr}_{L/K}(\alpha)$ for $\alpha \in L, x \in K$, and provided $K \subseteq L$.
3. $\text{Tr}_{L/K}(x) = hx$ for $x \in K$.
4. $\text{Tr}_{L/K}(\alpha)^p = \text{Tr}_{L/K}(\alpha)$ for $\alpha \in L$.

7.2 Sets of conics

Consider $PG(2, 2^m)$ co-ordinatised by homogenous co-ordinates in the usual way. Let \mathcal{C} be the set of conics

$$F_{\alpha, \beta, \lambda} : \alpha x^2 + xy + \beta y^2 + \lambda z^2 = 0, \quad \lambda \in GF(2^m) \cup \{\infty\},$$

where α, β are non-zero elements of $GF(2^m)$ such that the quadratic polynomial $\alpha\zeta^2 + \zeta + \beta$ is irreducible over $GF(2^m)$. This condition is equivalent to requiring that α, β satisfy

$$\text{Tr}_{2^m/2}(\alpha\beta) = 1, \tag{7.1}$$

where we will use $\text{Tr}_{2^m/2}$ to denote $\text{Tr}_{GF(2^m)/GF(2)}$ for the remainder of this chapter.

Notice that $F_{\alpha, \beta, 0} := F_0$ is the point $(0, 0, 1)$, $F_{\alpha, \beta, \infty} := F_\infty$ is the line at infinity, $z^2 = 0$, and every other conic is non-degenerate with nucleus F_0 . Notice also that for fixed α and β satisfying $\text{Tr}_{2^m/2}(\alpha\beta) = 1$ the corresponding conics in \mathcal{C} are isomorphic to a set of conics constructed as in Denniston [9] (see Section 5.3). Specifically, consider a collineation H that maps

$$\begin{aligned} x &\mapsto x' = x\sqrt{\alpha} \\ y &\mapsto y' = y\sqrt{\beta} \\ z &\mapsto z' = z. \end{aligned}$$

Now, $\alpha x^2 + xy + \beta y^2 + \lambda z^2 = x'^2 + \frac{x'y'}{\sqrt{\alpha\beta}} + y'^2 + \lambda z'^2$, so under H , $\alpha x^2 + xy + \beta y^2 + \lambda z^2 \mapsto x^2 + \frac{xy}{\sqrt{\alpha\beta}} + y^2 + \lambda z^2$ which is a conic in the standard pencil.

We now define a composition operation on two non-degenerate conics. Let $F_{\alpha,\beta,\lambda}$ and $F_{\alpha',\beta',\lambda'}$ be two conics in \mathcal{C} , with $\lambda \neq \lambda'$. Define the composition of these two conics:

$$F_{\alpha \oplus \alpha', \beta \oplus \beta', \lambda \oplus \lambda'} = F_{\alpha,\beta,\lambda} \oplus F_{\alpha',\beta',\lambda'}$$

where

$$\alpha \oplus \alpha' = \frac{\alpha\lambda + \alpha'\lambda'}{\lambda + \lambda'}, \quad \beta \oplus \beta' = \frac{\beta\lambda + \beta'\lambda'}{\lambda + \lambda'}, \quad \lambda \oplus \lambda' = \lambda + \lambda'.$$

The operation is commutative, since

$$\alpha \oplus \alpha' = \frac{\alpha\lambda + \alpha'\lambda'}{\lambda + \lambda'} = \frac{\alpha'\lambda' + \alpha\lambda}{\lambda' + \lambda} = \alpha' \oplus \alpha.$$

The operation is also associative, since

$$(\alpha \oplus \alpha') \oplus \alpha'' = \alpha \oplus (\alpha' \oplus \alpha'') = \frac{\alpha\lambda + \alpha'\lambda' + \alpha''\lambda''}{\lambda + \lambda' + \lambda''}.$$

Finally, the operation is idempotent in the first two parameters, since

$$F_{\alpha,\beta,\lambda} \oplus F_{\alpha,\beta,\lambda} = F_{\alpha,\beta,\lambda+\lambda}.$$

Note that the composition of two non-degenerate conics is not, in general, a non-degenerate conic.

Lemma 7.1. [18] *Two non-degenerate conics $F_{\alpha,\beta,\lambda}$, $F_{\alpha',\beta',\lambda'}$, $\lambda \neq \lambda'$ and their composition $F_{\alpha,\beta,\lambda} \oplus F_{\alpha',\beta',\lambda'}$ are mutually disjoint if $\text{Tr}_{2^m/2}((\alpha \oplus \alpha')(\beta \oplus \beta')) = 1$.*

Proof. We aim to map the three conics into a standard pencil. Let

$$A = \frac{\alpha'\lambda + \alpha\lambda'}{\lambda + \lambda'}, \quad B = \frac{\beta'\lambda + \beta\lambda'}{\lambda + \lambda'}, \quad C = \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + (\alpha\beta + \alpha'\beta')\lambda^2}{\lambda^2 + \lambda'^2},$$

and let

$$\begin{aligned}
\epsilon &= AB \\
&= \frac{\alpha'\lambda + \alpha\lambda'}{\lambda + \lambda'} \frac{\beta'\lambda + \beta\lambda'}{\lambda + \lambda'} \\
&= \frac{(\alpha'\lambda + \alpha\lambda')(\beta'\lambda + \beta\lambda')}{(\lambda + \lambda')^2} \\
&= \frac{\alpha'\beta'\lambda^2 + \alpha'\beta\lambda\lambda' + \alpha\beta'\lambda\lambda' + \alpha\beta\lambda'^2}{\lambda^2 + \lambda'^2} \\
&= \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + \alpha'\beta'\lambda^2 + \alpha\beta\lambda'^2}{\lambda^2 + \lambda'^2}. \tag{7.2}
\end{aligned}$$

