UNIVERSITÀ DEGLI STUDI DI ROMA

“LA SAPIENZA”

The geometry of finite fields

Simeon Ball

Quaderni Elettronici del Seminario di Geometria Combinatoria

2E (Maggio 2001)

http://www.mat.uniroma1.it/~combinat/quaderni

Dipartimento di Matematica “Guido Castelnuovo”

P.le Aldo Moro, 2 - 00185 Roma - Italia

Preface

These notes are about the geometry of finite fields. The central purpose is to look at the implications that $GF(q^n)$ is an n-dimensional vector space over $GF(q)$ to geometries such as $PG(n-1,q)$, $AG(n,q)$ and the classical polar spaces. The very basics of finite geometry have also been included in an attempt to make the notes as self-contained as possible and requiring only some knowledge of linear algebra.

I have taken parts of Chapters 1, 2, 4 and 6 from

"Projective and Polar Spaces" by Peter Cameron, available from
www.maths.qmw.ac.uk/ pjc/

I am very grateful for the permission to use this material and the LaTeXsource files. It may prove helpful to use his notes alongside these. Other notes that should prove useful are

"Generalized Polygons and Semipartial Geometries" by F. de Clerck, J. A. Thas and H. Van Maldeghem, available from www.cage.rug.ac.be/ fdc/

"Flocks, ovals and generalised quadrangles (Four Lectures in Napoli, June 2000)" by Maska Law and Tim Penttila, available from
thysanotus.maths.uwa.edu.au/research/reports/

"Classical Groups" by Peter Cameron, available from
www.maths.qmw.ac.uk/ pjc/

Chapter 1 is a brief introduction to projective spaces and concludes with the basic idea of how to see $PG(n-1,q)$ and $AG(n,q)$ as subsets of elements of the field

$GF(q^n)$. Chapter 2 introduces some interesting subsets of points found in projective spaces, in particular maximal arcs in finite projective planes and introduces related incidence structures such as inversive planes and partial geometries. We also prove a theorem about maximal arcs using finite fields.

Chapter 3 is an introduction to polar spaces including representing the classical polar spaces as subsets of finite fields. The section is concluded with the introduction of m-systems of polar spaces and the construction of maximal arcs from particular m-systems.

Chapter 4 contains a very brief introduction to generalised quadrangles and is mainly concerned with ovoids and spreads of the symplectic generalised quadrangle which are again considered as subsets of finite fields.

In addition to those notes mentioned above the following texts may well be of use.

The books by J. W. P. Hirschfeld [Hir] and J. W. P. Hirschfeld and J. A. Thas [HT] provide a comprehensive reference to projective geometries related to finite fields. The book by D. R. Hughes and F. C. Piper [HP] is a useful reference for projective planes. The book on finite fields by R. Lidl and H. Niederreiter [LN] contains a section on linearised polynomials which are in essence what these notes are about. Although now out of print the book about the classical groups by D. E. Taylor [Tay] is worth searching out and finally for further reading on bilinear forms see Chevalley [Che].

I am grateful to Prof. D. Jungnickel for his careful reading of these notes which eliminated many mistakes, to Prof. D. Ghinelli for giving me the opportunity to give a course at “La Sapienza” for which these notes were compiled, and to Francesca Merola and Daniele Gewurz for their help with the course and with the notes. Corrections or any other comments will be gratefully received at the e-mail address below.

Simeon Ball, London and Rome, 2001
simeon@maths.qmw.ac.uk

Contents

1

Projective spaces

1.1 Projective spaces

A theorem of Galois states that a finite field has prime power order and for any prime power q, there is a unique finite field of order q. The unique field of order q is denoted by $\mathrm{GF}(q)$. If $q = p^d$ with p prime, its additive structure is that of a d-dimensional vector space over its prime field $\mathrm{GF}(p)$ (the integers modulo p). Its multiplicative group is cyclic (of order $q-1$), and its automorphism group is cyclic (of order d). If $d = 1$ (that is, if q is prime), then $\mathrm{GF}(q)$ is the ring of integers mod q.

A projective space of dimension n over a field F can be constructed in either of two ways: by adding a hyperplane at infinity to an affine space, or by "projection" of an $(n+1)$-dimensional space. Both methods have their importance, but the second is the more natural.

Thus, let V be an $(n+1)$-dimensional vector space over F. The *projective space* $\mathrm{PG}(n,F)$ is the geometry whose *points, lines, planes,* ... are the vector subspaces of V of dimensions 1, 2, 3, ...

Note the dimension shift: a d-dimensional projective subspace (or flat) is a $(d+1)$-dimensional vector subspace. This is done in order to ensure that familiar geometrical properties hold. For example, two points lie on a unique line; two intersecting lines lie in a unique plane; and so on. Moreover, any d-dimensional projective subspace is a d-dimensional projective space in its own right (when

equipped with the subspaces it contains).

To avoid confusion (if possible) the term *rank* (in symbols, rk) is reserved for vector space dimension, so that unqualified "dimension" will be geometric dimension.

A *hyperplane* is a subspace of codimension 1 (that is, of dimension one less than the whole space). If H is a hyperplane and L a line not contained in H, then $H \cap L$ is a point.

A projective plane (that is, $\mathrm{PG}(2,F)$) has the property that any two lines meet in a (unique) point. For, if $\mathrm{rk}(V) = 3$ and $U, W \subseteq V$ with $\mathrm{rk}(U) = \mathrm{rk}(W) = 2$, then $U + W = V$, and so $\mathrm{rk}(U \cap W) = 1$; that is, $U \cap W$ is a point.

A geometric property of projective spaces is the following.

Proposition 1.1 (Desargues' Theorem) *In Figure 1.1, the three points p_{12}, p_{13}, p_{23} are collinear.*

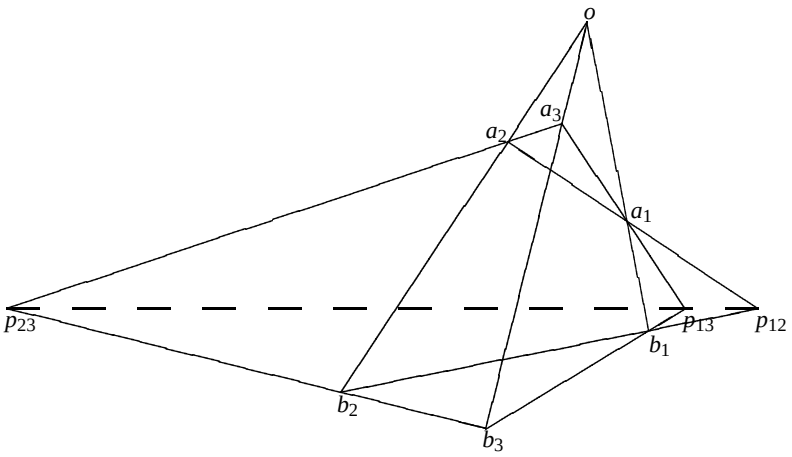

Figure 1.1: Desargues' Theorem

In the case where the figure is not contained in a plane, the result is obvious geometrically. For each of the three points p_{12}, p_{13}, p_{23} lies in both the planes

$a_1a_2a_3$ and $b_1b_2b_3$; these planes are distinct, and both lie in the 3-dimensional space spanned by the three lines through o, and so their intersection is a line.