Notice that

$$\begin{aligned}
\alpha\beta + C &= \alpha\beta + \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + (\alpha\beta + \alpha'\beta')\lambda^2}{\lambda^2 + \lambda'^2} \\
&= \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + \alpha\beta\lambda^2 + \alpha'\beta'\lambda^2 + \alpha\beta\lambda^2 + \alpha\beta\lambda'^2}{\lambda^2 + \lambda'^2} \\
&= \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + \alpha'\beta'\lambda^2 + \alpha\beta\lambda'^2}{\lambda^2 + \lambda'^2} \\
&= AB \quad (\text{by Equation 7.2}) \tag{7.3}
\end{aligned}$$

and that

$$\begin{aligned}
\alpha'\beta' + C &= \alpha'\beta' + \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + (\alpha\beta + \alpha'\beta')\lambda^2}{\lambda^2 + \lambda'^2} \\
&= \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + \alpha\beta\lambda^2 + \alpha'\beta'\lambda^2 + \alpha'\beta'\lambda^2 + \alpha'\beta'\lambda'^2}{\lambda^2 + \lambda'^2} \\
&= \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + \alpha\beta\lambda^2 + \alpha'\beta'\lambda'^2}{\lambda^2 + \lambda'^2}. \tag{7.4}
\end{aligned}$$

Now,

$$\begin{aligned}
(\alpha \oplus \alpha')(\beta \oplus \beta') &= \left(\frac{\alpha\lambda + \alpha'\lambda'}{\lambda + \lambda'} \right) \left(\frac{\beta\lambda + \beta'\lambda'}{\lambda + \lambda'} \right) \\
&= \frac{\alpha\beta\lambda^2 + \alpha\beta'\lambda\lambda' + \alpha'\beta\lambda\lambda' + \alpha'\beta'\lambda'^2}{\lambda^2 + \lambda'^2} \\
&= \frac{(\alpha\beta' + \beta\alpha')\lambda\lambda' + \alpha\beta\lambda^2 + \alpha'\beta'\lambda'^2}{\lambda^2 + \lambda'^2} \\
&= \alpha'\beta' + C \quad (\text{by Equation 7.4}). \tag{7.5}
\end{aligned}$$

Recall that $\text{Tr}_{2^m/2}(\alpha\beta) = \text{Tr}_{2^m/2}(\alpha'\beta') = 1$ (by Equation 7.1), and we have that

$$\begin{aligned}
\text{Tr}_{2^m/2}(\epsilon) &= \text{Tr}_{2^m/2}(AB) \\
&= \text{Tr}_{2^m/2}(\alpha\beta) + \text{Tr}_{2^m/2}(C) \quad (\text{by Equation 7.3}) \\
&= \text{Tr}_{2^m/2}(\alpha'\beta') + \text{Tr}_{2^m/2}(C) \\
&= \text{Tr}_{2^m/2}((\alpha \oplus \alpha')(\beta \oplus \beta')) \quad (\text{by Equation 7.5}) \\
&= 1.
\end{aligned}$$

This implies that both $A, B \neq 0$, and that $\text{Tr}_{2^m/2}(C) = 0$.

Consider a collineation H of $PG(2, 2^m)$ represented by the matrix

$$H = \begin{pmatrix} a & 0 & 0 \\ 0 & 1/a & 0 \\ ab & c/a & 1 \end{pmatrix}$$

which maps

$$\begin{aligned}
x &\mapsto x' = ax \\
y &\mapsto y' = \frac{y}{a} \\
z &\mapsto z' = abx + \frac{c}{a}y + z.
\end{aligned}$$

Let

$$a = \sqrt{A}, \quad b = \sqrt{\frac{\alpha + A}{A\lambda}}, \quad c = \sqrt{\frac{A(\beta + B)}{\lambda}}.$$

Then, we can observe the effect of the mapping H on the three conics $F_{\alpha,\beta,\lambda}$, $F_{\alpha',\beta',\lambda'}$ and $F_{\alpha,\beta,\lambda} \oplus F_{\alpha',\beta',\lambda'}$ by considering just the first:

$$\begin{aligned}
&\alpha x^2 + xy + \beta y^2 + \lambda z^2 \\
&= \frac{\alpha}{a^2}x'^2 + x'y' + \beta a^2 y'^2 + \lambda(bx' + cy' + z')^2 \\
&= \frac{\alpha}{A}x'^2 + x'y' + \beta A y'^2 + \lambda\left(\frac{\alpha + A}{A\lambda}x'^2 + \frac{A(B + \beta)}{\lambda}y'^2 + z'^2\right) \\
&= x'^2 + x'y' + \epsilon y'^2 + \lambda z'^2 \\
&= F_{1,\epsilon,\lambda}.
\end{aligned}$$

Similar calculations show that the coefficient of x'^2 will always map to 1, the coefficient of y'^2 will always map to ϵ , and the coefficient of z'^2 is unchanged by H . Thus, under H we have:

$$\begin{aligned} F_{\alpha,\beta,\lambda} &\longrightarrow F_{1,\epsilon,\lambda} \\ F_{\alpha',\beta',\lambda'} &\longrightarrow F_{1,\epsilon,\lambda'} \\ F_{\alpha,\beta,\lambda} \oplus F_{\alpha',\beta',\lambda'} &\longrightarrow F_{1,\epsilon,\lambda+\lambda'}. \end{aligned}$$

Since ϵ has trace 1, the three conics $F_{1,\epsilon,\lambda}$, $F_{1,\epsilon,\lambda'}$ and $F_{1,\epsilon,\lambda+\lambda'}$ are isomorphic to a subset of the standard pencil. Therefore, $F_{\alpha,\beta,\lambda}$, $F_{\alpha',\beta',\lambda'}$ and $F_{\alpha,\beta,\lambda} \oplus F_{\alpha',\beta',\lambda'}$ are mutually disjoint if $\text{Tr}_{2^m/2}((\alpha \oplus \alpha')(\beta \oplus \beta')) = 1$. \square

Notice that the collineation H in Lemma 7.1 is actually the *inverse* of the collineation quoted in Mathon's paper [18].

Now we define the notion of a closure.

Definition 7.3. A subset $\mathcal{F} \subset \mathcal{C}$ of non-degenerate conics is said to be *closed under composition* if $F_1, F_2 \in \mathcal{F} \Rightarrow F_1 \oplus F_2 \in \mathcal{F}$. The *closure* of a set of non-degenerate conics is the smallest closed set containing those conics.

Lemma 7.2. [18] *Let $F_1 = F_{\alpha_1,\beta_1,\lambda_1}$, $F_2 = F_{\alpha_2,\beta_2,\lambda_2}$ and $F' = F_{\alpha',\beta',\lambda'}$ be three non-degenerate conics. Then*

$$(F_1 \oplus F') \oplus (F_2 \oplus F') = F_1 \oplus F_2.$$

Proof. We can show this by expanding the expression on the left:

$$\begin{aligned} &(F_1 \oplus F') \oplus (F_2 \oplus F') \\ &= (F_{\alpha_1,\beta_1,\lambda_1} \oplus F_{\alpha',\beta',\lambda'}) \oplus (F_{\alpha_2,\beta_2,\lambda_2} \oplus F_{\alpha',\beta',\lambda'}) \\ &= F_{\alpha_1 \oplus \alpha', \beta_1 \oplus \beta', \lambda_1 \oplus \lambda'} \oplus F_{\alpha_2 \oplus \alpha', \beta_2 \oplus \beta', \lambda_2 \oplus \lambda'} \\ &= F_{\frac{\alpha_1 \lambda_1 + \alpha' \lambda'}{\lambda_1 + \lambda'}, \frac{\beta_1 \lambda_1 + \beta' \lambda'}{\lambda_1 + \lambda'}, \lambda_1 + \lambda'} \oplus F_{\frac{\alpha_2 \lambda_2 + \alpha' \lambda'}{\lambda_2 + \lambda'}, \frac{\beta_2 \lambda_2 + \beta' \lambda'}{\lambda_2 + \lambda'}, \lambda_2 + \lambda'} \\ &= F_{\frac{\alpha_1 \lambda_1 + \alpha' \lambda'}{\lambda_1 + \lambda'} \oplus \frac{\alpha_2 \lambda_2 + \alpha' \lambda'}{\lambda_2 + \lambda'}, \frac{\beta_1 \lambda_1 + \beta' \lambda'}{\lambda_1 + \lambda'} \oplus \frac{\beta_2 \lambda_2 + \beta' \lambda'}{\lambda_2 + \lambda'}, (\lambda_1 + \lambda') \oplus (\lambda_2 + \lambda')} \end{aligned} \tag{7.6}$$

At this point, observe that

$$\frac{\left(\frac{\alpha_1 \lambda_1 + \alpha' \lambda'}{\lambda_1 + \lambda'}\right) (\lambda_1 + \lambda') + \left(\frac{\alpha_2 \lambda_2 + \alpha' \lambda'}{\lambda_2 + \lambda'}\right) (\lambda_2 + \lambda')}{(\lambda_1 + \lambda') + (\lambda_2 + \lambda')} = \frac{\alpha_1 \lambda_1 + \alpha_2 \lambda_2}{\lambda_1 + \lambda_2},$$

and that

$$\frac{\left(\frac{\beta_1\lambda_1+\beta'\lambda'}{\lambda_1+\lambda'}\right)(\lambda_1+\lambda') + \left(\frac{\beta_2\lambda_2+\beta'\lambda'}{\lambda_2+\lambda'}\right)(\lambda_2+\lambda')}{(\lambda_1+\lambda') + (\lambda_2+\lambda')} = \frac{\beta_1\lambda_1 + \beta_2\lambda_2}{\lambda_1 + \lambda_2}.$$

So, continuing from Equation 7.6,

$$\begin{aligned} &= F_{\frac{\alpha_1\lambda_1+\alpha_2\lambda_2}{\lambda_1+\lambda_2}, \frac{\beta_1\lambda_1+\beta_2\lambda_2}{\lambda_1+\lambda_2}, \lambda_1+\lambda_2} \\ &= F_1 \oplus F_2 \end{aligned}$$

□

Lemma 7.3. [18] *Suppose a set $\mathcal{F} \subset \mathcal{C}$ containing N non-degenerate conics is closed under composition. Let $F' = F_{\alpha', \beta', \lambda'} \in \mathcal{C} - \mathcal{F}$ be a non-degenerate conic with $\text{Tr}_{2^m/2}(\alpha'\beta') = 1$ such that $\text{Tr}_{2^m/2}((\alpha \oplus \alpha')(\beta \oplus \beta')) = 1$ for all $F_{\alpha, \beta, \lambda} \in \mathcal{F}$. Then the closure $\mathcal{F}' = \langle \mathcal{F} \cup \{F'\} \rangle$ contains $2N + 1$ conics and $\mathcal{F}' = \{F, F', F \oplus F' | F \in \mathcal{F}\}$.*

Proof. We have the condition that $\text{Tr}_{2^m/2}((\alpha \oplus \alpha')(\beta \oplus \beta')) = 1$ for all $F_{\alpha, \beta, \lambda} \in \mathcal{F}$. Now $F' \notin \mathcal{F}$, so $F' \oplus F \notin \mathcal{F}$ for all $F \in \mathcal{F}$, since \mathcal{F} is closed under composition. So for each $F \in \mathcal{F}$, we get one additional conic with the operation $F \oplus F'$. We also get a final additional conic with the inclusion of F' itself. The composition of any two of these additional conics is of the form $(F_1 \oplus F') \oplus (F_2 \oplus F') = F_1 \oplus F_2$ by Lemma 7.2. Further, $F_1 \oplus F_2 \in \mathcal{F}$ since \mathcal{F} is closed, so we get no further conics. Therefore, $|\mathcal{F}'| = 2N + 1$ and $\mathcal{F}' = \{F, F', F \oplus F' | F \in \mathcal{F}\}$. □

We can start with a single conic and repeatedly apply Lemma 7.3 to obtain the following result.