The case where the figure is contained in a plane π can be deduced from the "general" case as follows. Take a plane $H \neq \pi$ containing p_{12} and p_{13}. Choose a_4, $b_4 \notin \pi$ collinear with o in the 3-space spanned by H and o in such a way that $p_{14} \in H$ (p_{14} is defined in the same way as the other p_{ij}). The geometric argument of the preceding paragraph shows that p_{12}, p_{14} and p_{24} are collinear and that p_{13}, p_{14} and p_{34} are collinear. The line joining p_{24} and p_{34} is contained in H and the non-planar Desargues' Theorem for the triangles $a_2a_3a_4$ and $b_2b_3b_4$ implies that p_{23} is on this line. Therefore H contains p_{23} as well as p_{13} and p_{12} and π also contains these points . The two planes H and π meet in a line so these points are collinear.

(The crucial fact is that the plane can be embedded in a 3-dimensional space.)

Let V be a vector space of rank $n+1$ over F, and V^* its dual space. The vector space V^* has the same rank as V. Thus we have projective spaces $\mathrm{PG}(n,F)$'s, standing in a dual relation to one another. More precisely, we have a bijection between the flats of the $\mathrm{PG}(n,F)$'s, given by

$$U \leftrightarrow \mathrm{Ann}(U) = \{\mathbf{f} \in V^* : (\forall \mathbf{u} \in U)\ (\mathbf{fu} = 0)\}.$$

This correspondence preserves incidence and reverses inclusion:

$$\begin{aligned} U_1 \subseteq U_2 &\Rightarrow \mathrm{Ann}(U_2) \subseteq \mathrm{Ann}(U_1), \\ \mathrm{Ann}(U_1 + U_2) &= \mathrm{Ann}(U_1) \cap \mathrm{Ann}(U_2), \\ \mathrm{Ann}(U_1 \cap U_2) &= \mathrm{Ann}(U_1) + \mathrm{Ann}(U_2). \end{aligned}$$

Moreover, the (geometric) dimension of $\mathrm{Ann}(U)$ is $n - 1 - \dim(U)$.

This gives rise to a *duality principle*, where any configuration theorem in projective space translates into another in which inclusions are reversed and dimensions suitably modified. For example, in the plane, the dual of the statement that two points lie on a unique line is the statement that two lines meet in a unique point.

We turn briefly to affine spaces. The description closest to that of projective spaces runs as follows. Let V be a vector space of rank n over F. The *points*, *lines*, *planes*, ... of the *affine space* $\mathrm{AG}(n,F)$ are the cosets of the vector subspaces of rank 0, 1, 2, ... (No dimension shift this time!) In particular, points are cosets of the zero

subspace, in other words, singletons, and we can identify them with the vectors of V. So the affine space is "a vector space with no distinguished origin".

The other description is: $\mathrm{AG}(n,F)$ is obtained from $\mathrm{PG}(n,F)$ by deleting a hyperplane together with all the subspaces it contains.

The two descriptions are matched up as follows. Take the vector space

$$V = F^{n+1} = \{(x_0, x_1, \ldots, x_n) : x_0, \ldots, x_n \in F\}.$$

Let W be the hyperplane defined by the equation $x_0 = 0$. The points remaining are rank 1 subspaces spanned by vectors with $x_0 \neq 0$; each point has a unique spanning vector with $x_0 = 1$. Then the correspondence between points in the two descriptions is given by

$$\langle (1, x_1, \ldots, x_n) \rangle \leftrightarrow (x_1, \ldots, x_n).$$

In $\mathrm{AG}(n,F)$, we say that two subspaces are *parallel* if (in the first description) they are cosets of the same vector subspace, or (in the second description) they have the same intersection with the deleted hyperplane. Parallelism is an equivalence relation. Now the projective space can be recovered from the affine space as follows. To each parallel class of d-dimensional subspaces of $\mathrm{AG}(n,F)$ corresponds a unique $(d-1)$-dimensional subspace of $\mathrm{PG}(n-1,F)$. Adjoin to the affine space the points (and subspaces) of $\mathrm{PG}(n-1,F)$, and adjoin to all members of a parallel class all the points in the corresponding subspace. The result is $\mathrm{PG}(n,F)$.

The distinguished hyperplane is called the *hyperplane at infinity* or *ideal hyperplane*. Thus, an affine space can also be regarded as "a projective space with a distinguished hyperplane".

1.2 Projective planes

Projective and affine planes are more than just spaces of smallest (non-trivial) dimension: as we will see, they are exceptional. The geometry $\mathrm{PG}(2,F)$ has the following properties:

(PP1) Any two points lie on exactly one line.

(PP2) Any two lines meet in exactly one point.

(PP3) There exist four points, no three of which are collinear.

The term *projective plane* will now be used in a more general sense, to refer to any structure of points and lines which satisfies conditions (PP1)-(PP3) above.

In a projective plane, let p and L be a point and line which are not incident. The incidence defines a bijection between the points on L and the lines through p. By (PP3), given any two lines, there is a point incident with neither; so the two lines contain equally many points. Similarly, each point lies on the same number of lines; and these two constants are equal. The *order* of the plane is defined to be one less than this number. The order of $\mathrm{PG}(2,F)$ is equal to the cardinality of F.

Given a finite projective plane of order n, each of the $n+1$ lines through a point p contains n further points, with no duplications, and all points are accounted for in this way. So there are n^2+n+1 points, and the same number of lines.

Do there exist projective planes not of the form $\mathrm{PG}(2,F)$? The easiest such example is infinite; finite examples will appear later.

Example: *Free planes.* Start with any configuration of points and lines having the property that two points lie on at most one line (and dually), and satisfying (PP3). Perform the following construction. At odd-numbered stages, introduce a new line incident with each pair of points not already incident with a line. At even-numbered stages, act dually: add a new point incident with each pair of lines for which such a point doesn't yet exist. After countably many stages, a projective plane is obtained. For given any two points, there will be an earlier stage at which both are introduced; by the next stage, a unique line is incident with both; and no further line incident with both is added subsequently; so (PP1) holds. Dually, (PP2) holds. Finally, (PP3) is true initially and remains so. If we start with a configuration violating Desargues' Theorem (for example, the Desargues configuration with the line pqr "broken" into separate lines pq, qr, rp), then the resulting plane doesn't satisfy Desargues' Theorem, and so is not a $\mathrm{PG}(2,F)$.

The *Bruck–Ryser Theorem* asserts that, if a projective plane of order n exists, where $n \equiv 1$ or 2 (mod 4), then n must be the sum of two squares. Thus, for example, there is no projective plane of order 6 or 14. This theorem gives no information about 10, 12, 15, 18, ... Recently, Lam, Swiercz and Thiel showed by an extensive computation that there is no projective plane of order 10. The other values mentioned are undecided.

An *affine plane* is an incidence structure of points and lines satisfying the following conditions (in which two lines are called *parallel* if they are equal or disjoint):

(AP1) Two points lie on a unique line.

(AP2) Given a point p and line L, there is a unique line which contains p and is parallel to L.

(AP3) There exist three non-collinear points.

Again it holds that $\mathrm{AG}(2,F)$ is an affine plane. More generally, if a line and all its points are removed from a projective plane, the result is an affine plane. (The removed points and line are said to be "at infinity". Two lines are parallel if and only if they contain the same point at infinity.

Conversely, let an affine plane be given, with point set $\mathcal{P}$ and line set $\mathcal{L}$. It follows from (AP2) that parallelism is an equivalence relation on $\mathcal{L}$. Let Q be the set of equivalence classes. For each line $L \in \mathcal{L}$, let $L^+ = L \cup \{Q\}$, where Q is the parallel class containing L. Then the structure with point set $\mathcal{P} \cup Q$, and line set $\{L^+ : L \in \mathcal{L}\} \cup \{Q\}$, is a projective plane. Choosing Q as the line at infinity, we recover the original affine plane.

In a finite affine plane, there is an integer $n > 1$ such that every line has n points, every point lies on $n+1$ lines, there are n^2 points and there are $n+1$ parallel classes with n lines in each. The number n is the *order* of the affine plane. All these facts are left as an exercise.

1.3 Desarguesian planes

Theorem 1.2 *A projective plane is isomorphic to* $\mathrm{PG}(2,F)$ *for some* F *if and only if it satisfies Desargues' Theorem.*

I do not propose to give a proof of this important result; but some comments on the proof are in order.

The field operations (addition and multiplication) can be defined geometrically, once a set of four points with no three collinear has been chosen. By (PP3), such a set of points exists in any projective plane. So it is possible to define two binary

operations on a set consisting of a line with a point removed, and to coordinatise the plane with this algebraic object. Now any field axiom translates into a certain "configuration theorem", so that the plane is a $\mathrm{PG}(2,F)$ if and only if all these "configuration theorems" hold. What is not obvious, and quite remarkable, is that all these "configuration theorems" follow from Desargues' Theorem.

Another method, more difficult in principle but much easier in detail, exploits the relation between Desargues' Theorem and collineations.

Let p be a point and L a line. A *central collineation* with centre p and axis L is a collineation fixing every point on L and every line through p. It is called an *elation* if p is on L, a *homology* otherwise. The central collineations with centre p and axis L form a group. The plane is said to be (p,L)-*transitive* if this group permutes transitively the set $M \setminus \{p, L \cap M\}$ for any line $M \neq L$ on p (or, equivalently, the set of lines on q different from L and pq, where $q \neq p$ is a point of L).

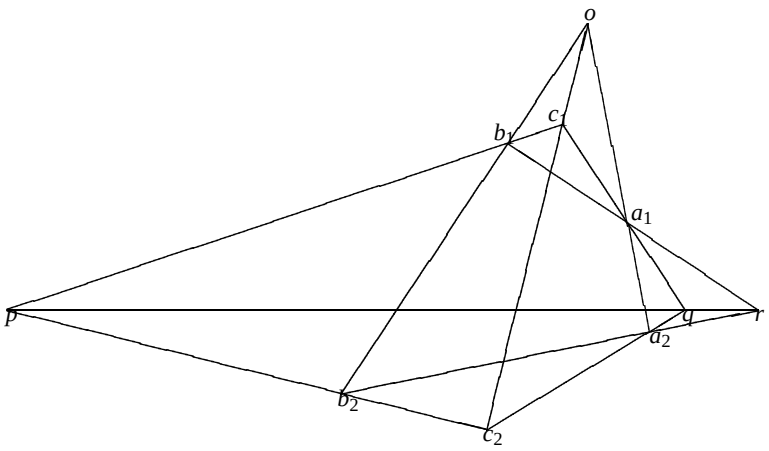

Figure 1.2: The Desargues configuration

Theorem 1.3 *A projective plane satisfies Desargues' Theorem if and only if it is* (p,L)*-transitive for all points p and lines L.*

Proof Assume that the plane is (p,L)-transitive for all points p and lines L. Let us take another look at the Desargues configuration (Fig. 1.2). Let L be the line rq.

We wish to show that p is incident with L. There is a central collineation taking a_1 to a_2 which is completely determined determined at every point. For example the line b_1a_1 meets L in r and ra_2 meets ob_1 in b_2. Therefore b_1 is taken to b_2. Similarly c_1 is taken to c_2 and p is fixed by the collineation. Since $p \neq o$ it is incident with L.

Conversely, we need to find a central collineation taking a_1 to a_2 fixing the line L pointwise and every line incident with o. The collineation is now completely determined at every point and specifically b_1 is taken to b_2 and c_1 is taken to c_2. The point p is fixed and we have a collineation. ∎

In view of Theorem 1.2 projective planes over fields are called *Desarguesian planes*.

1.4 The geometry of finite fields

The field $GF(q^n)$ is a vector space of rank n over $GF(q)$. In Section 1.1 we defined $PG(n-1, GF(q))$ (which we denote from now on as $PG(n-1,q)$) from the subspaces of V, a vector space of rank n over $GF(q)$. The following theorem allows us to identify the subspaces of $GF(q^n)$ by polynomials.

Theorem 1.4 *The set*

$$U = \left\{ x \in GF(q^n) \;\middle|\; \sum_{i=0}^{n-1} a_i x^{q^i} = 0 \right\}$$

is a subspace over $GF(q)$. If U has rank r (projective $(r-1)$-dimensional subspace) then the $GF(q^n)$-rank of the matrix $B = (b_{ij})$ defined by $b_{ij} = a_{j-i}^{q^i}$, where the indices are taken modulo n, is at most $n-r$.

Proof It is easy to check that the set U of zeros of $\sum_{j=0}^{n-1} a_j x^{q^j}$ form a subspace and any element of U is also a zero of

$$\sum_{j=0}^{n-1} a_j^{q^i} x^{q^{i+j}} = \sum_{j=0}^{n-1} a_{j-i}^{q^i} x^{q^j},$$

where again the indices are taken modulo n.