Corollary 7.4. [18] *A closed set $\mathcal{F} \subset \mathcal{C}$ of conics on a common nucleus contains $2^d - 1$ conics, $1 \leq d \leq m$.*

Proof. Consider the case where we start with a single conic, so $|\mathcal{F}| = 1 = 2^d - 1$ where $d = 1$. Now, consider a set where $|\mathcal{F}| = 2^k - 1$ for some k . If there exists a conic $F' = F_{\alpha', \beta', \lambda'}$ not in \mathcal{F} that has the property

$\text{Tr}_{2^m/2}((\alpha \oplus \alpha')(\beta \oplus \beta')) = 1$ for all $F_{\alpha,\beta,\lambda} \in \mathcal{F}$, then by Lemma 7.3, we can add this conic to \mathcal{F} and increase the size of \mathcal{F} to

$$\begin{aligned} 2(2^k - 1) + 1 &= 2^{k+1} - 2 + 1 \\ &= 2^{k+1} - 1. \end{aligned}$$

So by induction, $|\mathcal{F}| = 2^d - 1$, $1 \leq d \leq m$. \square

Of course, there need not be such a conic outside \mathcal{F} , hence it is possible that $k < m$ and \mathcal{F} cannot be made any larger. Notice also that $|\mathcal{F}| \leq 2^m - 1 = q - 1$ since elements of \mathcal{F} must have distinct values of λ , and $\lambda = 0$ is degenerate.

Theorem 7.5. [18] *Let \mathcal{F} be a closed set of $2^d - 1$ conics with a common nucleus F_0 in $PG(2, 2^m)$, $1 \leq d \leq m$. Then the set of points of all conics in \mathcal{F} together with F_0 form a maximal $\{2^{m+d} - 2^m + 2^d, 2^d\}$ -arc \mathcal{K} in $PG(2, 2^m)$.*

Proof. We will show that every line of $PG(2, 2^m)$ meets \mathcal{K} in zero or 2^d points. Since $\text{Tr}_{2^m/2}(\alpha\beta) = 1$, the line at infinity F_∞ is external to \mathcal{K} . Every other line in $PG(2, 2^m)$ meets F_∞ in one of its points $(1, 0, 0)$ or $(a, 1, 0)$, $a \in GF(2^m)$, and hence belongs to the set of lines $\{[0, 1, 0], [0, b, 1], [1, a, b] \mid a, b \in GF(2^m)\}$.

The lines $[0, 1, 0]$ and $[1, a, 0]$ meet the common nucleus F_0 , and are therefore tangent to every conic in \mathcal{F} . Consequently, each of these lines meets \mathcal{K} in $|\mathcal{F}| + 1 = 2^d$ points.

Any of the remaining lines meet a conic $F \in \mathcal{F}$ in either zero or two points. A line $l = [0, b, 1]$, $b \in GF(2^m)$, has points $(x, 1, b)$, $x \in GF(2^m)$ and $(1, 0, 0)$ on the line at infinity. The line l is disjoint from $F = F_{\alpha,\beta,\lambda}$ if and only if the quadratic equation $\alpha x^2 + x + \beta + \lambda b^2 = 0$ has no solution in $GF(2^m)$. A quadratic $Ax^2 + Bx + C$ has solutions if and only if $\text{Tr}_{2^m/2}(AC/B^2) = 0$, so in this case, we have no solutions if

$$\begin{aligned} &\text{Tr}_{2^m/2} \left(\frac{\alpha(\beta + \lambda b^2)}{1^2} \right) = 1 \\ \iff &\text{Tr}_{2^m/2}(\alpha\beta) + \text{Tr}_{2^m/2}(\alpha b^2 \lambda) = 1 \\ \iff &\text{Tr}_{2^m/2}(\alpha b^2 \lambda) = 0. \end{aligned}$$

So l being disjoint to F is equivalent to the condition that

$$\mathrm{Tr}_{2^m/2}(\alpha, \beta, \lambda) = \mathrm{Tr}_{2^m/2}(\alpha b^2 \lambda) = 0. \quad (7.7)$$

Similarly, a line $m = [1, a, b]$, $a, b \in GF(2^m)$ and $b \neq 0$, has points $(a + bx, 1, x)$, $x \in GF(2^m)$, and $(b, 0, 1)$. If $(b, 0, 1) \in F$, then m must intersect F in another point which has co-ordinates $(a + bx, 1, x)$, $x \in GF(2^m)$. So the line m is disjoint from $F = F_{\alpha, \beta, \lambda}$ if and only if the quadratic equation $\alpha(a + bx)^2 + (a + bx) + \beta + \lambda x^2 = 0$ has no solution in $GF(2^m)$. This is equivalent to the condition that

$$\mathrm{Tr}_{2^m/2}(\alpha, \beta, \lambda) = \mathrm{Tr}_{2^m/2} \left(\frac{\alpha a^2 + a + \beta}{b^2} \lambda \right) = 0. \quad (7.8)$$

We can verify that in both cases, the following condition holds:

$$\mathrm{Tr}_{2^m/2}(\alpha \oplus \alpha', \beta \oplus \beta', \lambda \oplus \lambda') = \mathrm{Tr}_{2^m/2}(\alpha, \beta, \lambda) + \mathrm{Tr}_{2^m/2}(\alpha', \beta', \lambda'). \quad (7.9)$$