For all $x \in U$ the vector $\mathbf{x} = (x, x^q, x^{q^2}, \ldots, x^{q^{n-1}}) \in V(n, q^n)$ is in the kernel of B. Moreover if $\mathbf{x} = \lambda \mathbf{y}$ for x and $y \in U$ and $\lambda \in GF(q^n)$ then $x = \lambda y$ and $x^q = \lambda y^q$ and $\lambda = x/y = x^q/y^q \in GF(q)$. There are r elements of U linearly independent over $GF(q)$ and therefore r vectors of the form $(x, x^q, x^{q^2}, \ldots, x^{q^{n-1}})$ linearly independent over $GF(q^n)$. Hence the kernel of B is a subspace over $GF(q^n)$ of rank at least r and by the rank-nullity theorem the $GF(q^n)$-rank of B is at most $n-r$. ∎

Given a subspace U of rank r the polynomial

$$\prod_{u \in U} (x - u)$$

is a monic polynomial of degree q^r of the form

$$x^{q^r} + \sum_{j=0}^{r-1} a_j x^{q^j}.$$

The previous theorem allows us to calculate necessary and sufficient conditions on the coefficients to determine when such a polynomial (sometimes referred to a as a *linearised polynomial*) is a subspace. Note they are precisely the linearised polynomials which are factors of the polynomial

$$x^{q^n} - x = \prod_{\varepsilon \in GF(q^n)} (x - \varepsilon).$$

It is a simple matter to calculate these polynomials for the rank 1 subspace (points) and the rank $n-1$ subspaces (hyperplanes) by applying Theorem 1.4. The set

$$\left\{ x \in GF(q^n) \;\middle|\; x^q - ax = 0 \right\}$$

is a rank 1 subspace of $GF(q^n)$ when $a^{q^{n-1}+q^{n-2}+\ldots+q+1} = 1$. The set

$$\left\{ x \in GF(q^n) \;\middle|\; x^{q^{n-1}} + \sum_{i=0}^{n-2} a^{1+q+\ldots+q^{n-i-2}} x^{q^i} = 0 \right\}$$

is a rank $n-1$ subspace when $a^{q^{n-1}+q^{n-2}+\ldots+q+1} = 1$.

Note that we now know all the polynomials defining the points and lines of $PG(2, q)$.

We now look for a similar way of considering $AG(n,GF(q))$ (which we shall denote from now on as $AG(n,q)$). The field $GF(q^n)$ is a vector space of rank n and we follow 1.1. A coset of a subspace of rank r is a set of size q^r of the form

$$\left\{x+\lambda \;\middle|\; \sum_{i=0}^{r} a_i x^{q^i} = 0\right\}$$

where $\lambda \in GF(q^n)$ and the set of zeros of the polynomial $\sum_{i=0}^{r} a_i x^{q^i}$ is a subspace of rank r. Therefore a subspace of $AG(n,q)$ is a set

$$\left\{x \;\middle|\; \sum_{i=0}^{r} a_i x^{q^i} - \sum_{i=0}^{r} a_i \lambda^{q^i} = 0\right\}.$$

Note that a polynomial of the form $\sum_{i=0}^{r} a_i x^{q^i} + b$ defines a subspace of $AG(n,q)$ of dimension r if and only if it is a factor of $x^{q^n} - x$.

A point of $AG(n,q)$ is a singleton set $\{x\}$ where $x \in GF(q^n)$. Therefore we refer to the elements of $GF(q^n)$ as the points of $AG(n,q)$. The lines of $AG(n,q)$ are sets

$$\left\{x \in GF(q^n) \;\middle|\; x^q - ax - (\lambda^q + a\lambda) = 0\right\}$$

where $a^{q^{n-1}+q^{n-2}+\ldots+q+1} = 1$ and $\lambda \in GF(q^n)$.

It is sometimes useful to view projective and affine spaces in this way because it is often simple to calculate an algebraic condition for a geometric property which in turn can lead to solutions of otherwise difficult problems.

Let us consider three points u, v and w in $AG(2,q)$. What is the condition that they are collinear ? A line of $AG(2,q)$ is

$$\left\{x \in GF(q^2) \;\middle|\; x^q - ax + b = 0\right\}$$

where $a^{q+1} = 1$ and $b \in GF(q^2)$. The points u, v and w are collinear iff there exists a and b such that

$$b = -au - u^q = -av - v^q = -aw - w^q$$

which implies that

$$(u-v)^{q-1} = (v-w)^{q-1} = (w-u)^{q-1}.$$

Consider the following problem: Let $\mathcal{S}$ be a set of $q+1$ points of $AG(2,q)$ and let $\mathcal{N}$ be the set of points disjoint from $\mathcal{S}$ with the property that every line incident with a point of $\mathcal{N}$ is incident with a point of $\mathcal{S}$. Such a point $p \in \mathcal{N}$ is called a *nucleus*. How large can the set $\mathcal{N}$ be ? Let us consider $AG(2,q)$ as $GF(q^2)$ and define $f \in GF(q^2)[X]$ by

$$f(X) = \sum_{b \in \mathcal{S}} (X-b)^{q-1}.$$

If $x \in \mathcal{N} \subset GF(q^2)$ then the values of $(x-b)^{q-1}$ for $b \in \mathcal{S}$ are pair-wise distinct and non-zero. However $((x-b)^{q-1})^{q+1} = (x-b)^{q^2-1} = 1$ in $GF(q^2)$ so $(x-b)^{q-1}$ is a $(q+1)-$st root of unity. The sum of these roots of unity is zero and so $f(x) = 0$. The polynomial $f(X)$ has exactly degree $q-1$ (it is not identically zero since the coefficient of X^{q-1} is 1). Hence f can have at most $q-1$ zeros and therefore $|\mathcal{N}| \leq q-1$.

This is the Blokhuis-Wilbrink theorem on nuclei.

Exercises

1. Show that the sets

$$\{x \in GF(q^4) \mid x^{q^2} + cx^q + ex = 0\}$$

are rank 2 subspaces over $GF(q)$ (lines of $PG(3,q)$) if and only if $e^{q^3+q^2+q+1} = 1$ and $c^{q+1} = e^q - e^{q^2+q+1}$.

2. Prove that a set $\mathcal{S}$ of $q+k$ points in $AG(2,q)$ can have at most $k(q-1)$ nuclei. (Hint: look at the coefficient of T^q in the polynomial

$$F(T,X) = \prod_{b \in \mathcal{S}} (T - (X-b)^{q-1}).$$

What does the polynomial $F(T,x)$ look like when x is a nucleus ?) Hence show that a set of points in $AG(2,q)$ which is incident with every line has at least $2q-1$ points. Such a set is called a *blocking set*.

2

Subsets of projective spaces

2.1 Spreads and translation planes

Let V be a vector space over F, having even rank $2n$. A *spread* $\mathcal{S}$ is a set of subspaces of V of rank n, having the property that any non-zero vector of V lies in a unique member of $\mathcal{S}$. A trivial example occurs when $n = 1$ and $\mathcal{S}$ consists of all the rank 1 subspaces.

The importance of spreads comes from the following result, whose proof is straightforward.