Firstly, for Equation 7.7,

$$\begin{aligned} & \mathrm{Tr}_{2^m/2}(\alpha \oplus \alpha', \beta \oplus \beta', \lambda \oplus \lambda') \\ = & \mathrm{Tr}_{2^m/2} \left(\frac{\alpha \lambda + \alpha' \lambda'}{\lambda + \lambda'}, \frac{\beta \lambda + \beta' \lambda'}{\lambda + \lambda'}, \lambda + \lambda' \right) \\ = & \mathrm{Tr}_{2^m/2} \left(\frac{\alpha \lambda + \alpha' \lambda'}{\lambda + \lambda'} b^2 (\lambda + \lambda') \right) \\ = & \mathrm{Tr}_{2^m/2}((\alpha \lambda + \alpha' \lambda') b^2) \\ = & \mathrm{Tr}_{2^m/2}(\alpha b^2 \lambda) + \mathrm{Tr}_{2^m/2}(\alpha' b^2 \lambda') \\ = & \mathrm{Tr}_{2^m/2}(\alpha, \beta, \lambda) + \mathrm{Tr}_{2^m/2}(\alpha', \beta', \lambda'). \end{aligned}$$

Similarly, for Equation 7.8,

$$\begin{aligned}
& \text{Tr}_{2^m/2}(\alpha \oplus \alpha', \beta \oplus \beta', \lambda \oplus \lambda') \\
&= \text{Tr}_{2^m/2} \left(\frac{\alpha\lambda + \alpha'\lambda'}{\lambda + \lambda'}, \frac{\beta\lambda + \beta'\lambda'}{\lambda + \lambda'}, \lambda + \lambda' \right) \\
&= \text{Tr}_{2^m/2} \left(\frac{\frac{\alpha\lambda + \alpha'\lambda'}{\lambda + \lambda'} a^2 + a + \frac{\beta\lambda + \beta'\lambda'}{\lambda + \lambda'}}{b^2} (\lambda + \lambda') \right) \\
&= \text{Tr}_{2^m/2} \left(\frac{(\alpha\lambda + \alpha'\lambda')a^2 + a(\lambda + \lambda') + (\beta\lambda + \beta'\lambda')}{b^2} \right) \\
&= \text{Tr}_{2^m/2} \left(\frac{\alpha a^2 + a + \beta}{b^2} \lambda + \frac{\alpha' a^2 + a + \beta'}{b^2} \lambda' \right) \\
&= \text{Tr}_{2^m/2} \left(\frac{\alpha a^2 + a + \beta}{b^2} \lambda \right) + \text{Tr}_{2^m/2} \left(\frac{\alpha' a^2 + a + \beta'}{b^2} \lambda' \right) \\
&= \text{Tr}_{2^m/2}(\alpha, \beta, \lambda) + \text{Tr}_{2^m/2}(\alpha', \beta', \lambda').
\end{aligned}$$

Hence, if a line l does not meet both F and F' , then it also does not meet $F \oplus F'$. There are two ways for l to intersect the conics in \mathcal{F} . If $\text{Tr}_{2^m/2}(F) = 0$ for all $F \in \mathcal{F}$, then l is disjoint from \mathcal{K} . However, if $\text{Tr}_{2^m/2}(F) = 1$ for some $F \in \mathcal{F}$, then by the argument in Lemma 7.3 we may write $\mathcal{F} = \{F, F', F \oplus F' | F' \in \mathcal{F}'\}$ for \mathcal{F}' some closed set of conics. Hence, by Equation 7.9, there are exactly 2^{d-1} conics in \mathcal{F} with trace 1. By Lemma 7.1, these conics are mutually disjoint. Therefore l intersects \mathcal{K} in 2^d points, and \mathcal{K} is a maximal $\{2^{m+d} - 2^m + 2^d; 2^d\}$ -arc. \square

We will now consider an example of a closed set conics provided by Mathon. The set is $\mathcal{F} = \{F_{\alpha, \beta, \lambda}\}$ with parameters α and β which are polynomials in λ .

Theorem 7.6. [18] *Let $p(\lambda) = \sum_{i=0}^{r-1} a_i \lambda^{2^i-1}$ and $q(\lambda) = \sum_{i=0}^{s-1} b_i \lambda^{2^i-1}$ be polynomials with coefficients in $GF(2^m)$. For an additive subgroup A of order 2^d in $GF(2^m)$ let $\mathcal{F} = \{F_{p(\lambda), q(\lambda), \lambda} | \lambda \in A - \{0\}\} \subset \mathcal{C}$ be a set of conics with a common nucleus F_0 . If $\text{Tr}_{2^m/2}(p(\lambda)q(\lambda)) = 1$ for every $\lambda \in A - \{0\}$, then the set of points on all conics in \mathcal{F} together with F_0 form a maximal $\{2^{m+d} - 2^m + 2^d; d^d\}$ -arc \mathcal{K} in $PG(2, 2^m)$. If both $p(\lambda)$ and $q(\lambda)$ have degree ≤ 1 then \mathcal{K} is a Denniston maximal arc.*

Proof. We need to show that \mathcal{F} is a closed set of non-degenerate conics. Since $\text{Tr}_{2m/2}(p(\lambda)q(\lambda)) = 1$, the conics are non-degenerate, so we must now check closure under composition. Consider $F_{p(\lambda)\oplus p(\lambda'),q(\lambda)\oplus q(\lambda'),\lambda\oplus\lambda'}$ for $\lambda, \lambda' \in GF(q) - \{0\}$, $\lambda \neq \lambda'$. Now, $\lambda^{2^i} + \lambda'^{2^i} = (\lambda + \lambda')^{2^i}$, and so we have

$$p(\lambda) \oplus p(\lambda') = \frac{p(\lambda)\lambda + p(\lambda')\lambda'}{\lambda + \lambda'} = \sum_{i=0}^{r-1} a_i \frac{\lambda^{2^i} + \lambda'^{2^i}}{\lambda + \lambda'} = \sum_{i=0}^{r-1} a_i (\lambda + \lambda')^{2^i - 1},$$

and the same is true for $q(\lambda)$. Consequently, we have

$$F_{p(\lambda),q(\lambda),\lambda} \oplus F_{p(\lambda'),q(\lambda'),\lambda'} = F_{p(\lambda)\oplus p(\lambda'),q(\lambda)\oplus q(\lambda'),\lambda\oplus\lambda'} = F_{p(\lambda+\lambda'),q(\lambda+\lambda'),\lambda+\lambda'}.$$

Since $\lambda + \lambda' \in A$, the set \mathcal{F} is closed, and the points in its conics together with F_0 form a maximal arc by Theorem 7.5.

Now let $p(\lambda) = a_0 + a_1\lambda$ and $q(\lambda) = b_0 + b_1\lambda$. Consider a collineation H of $PG(2, 2^m)$ represented by the matrix

$$H = \begin{pmatrix} a & 0 & 0 \\ 0 & 1/a & 0 \\ ab & a/c & 1 \end{pmatrix}$$

which maps

$$\begin{aligned} x &\mapsto x' = ax \\ y &\mapsto y' = \frac{y}{a} \\ z &\mapsto z' = abx + \frac{c}{a}y + z. \end{aligned}$$

Let

$$a = \sqrt{a_0}, \quad b = \sqrt{\frac{a_1}{a_0}}, \quad c = \sqrt{a_0 b_1}, \quad \epsilon = a_0 b_0.$$

Observe the effect of the mapping H on the conic $F_{p(\lambda),q(\lambda),\lambda}$:

$$\begin{aligned} & p(\lambda)x^2 + xy + q(\lambda)y^2 + \lambda z^2 \\ &= \frac{p(\lambda)}{a^2}x'^2 + x'y' + q(\lambda)a^2y'^2 + \lambda(bx' + cy' + z')^2 \\ &= \frac{a_0 + a_1\lambda}{a_0}x'^2 + x'y' + (b_0 + b_1\lambda)a_0y'^2 + \lambda \left(\frac{a_1}{a_0}x'^2 + a_0b_1y'^2 + z'^2 \right) \\ &= x'^2 + x'y' + \epsilon y'^2 + \lambda z'^2. \end{aligned}$$

This shows that H maps $F_{p(\lambda),q(\lambda),\lambda}$ onto $F_{1,\epsilon,\lambda}$, a subset of the standard pencil, whenever $\text{Tr}_{2^m/2}(a_0b_0) = 1$. Therefore, if both $p(\lambda)$ and $q(\lambda)$ have degree ≤ 1 then \mathcal{K} is a Denniston maximal arc. \square

7.3 An example of the Mathon construction

In this section we will consider an example of the construction presented above, also due to Mathon [18].

Lemma 7.7. [18] *Let G_{2^m} be the subfield of $GF(2^{2m})$ of order 2^m , and let $x \in G_{2^m}$. (Since $GF(2^{2m})$ can be constructed as the quadratic extension of $GF(2^m)$, it must contain a subfield of order 2^m .) Then, $\text{Tr}_{2^{2m}/2}(x) = 0$.*

Proof. Recall that $x^{2^m} = x$ for all x , simply as a property of finite fields. Then,

$$\begin{aligned}
& \text{Tr}_{2^{2m}/2}(x) \\
&= x + x^2 + x^4 + \cdots + x^{2^{2m-1}} \\
&= x + x^2 + x^4 + \cdots + x^{2^{m-1}} + \\
&\quad x^{2^m} + x^{2^{m+1}} + x^{2^{m+2}} + \cdots + x^{2^{2m-1}} \\
&= x + x^2 + x^4 + \cdots + x^{2^{m-1}} + \\
&\quad x + (x)^2 + (x)^4 \cdots + (x)^{2^{m-1}} \\
&= 0.
\end{aligned}$$

\square

Theorem 7.8. [18] *Let $\epsilon \in GF(2^{2m})$ be an element with $\text{Tr}_{2^{2m}/2}(\epsilon) = 1$. Let $q(\lambda) = \sum_{i=0}^{r-1} b_i \lambda^{2^i-1}$ be a polynomial with coefficients $b_0 = \epsilon$, $b_i \in \{0, 1\}$ for $i = 1, \dots, r-1$. Then the set of conics $\mathcal{F} = \{F_{1,q(\lambda),\lambda} \mid \lambda \in G_{2^m}\}$ form maximal arcs of degree 2^m in $PG(2, 2^{2m})$.*

Proof. We can use Theorem 7.6 (where, in this case, $p(\lambda) = 1$), provided the

trace of $q(\lambda)$ satisfies the condition that $\text{Tr}_{2^{2m}/2}(p(\lambda)q(\lambda)) = 1$. Firstly,

$$\begin{aligned}\text{Tr}_{2^{2m}/2}(q(\lambda)) &= \text{Tr}_{2^{2m}/2}\left(\sum_{i=0}^{r-1} b_i \lambda^{2^i-1}\right) \\ &= \sum_{i=0}^{r-1} \text{Tr}_{2^{2m}/2}(b_i \lambda^{2^i-1}).\end{aligned}$$

Since $\lambda \in G_{2^m}$, and $b_i \in \{0, 1\}$, $\text{Tr}_{2^{2m}/2}(b_i \lambda^{2^i-1}) = 0$ for all $i \neq 0$ (by Lemma 7.7), and

$$\begin{aligned}\text{Tr}_{2^{2m}/2}(q(\lambda)) &= \text{Tr}_{2^{2m}/2}(\epsilon) \\ &= 1.\end{aligned}$$

Thus the requirement is satisfied, and the set of conics $\mathcal{F} = \{F_{1,q(\lambda),\lambda} \mid \lambda \in G_{2^m}\}$ form maximal arcs of degree 2^m in $PG(2, 2^{2m})$ by Theorem 7.6. \square

This construction gives examples of non-Denniston maximal arcs.