Proposition 2.1 *Let $\mathcal{S}$ be a spread in V, and $\mathcal{L}$ the set of all cosets of members of $\mathcal{S}$. Then $(V, \mathcal{L})$ is an affine plane. The projective plane obtained by adding a line at infinity L_∞ is (p, L_∞)-transitive for all $p \in L_\infty$.* ∎

For finite planes, the converse of the last statement is also true. An affine plane with the property that the projective completion is (p, L_∞)-transitive for all $p \in L_\infty$ is called a *translation plane*.

Example. Let K be an extension field of F with degree n. Take V to be a rank 2 vector space over K, and $\mathcal{S}$ the set of rank 1 K-subspaces. Then, of course, the resulting affine plane is $\mathrm{AG}(2, K)$. Now forget the K-structure, and regard V

as an F- vector space. Such a spread is called *Desarguesian*, because it can be recognised by the fact that the affine plane is Desarguesian.

Projectively, a spread is a set of $(n-1)$-dimensional flats in $\mathrm{PG}(2n-1,F)$, which partitions the points of F. We will examine further the case $n=1$.

Lemma 2.2 *Given three pairwise skew lines in* $\mathrm{PG}(3,F)$*, there is a unique common transversal through any point on one of the lines.*

Proof Let L_1,L_2,L_3 be the lines, and $p \in L_1$. The quotient space by p is a projective plane $\mathrm{PG}(2,F)$, and $\Pi_1 = \langle p, L_2\rangle$ and $\Pi_2 = \langle p, L_3\rangle$ are distinct lines in this plane; they meet in a unique point, which corresponds to a line M containing p and lying in Π_1 and Π_2, hence meeting L_2 and L_3. ■

Now let $\mathcal{R}'$ be the set of common transversals to the three pairwise skew lines. The lines in $\mathcal{R}'$ are pairwise skew, by 2.2.

Lemma 2.3 *A common transversal to three lines of* $\mathcal{R}'$ *is a transversal to all of them.* ■

Let $\mathcal{R}$ be the set of all common transversals to $\mathcal{R}'$. The set $\mathcal{R}$ is called a *regulus*, and $\mathcal{R}'$ (which is also a regulus) is the *opposite regulus*. Thus, three pairwise skew lines lie in a unique regulus.

A spread is *regular* if it contains the regulus through any three of its lines.

Theorem 2.4 *A spread is Desarguesian if and only if it is regular.* ■

If we take a regular spread, and replace the lines in a regulus in this spread by those in the opposite regulus, the result is still a spread; for a regulus and its opposite cover the same set of points. This process is referred to as *derivation*. It gives rise to non-Desarguesian translation planes:

Proposition 2.5 *If* $|F| > 2$*, then a derivation of a regular spread is not regular.*

Proof Choose two reguli $\mathcal{R}_1$, $\mathcal{R}_2$ with a unique line in common. If we replace $\mathcal{R}_1$ by its opposite, then the regulus $\mathcal{R}_2$ contains three lines of the spread but is not contained in the spread. ■

It is possible to push this much further. For example, any set of pairwise disjoint reguli can be replaced by their opposites.

2.2 Ovals

For projective geometries over finite fields, it is very natural to ask for characterisations of interesting sets of points by hypotheses on their intersections with lines.

If a polynomial f in $x_1, \ldots, x_{n+1}$ is *homogeneous*, that is, a sum of terms all of the same degree, then $f(\mathbf{v}) = 0$ implies $f(\alpha\mathbf{v}) = 0$ for all $\alpha \in F$. So, if f vanishes at a non-zero vector, then it vanishes at the rank 1 subspace (the point of $\mathrm{PG}(n,F)$) it spans. The *algebraic variety* defined by f is the set of points spanned by zeros of f. We are concerned here only with the case $n = 2$, in which case (assuming that f does not vanish identically) this set is called an *algebraic curve*.

Now consider the case where f has degree 2, and $F = \mathrm{GF}(q)$, where q is an *odd* prime power. The curve it defines may be a single point, or a line, or two lines; but, if none of these occurs, then it is equivalent (under the group $\mathrm{PGL}(3,q)$) to the curve defined by the equation $x_1^2 + x_2^2 + x_3^2 = 0$ (see Exercise 1). Any curve equivalent to this one is called a *conic* (or *irreducible conic*).

It can be shown that a conic has $q+1$ points, no three of which are collinear. This leads us to define an *oval* as a set of points with the property that no three are collinear. A conic is therefore an oval and when q is odd Segre's theorem says that the converse is true.

Theorem 2.6 (Segre's Theorem) *For q odd, an oval is a conic.*

I do not wish to give a proof of this important theorem, a proof can be found in Cameron [2] or Hirschfeld [Hir] or Hughes and Piper [HP].

The analogue of Segre's Theorem over $\mathrm{GF}(q)$ with even q is false. In this case, the tangents to an oval S all pass through a single point n, the *nucleus* of the oval; and,

for any $p \in S$, the set $S \cup \{n\} \setminus \{p\}$ is also an oval. But, if $q > 4$, then at most one of these ovals can be a conic; these ovals have q common points. For sufficiently large q ($q \geq 16$) there are other ovals, not arising from this construction. For information on ovals in planes of even order see [1] or [4].

2.3 Ovoids and inversive planes

Ovoids are 3-dimensional analogues of ovals. They have added importance because of their connection with inversive planes, which are one-point extensions of affine planes.

An *ovoid* in $\mathrm{PG}(3,F)$ is a set O of points with the properties

(O1) no three points of O are collinear;

(O2) the tangents to O through a point of O form a plane pencil.

(If a set of points satisfies (O1), a line is called a *secant*, *tangent* or *external line* if it meets the set in 2, 1 or 0 points respectively. The plane containing the tangents to an ovoid at a point x is called the *tangent plane* at x.)

The classical examples of ovoids are the *elliptic quadrics*. Let $\alpha x^2 + \beta x + \gamma$ be an irreducible quadratic over the field F. The elliptic quadric consists of the points of $\mathrm{PG}(3,F)$ whose coordinates (x_1,x_2,x_3,x_4) satisfy

$$x_1x_2 + \alpha x_3^2 + \beta x_3x_4 + \gamma x_4^2 = 0.$$

The proof that these points do form an ovoid is left as an exercise.

Over finite fields, ovoids are rare. Barlotti and Panella showed the following analogue of Segre's theorem on ovals:

Theorem 2.7 *Any ovoid in* $\mathrm{PG}(3,q)$*, for q an odd prime power, is an elliptic quadric.* ■

For even q, just one further family is known, the *Suzuki–Tits ovoids* which we will construct in Section 4.3

An *inversive plane* is, as said above, a one-point extension of an affine plane. That is, it is a pair $(X, \mathcal{C})$, where X is a set of points, and $\mathcal{C}$ a collection of subsets of X called *circles*, satisfying

(I1) any three points lie in a unique circle;

(I2) if x, y are points and C a circle with $x \in C$ and $y \notin C$, then there is a unique circle C' satisfying $y \in C'$ and $C \cap C' = \{x\}$;

(I3) there exist four non-concircular points.