Chapter 8

Further constructions from sets of conics

Several papers written after Mathon [18] have used a similar approach to describe new constructions of maximal arcs. In this chapter we will survey three papers, written by Hamilton [12], and Hamilton and Mathon [13] [14]. Some results from these papers will be presented without proof.

Hamilton and Mathon [13] show that a closed set of conics remains a closed set of conics in any odd-order extension of the underlying field.

Theorem 8.1. [13] *Let \mathcal{G} be a closed set of conics in $PG(2, q)$. Then the equations of the conics of \mathcal{G} give a closed set of conics in $PG(2, q^m)$, for any $m \geq 1$, m odd.*

It follows from this theorem that given a degree n maximal arc \mathcal{K} in $PG(2, q)$ arising from a closed set of conics, there exist degree n maximal arcs \mathcal{K}_m in $PG(2, q^m)$ for all odd positive integers m .

For the remainder of this chapter, let $GF(q)^*$ denote $GF(q) - \{0\}$. A new construction is then considered.

Theorem 8.2. [13] *Let $r(\lambda) = \sum_{i=0}^{m-1} b_i \lambda^{2^i - 1}$ be any polynomial with coefficients $b_i \in GF(q^m)$ such that $\text{Tr}_{q^m/2}(b_0) = 1$ and for $i > 0$, $\text{Tr}_{q^m/q}(b_i) = 0$.*

Then the points of

$$\mathcal{G} = \{F_{1,r(\lambda),\lambda} \mid \lambda \in GF(q)^*\} \cup \{F_0\}$$

form a degree q maximal arc in $PG(2, q^m)$.

This is proved by showing that $\text{Tr}_{q^{m/2}}(r(\lambda)) = 1$, and then applying Theorem 7.6. Using Theorem 8.1, we can also construct maximal arcs in odd-order extensions of the plane. The authors also note that taking a subset A of $GF(q)^*$ such that $A \cup \{0\}$ is closed under addition allows the construction of a maximal arc whose conics correspond to the elements of A . Hence Theorem 8.2 also implies the existence of a maximal arc of degree r for all r dividing n , though the authors note that some of these may be of Denniston type, that is, not new constructions. The authors present a lemma which shows that non-Denniston maximal arcs contain maximal arcs of smaller degree that are also non-Denniston for $r \geq 8$.

Lemma 8.3. [13] *Let \mathcal{G} be a closed set of conics giving rise to a degree n non-Denniston maximal arc \mathcal{K} in $PG(2, q)$ with $8 \leq n < q/2$. Then there exist maximal arcs of degree r that are non-Denniston in $PG(2, q)$ for all $r \geq 8$, and $r \mid n$.*

Hamilton and Mathon [13] proceed to examine the structure of these new maximal arcs, and describe how they relate to other known constructions, including those due to Thas (1974) (see Chapter 6) and Denniston (see Chapter 5).

In [12], Hamilton presents a method for testing whether a closed set of conics is of Denniston type, and thus whether the resultant maximal arc will be a Denniston maximal arc. He notes that while a Denniston maximal arc has a unique line at infinity, a general closed set of conics can have more than one.

Let A be a subset of $GF(q)^*$ such that $A \cup \{0\}$ is closed under addition. Suppose we have a closed set of conics where A is the set of values over which

λ ranges. Then there are functions $p : A \rightarrow GF(q)$ and $r : A \rightarrow GF(q)$ such that the closed set of conics is described by the equations

$$\{p(\lambda)x^2 + xy + r(\lambda)y^2 + \lambda z^2 = 0 \mid \lambda \in A\}. \quad (8.1)$$

Hamilton then presents the following theorem as a test for whether the resulting maximal arc will be of Denniston type.

Theorem 8.4. [12] *Let \mathcal{C} be a closed set of conics in $PG(2, q)$ with polynomials $p, r : A \rightarrow GF(q)$, $A \subset GF(q)^*$, defining a maximal arc \mathcal{K} as in Equation 8.1. Then \mathcal{K} is of Denniston type if and only if for all $\lambda, \lambda' \in A$, $\lambda \neq \lambda'$, both $\frac{p(\lambda)+p(\lambda')}{\lambda+\lambda'}$ and $\frac{r(\lambda)+r(\lambda')}{\lambda+\lambda'}$ are constant.*

Hamilton presents a corollary to this theorem which proves that the maximal arcs constructed in Theorem 7.8 are new constructions, not of Denniston type. He also presents the following, more general, corollary.

Corollary 8.5. [12] *Let A be a subset of $GF(q)$ with functions $p, r : A \rightarrow GF(q)$ such that $\{p(\lambda)x^2 + xy + r(\lambda)y^2 + \lambda z^2 = 0 \mid \lambda \in A\}$ is the set of equations for a closed set of conics. Suppose that either $\frac{p(\lambda)+p(\lambda')}{\lambda+\lambda'}$ or $\frac{r(\lambda)+r(\lambda')}{\lambda+\lambda'}$ is a polynomial of degree d in λ and λ' , and that $1 < d < |A| - 1$. Then the closed set of conics gives rise to a maximal arc which is not of Denniston type.*

The two corollaries are proved similarly by showing that the constraint imposed by Theorem 8.4 cannot be met by every λ and λ' in A . The remainder of the paper is a presentation of a construction of non-Denniston maximal arcs in $PG(2, 2^h)$, h odd.

Hamilton and Mathon [14] give a construction for maximal arcs of non-Denniston type for all n dividing q in $PG(2, q)$ where q is even. The method begins by constructing a new closed set of conics using the following lemma.

Lemma 8.6. [14] *Let $b_1, b_2 \in GF(2^h)$, $b_2 \neq 0$. Then the function $Q : GF(2^h)^* \rightarrow GF(2)$ given by $Q(\lambda) = \text{Tr}_{2^h/2}(b_1\lambda + b_2\lambda^3)$ is a quadratic form on $GF(2^h)^*$ considered as a projective space $PG(h-1, 2)$ of dimension $h-1$ over $GF(2)$.*

Closed sets of conics, and hence maximal arcs, can then be constructed in the following way.

Theorem 8.7. [14] *Choose $b_0, b_1, b_2 \in GF(2^h)$ with $b_2 \neq 0$ and $\text{Tr}_{2^h/2}(b_0) = 1$. Define the quadratic form $Q(\lambda) = \text{Tr}_{2^h/2}(b_1\lambda + b_2\lambda^3)$ on $GF(2^h)^*$ considered as a projective space $PG(h-1, 2)$, and let A be a subspace of the associated quadric. Then the set*

$$\{x^2 + xy + (b_0 + b_1\lambda + b_2\lambda^3)y^2 + \lambda z^2 = 0 \mid \lambda \in A\}$$

is a closed set of conics giving rise to a maximal arc of degree $|A| + 1$.

The degree of such a maximal arc depends on the characteristics of the quadric. Hamilton and Mathon give the following corollary regarding the spectrum of arcs in $PG(2, 2^h)$.

Corollary 8.8. [14] *In $PG(2, 2^h)$, $h \geq 4$, there exist maximal arcs of degree n that are not of Denniston type for all n dividing $q = 2^h$ with the possible exceptions of $n = 4$ or $n = q/4$.*

The remainder of the paper is concerned with isomorphisms among these new classes of maximal arcs.

Chapter 9

Conclusion

We have now completed a survey of most of the major constructions of maximal arcs in finite field planes. Having covered the introductory and background material in Chapters 2 and 3, we looked at the trivial maximal arcs and the existence results on non-trivial maximal arcs in Chapter 4. In particular, we saw that non-trivial maximal arcs do not exist in $PG(2, q)$, q odd. From here, the major constructions in $PG(2, q)$, q even, were covered in chronological order. Denniston's 1969 construction involving sets of conics and group theory was examined in Chapter 5. The construction due to Thas in 1974 involving the Bruck-Bose representation of a projective plane was covered in Chapter 6. (Thas's 1980 construction was not considered.) Mathon's recent (2002) construction was described in Chapter 7. Some papers involving subsequent work by Mathon and Hamilton were presented in Chapter 8.

Bibliography

- [1] Johannes André, *Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe*, Math. Z. **60** (1954), 156–186.
- [2] Simeon Ball and Aart Blokhuis, *An easier proof of the maximal arcs conjecture*, Proc. Amer. Math. Soc. **126** (1998), 3377–3380.
- [3] Simeon Ball, Aart Blokhuis, and Francesco Mazzocca, *Maximal arcs in Desarguesian planes of odd order do not exist*, Combinatorica **17** (1997), 31–41.
- [4] A. Barlotti, *Sui $\{k; n\}$ -archi di un piano lineare finito*, Boll. Un. Mat. Ital. **11** (1956), 553–556.
- [5] Aart Blokhuis, Nicholas Hamilton, and Henny Wilbrink, *On the non-existence of Thas maximal arcs in odd order projective planes*, European J. Combin **19** (1998), 413–417.
- [6] R. H. Bruck and R. C. Bose, *The construction of translation planes from projective spaces*, Journal of Algebra **1** (1964), 85–102.
- [7] A. Cossu, *Su alcune proprietà dei $\{k, n\}$ -archi di un piano proiettivo sopra un corpo finito*, Rend. Mat. e Appl. **20** (1961), 271–277.
- [8] H. S. M. Coxeter, *The real projective plane*, 3rd ed., Springer-Verlag, New York, 1993.
- [9] R. H. F. Denniston, *Some maximal arcs in finite projective planes*, Journal of Combinatorial Theory **6** (1969), 317–319.

- [10] John B. Fraleigh, *A first course in abstract algebra*, 7th ed., Pearson Education, Inc., Boston, 2003.
- [11] N. Hamilton, *Maximal arcs in finite projective planes and associated structures in projective spaces*, Ph.D. thesis, University of Western Australia, June 1995.
- [12] Nicholas Hamilton, *Degree 8 maximal arcs in $PG(2, 2^h)$, h odd*, to appear in *J. Comb. Theory Ser. A*, 2003.
- [13] Nicholas Hamilton and Rudolf Mathon, *More maximal arcs in Desarguesian projective planes and their geometric structure*, to appear in *Adv. Comb.*, 2003.
- [14] ———, *On the spectrum of non-Denniston maximal arcs in $PG(2, 2^h)$* , 2003.
- [15] James W. P. Hirschfeld, *Finite projective spaces of three dimensions*, 1st ed., Oxford University Press, Walton Street, Oxford, 1985.
- [16] ———, *Projective geometries over finite fields*, 2nd ed., Oxford University Press, Great Clarendon Street, Oxford, 1998.
- [17] A. F. Horadam, *A guide to undergraduate projective geometry*, 1st ed., Pergamon Press Australia, Rushcutters Bay, NSW, 1970.
- [18] R. Mathon, *New maximal arcs in Desarguesian planes*, *Journal of Combinatorial Theory, Series A* **97** (2002), 353–368.
- [19] J. A. Thas, *Construction of maximal arcs and partial geometries*, *Geometriae Dedicata* **3** (1974), 61–64.
- [20] Joseph A. Thas, *Handbook of incidence geometry: buildings and foundations*, ch. 7, Elsevier Science B. V., Amsterdam, The Netherlands, 1995.