It is readily checked that, for $x \in X$, the points different from x and circles containing x form an affine plane. The *order* of the inversive plane is the (common) order of its derived affine planes.

Proposition 2.8 *The points and non-trivial plane sections of an ovoid form an inversive plane.*

Proof A plane section of the ovoid O is non-trivial if it contains more than one point. Any three points of O are non-collinear, and so define a unique plane section. Given x, the points of O different from x and the circles containing x correspond to the lines through x not in the tangent plane T_x and the planes through x different from T_x; these are the points of the quotient space not incident with the line T_x/x and the lines different from T_x/x, which form an affine plane. ■

An inversive plane arising from an ovoid in this way is called *egglike*. Dembowski proved:

Theorem 2.9 *Any inversive plane of even order is egglike (and so its order is a power of 2).*

This is not known to hold for odd order, but no counterexamples are known.

There are configuration theorems (the *bundle theorem* and *Miquel's theorem* respectively) which characterise egglike inversive planes and "classical" inversive planes (coming from the elliptic quadric) respectively.

2.4 Maximal arcs and partial geometries

Let π be a projective plane (not necessarily $PG(2,F)$) of order n. A subset of points $\mathcal{M}$ of π with the property that every line is incident with 0 or r points of $\mathcal{M}$ is called a *maximal arc* of *degree* r. A point, an affine plane and the whole plane π are maximal arcs of degree 1, n and $n+1$ respectively and are known as trivial maximal arcs. In this section we assume that $\mathcal{M}$ is a non-trivial maximal arc.

Proposition 2.10 *The set $\mathcal{M}$ has $rn-n+r$ points and the set of lines $\mathcal{L}$ that are incident with no points of $\mathcal{M}$ is dual to a maximal arc of degree n/r in the dual plane π^*.*

Proof The number of points in $\mathcal{M}$ follows directly by counting the number of points in $\mathcal{M}$ that are incident with a line through a point of $\mathcal{M}$. Let p be a point of π not in $\mathcal{M}$. Then there are $n-n/r+1$ lines incident with p and incident with r points of $\mathcal{M}$ and therefore n/r lines incident with p and incident with no points of $\mathcal{M}$. Hence every point of π is incident with either 0 or n/r of these (external) lines (0-secants).

Note that r divides n and if $n=p^d$ for some prime p then $r=p^e$.

A maximal arc of degree 2 is called a *hyperoval*. The set of external lines to a hyperoval dualise to a maximal arc of degree $q/2$ in the dual plane. We turn our attention for the moment to the case $\pi=PG(2,q)$. The following theorem is Denniston's construction of maximal arcs. It constructs maximal arcs of every feasible order when q is even.

Theorem 2.11 *Let x^2+bx+1 be an irreducible quadratic form over $GF(q)$, $q=2^h$, and let C_λ be a conic in $PG(2,q)$ defined by the equation $x^2+bxy+y^2+\lambda z^2=0$. Let H be a subgroup of order 2^e of the additive group of $GF(q)$. Then the set $\mathcal{M}=\cup_{\lambda\in H}C_\lambda$ is a maximal arc of degree 2^e in $PG(2,q)$.*

Proof The conic C_0 is degenerate and consists of the single point $(0,0,1)$. The other $q-1$ conics C_λ have the common nucleus $(0,0,1)$, are disjoint and cover every point not on the line $z=0$. If L is a line incident with $(0,0,1)$ then it is incident with precisely one point of C_λ for every λ and therefore is incident with 2^e points of $\mathcal{M}$.

Let L be a line not incident with $(0,0,1)$ and assume that L has equation $ax+cy+z=0$. If L has no points incident with C_λ then

$$(1+\lambda a^2)x^2+bxy+(1+\lambda c^2)y^2=0$$

has no solutions in which x and y are not both zero. We make the substitution $v=b^{-1}(1+\lambda a^2)xy^{-1}$ and conclude that

$$v^2+v+b^{-2}(1+\lambda a^2)(1+\lambda c^2)=0$$

has no solutions in $GF(q)$. The function $Tr_{q\to 2}(x)=x+x^2+x^4+\ldots+x^{q/2}\in GF(2)$ for all $x\in GF(q)$. If the above quadratic has no solutions in $GF(q)$ then

$$Tr_{q\to 2}(b^{-2}(1+\lambda a^2)(1+\lambda c^2))=1$$

since $Tr_{q\to 2}(v^2+v)=v+v^q=0$. The quadratic $b^{-2}x^2+b^{-1}x+b^{-2}=0$ has no solutions by assumption from which it follows that $Tr_{q\to 2}(b^{-2})=1$, since $Tr_{q\to 2}(b^{-2}x^2+b^{-1}x)=0$. If $\lambda=\lambda_1$ and $\lambda=\lambda_2$ have the property that

$$Tr_{q\to 2}(b^{-2}\lambda(a^2+c^2)+\lambda^2a^2c^2b^{-2})=0$$

the additive property of the trace function $Tr(x+y)=Tr(x)+Tr(y)$ implies that $\lambda=\lambda_1+\lambda_2$ does too. In characteristic 2 every element is the additive inverse of itself. Therefore the set $G:=\{\lambda\in GF(q)\mid C_\lambda\cap L=\emptyset\}$ forms a subgroup of $GF(q)^+$. The line L is incident with q points not incident with the line $z=0$ and so there are $q/2$ quadratics that have two solutions in $GF(q)$ and $q/2$ that have no solutions, hence $|G|=q/2$.

If $H\leq G$ then $L\cap\mathcal{M}=\emptyset$. If H is not a subgroup of G then $GF(q)^+=HG$ and $H\cap G$ has index 2 in G and therefore $|G\cap H|=2^e/2=2^{e-1}$; the line L meets $\mathcal{M}$ in $2^{e-1}.2=2^e$ points. ■

The only known examples of maximal arcs in $PG(2,q)$ which are not Denniston maximal arcs are the hyperovals, the duals of the external lines to a hyperoval and those constructed by Thas (1974). There are about 10 infinite families of hyperovals in $PG(2,q)$ known, see [1] or [4]. The Thas (1974) maximal arcs are of degree $\sqrt{q}$ where $q=2^{4e+2}$. These are constructed from the Suziki-Tits ovoid via the Hamilton-Quinn-Thas construction which we shall see in Section 3.5. We shall construct the ovoid in Section 4.3.

When q is odd there are no known non-trivial maximal arcs. It has been shown by computer (Penttila and Royle [8]) that none of the planes of order 9 (the smallest planes) contain maximal arcs. When the plane is Desarguesian this is always the case. We need some preliminary lemmas before we prove this.

Lemma 2.12

$$\prod_{\varepsilon^{q+1}=1}(1+\varepsilon T) = 1 - T^{q+1}$$

Proof Let $U = -T^{-1}$. Then

$$\prod_{\varepsilon^{q+1}=1}(1+\varepsilon T) = \prod_{\varepsilon^{q+1}=1} U^{-q-1}(U-\varepsilon) = U^{-q-1}(U^{q+1}-1) = 1 - T^{q+1}.$$

Lemma 2.13 *(Lucas' Theorem) Let p be a prime, $a = a_0 + a_1 p + a_2 p^2 + \ldots$ and $b = b_0 + b_1 p + b_2 p^2 + \ldots$ be integers with $a > 0$. The binomial coefficient*

$$\binom{a}{b} = \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2}\ldots \pmod{p}.$$

Proof The coefficient of x^b in the expansion of $(1+x)^a$ is $\binom{a}{b}$ and modulo p

$$(1+x)^a = (1+x)^{a_0+a_1 p+a_2 p^2+\cdots} = (1+x)^{a_0}(1+x^p)^{a_1}(1+x^{p^2})^{a_2}\ldots.$$

The assertion follows by equating the coefficient of x^b in the above equation.

Lemma 2.14 *If $b \in GF(q)$ for all $b \in \mathcal{B}$ and $B(X) = \prod_{b\in\mathcal{B}}(1-bX)$ then*

$$B(X)\sum_{b\in\mathcal{B}}(1-bX)^{q-1} = -(X - X^q)B'(X),$$

where B' is the derivative of B with respect to X.

Proof By computing the derivative of $B(X)$ and expanding the denominator as an infinite sum we get

$$B'(X) = \left(\sum_{b\in\mathcal{B}}\frac{-b}{1-bX}\right)B(X) = -\left(\sum_{b\in\mathcal{B}}\sum_{i=0}^{\infty} b^{i+1}x^i\right)B(X).$$

Every $b \in \mathcal{B}$ are elements of $GF(q)$ and so $b^q = b$. Hence

$$(X - X^q)\left(\sum_{b\in\mathcal{B}}\sum_{i=0}^{\infty} b^{i+1}X^i\right) = \sum_{b\in\mathcal{B}}\sum_{i=0}^{q-1} b^i X^i = \sum_{b\in\mathcal{B}}(1-bX)^{q-1}.$$

Lemma 2.15 *If*

$$F(T,X) = \prod F_i(T,X)$$

where $F_i(T,x)$ divides some polynomial $G(T)$ for $X = x$ (X is evaluated at some x) then $F(T,x)$ divides $F_X(T,x)G(T)$ where $F_X(T,x)$ denotes the partial derivative of $F(T,X)$ with respect to X evaluated at $X = x$.

Proof We differentiate $F(T,X)$ with respect to X,

$$F_X(T,X) = \sum_i \partial F_i \prod_{j\neq i} F_j = (\sum_i \frac{\partial F_i}{F_i})F.$$

The terms in the denominator are factors of $G(T)$ when we evaluate $X = x$. Hence multiplying the above by $G(T)$ and putting $X = x$ we see the bracket becomes a polynomial in T and that $F(T,x)$ divides $F_X(T,x)G(T)$.

Theorem 2.16 *The only maximal arcs in $PG(2,q)$ when q is odd are the trivial ones.*

Proof Let $\mathcal{M}$ be a maximal arc of degree $r < q$. There is a line external to $\mathcal{M}$ so we may assume that it is a set of points of $AG(2,q)$ and as in Section 1.4 that it is a set of elements of $GF(q^2)$. Define the polynomials F in two variables and σ_k in one variable by

$$F(T,X) := \prod_{b\in\mathcal{M}}(1+(1-bX)^{q-1}T) = \sum_{k=0}^{rq-q+r}\sigma_k T^k$$

where σ_k is the k-th elementary symmetric function of the set of polynomials $\{(1-bX)^{q-1} \mid b \in \mathcal{M}\}$, a polynomial of degree at most $k(q-1)$ in X.

The point $1/x \in GF(q^2) \setminus \mathcal{M}$ is not contained in the arc so every line incident with $1/x$ is incident with either 0 or r points of $\mathcal{M}$. In the multiset

$\{(1/x-b)^{q-1} \mid b \in \mathcal{M}\}$ every element occurs therefore with multiplicity r so that in $F(T,x)$ every factor occurs exactly r times. Therefore $F(T,x)$ is an r-th power.

Every line incident with a point $1/x \in \mathcal{M}$ is incident with exactly $r-1$ other points of $\mathcal{M}$. In the multiset $\{(1/x-b)^{q-1} \mid b \in \mathcal{M}\}$ every $(q+1)$-st root of unity is repeated $r-1$ times and the element 0 appears once. Therefore by Lemma 2.12

$$F(T,x) = \prod_{b \in \mathcal{M}} (1+(1/x-b)^{q-1}x^{q-1}T) = (1-x^{q^2-1}T^{q+1})^{r-1} = (1-T^{q+1})^{r-1}.$$

Finally for $x=0$ the coefficient of T^j in $F(T,0)$ is $\binom{rq-q+r}{j}$ which we can evaluate using Lemma 2.13 and conclude that

$$F(T,0) = (1+T)^{rq-q+r} = 1+T^r-T^q+\ldots+T^{rq-q+r}.$$

The coefficient of T^k for $0<k<r$ in $F(T,x)$ is 0 for all $x \in GF(q^2)$, and so $\sigma_k(x)=0$. The degree of σ_k is at most $k(q-1)<q^2$, so these polynomials are identically zero. The first coefficient of F that is not necessarily identically zero therefore is σ_r. For all $x \in GF(q^2)$ the value of $\sigma_k(x)$, the coefficient of T^k, is zero unless r divides k or $q+1$ divides k. Hence for all $x \in GF(q^2)$ we have

$$F(T,x) = 1+\sum_{i=1}^{q-q/r+1} \sigma_{ir}T^{ir} + \sum_{i=1}^{r-1} \sigma_{i(q+1)}T^{i(q+1)}.$$

The coefficient of T^r in $F(T,0)$ is 1 and therefore $\sigma_r(0)=1$ and importantly it is not identically zero. On the other hand the coefficient of T^r in $(1-T^{q+1})^{r-1}$ is zero. Therefore $\sigma_r(x)=0$ for all $1/x \in \mathcal{M}$ and so the polynomial

$$B(X) := \prod_{b \in \mathcal{M}} (1-bX)$$

divides $\sigma_r(X)$.

The main objective of the proof is to show $(B\hat{\sigma}_r)' \equiv 0$ which will lead swiftly to a contradiction for $p \neq 2$.

The coefficient of T^{q+1} in $F(T,x)$ is $-\binom{r-1}{1} = 1$ for all $1/x \in \mathcal{M}$. Therefore $\sigma_{q+1}(x)=1$. The coefficient of T^{q+1} in $F(T,x)$ is zero for all $x \in GF(q^2) \setminus \mathcal{M}$ and therefore $\sigma_{q+1}(x)=0$.

The polynomial $-\sum_{b\in\mathcal{M}}(1-bX)^{q^2-1}$ is equal to 1 for all $X=x\in\mathcal{M}$ since there are $rq-q+r$ terms in the sum, one of which will be zero the others of which will be 1. For all other elements of $GF(q^2)$ it will be zero, since every term in the sum will be 1. Now σ_{q+1} takes the same values for all $x\in GF(q^2)$ and both are of degree q^2-1. Hence they are the same. The polynomial identity

$$(X-X^{q^2})B'(X)=\sigma_{q+1}(X)B(X)$$

follows by applying Lemma 2.14 to $\mathcal{M}$. We differentiate this, multiply by B and evaluate $X=x\in GF(q^2)$, to get the relation

$$BB'=B^2\sigma'_{q+1}$$

for all $x\in GF(q^2)$.

By Lemma 2.15 $F(T,x)$ divides

$$(1-T^{q+1})F_X(T,x).$$

Define the quotient of this division (dependent on x) to be $Q(T)$ and by computation

$$Q(T)=\sigma'_rT^r+R(T)T^{2r}+\sigma'_{q+1}T^{q+1}$$

where $R(T)$ is an r-th power (considered as a polynomial in T). We have that

$$F(T,x)Q(T)=(1-T^{q+1})F_X(T,x)$$

and by multiplying by $B(x)$ that for all $x\in GF(q^2)$

$$\left(\sum_{i=0}^{q-q/r+1}B(x)\sigma_{ir}T^{ir}\right)Q(T)=(1-T^{q+1})B(x)F_X(T,x).$$

By equating the coefficient of T^{q+1+r} we see that

$$B\sigma_r\sigma'_{q+1}=B(\sigma'_{q+1+r}-\sigma'_r).$$

Note that since $B(X)$ divides $\sigma_r(X)$ we can use the relation that

$$B^2\sigma'_{q+1}=BB'$$

and rearranging terms the above gives

$$B\sigma'_{q+1+r}=(B\sigma_r)'$$

for all $x \in GF(q^2)$. Equating successively the coefficient of $T^{i(q+1)+r}$ for $1 < i < r$ gives

$$B\sigma'_{i(q+1)+r} = B\sigma'_{(i-1)(q+1)+r} = (B\sigma_r)'.$$

Since $|\mathcal{M}| = rq - q + r$ it follows that $\sigma_{(r-1)(q+1)+r} \equiv 0$ and so

$$(B\sigma_r)' = 0$$

for all $x \in GF(q^2)$. The degree of $B\sigma_r$ is at most $(rq - q + r) + r(q-1) < q^2$ it follows that $(B\sigma_r)' \equiv 0$ identically, and hence $B\sigma_r$ is a p-th power. Now $B(X)$ does not have multiple factors so B^{p-1} divides σ_r. The degree of σ_r is at most $r(q-1)$ and it is not identically zero. Therefore $(p-1)(rq - q + r) \leq r(q-1)$ which gives a contradiction for $p > 2$. ∎

A *partial geometry* is a set of points and lines with the following properties.

(PG1) every two points are incident with at most one line;

(PG2) for all anti-flags (p, L) (p a point not incident with the line L) there are exactly α points incident with L and collinear with p.

Proposition 2.17 *Let $\mathcal{S}$ be a partial geometry with $\alpha > 1$. Then every line is incident with a constant $s+1$ number of points and every point is incident with a constant $t+1$ number of lines.*

Proof If two lines L_1 and L_2 are skew the number of lines meeting both L_1 and L_2 is $\alpha|L_1| = \alpha|L_2|$. If L_1 and L_2 are concurrent then the number of lines meeting both L_1 and L_2 is $(\alpha-1)(|L_1|-1) = (\alpha-1)(|L_2|-1)$. Hence since $\alpha > 1$ every line is incident with a constant number of lines. Dually the same argument works. ∎

This also holds for $\alpha = 1$ with some extra conditions. Such a partial geometry is called a *generalised quadrangle* and these geometries will be the topic of Chapter 4.

For more details on partial geometries see de Clerck, Thas and van Maldeghem [5]. The following examples are constructed from maximal arcs.

Example: $S(\mathcal{M})$ Let $\mathcal{M}$ be a non-trivial maximal arc of degree r in a projective plane π of order n. Let the points of $S(\mathcal{M})$ be the points of $\pi \setminus \mathcal{M}$ and the lines be the lines that are incident with r points of $\mathcal{M}$. Then $S(\mathcal{M})$ is a partial geometry with $\alpha = n - n/r + 1 - r$, $s = n - r$ and $t = n - n/r$.

Example: $T_2^*(\mathcal{M})$ Let $\mathcal{M}$ be a non-trivial maximal arc of degree r in a projective plane π or order n which is embedded in $PG(3,q)$ as a subplane. Hence $\pi \cong PG(2,q)$ and $n = q$ and q is necessarily even, by Theorem 2.16. Let the points of $T_2^*(\mathcal{M})$ be the points of $AG(3,q) = PG(3,q) \setminus \pi$ and the lines be the lines of $PG(3,q)$ incident with exactly one point of $\mathcal{M}$. Incidence in the partial geometry is the incidence in the projective space. Let (p,L) be an anti-flag of $T_2^*(\mathcal{M})$. Then the plane spanned by p and L in $PG(3,q)$ meets the plane π in a line M that is incident with r points of $\mathcal{M}$. The lines incident with p and the $r-1$ points of $M \setminus L$ are the only lines of $T_2^*(\mathcal{M})$ that meet the line L. The parameters are $\alpha = r - 1$, $s = q - 1$ and $t = rq - q + r - 1$.

Note that $T_2^*(\mathcal{M})$ is a generalised quadrangle when $\mathcal{M}$ is a hyperoval.

3

Polar spaces

3.1 Dualities and polarities

Recall that the dual V^* of a finite-dimensional vector space V over a commutative field F is a vector space of the same dimension over the field F, and there is thus an inclusion-reversing bijection between the projective space $\mathrm{PG}(n,F)$ and itself; there exists a *duality* of $\mathrm{PG}(n,F)$, an inclusion-reversing bijection of $\mathrm{PG}(n,F)$.

Let π be a duality of $PG(n,F)$. The fundamental theorem of projective geometry says that π is induced by a semilinear transformation T from $V = F^{n+1}$ to its dual space V^*, where T is associated to an automorphism σ of F: that is,

$$\begin{aligned}(\mathbf{v}_1+\mathbf{v}_2)T &= \mathbf{v}_1T+\mathbf{v}_2T,\\ (\alpha\mathbf{v})T &= \alpha^\sigma\mathbf{v}T.\end{aligned}$$

Define a function $b : V \times V \to F$ by the rule

$$b(\mathbf{v},\mathbf{w}) = (\mathbf{v})(\mathbf{w}T),$$

that is, the result of applying the element $\mathbf{w}T$ of V^* to $\mathbf{v}$. Then b is a *sesquilinear form*: it is linear as a function of the first argument, and semilinear as a function of the second — this means that

$$b(\mathbf{v},\mathbf{w}_1+\mathbf{w}_2) = b(\mathbf{v},\mathbf{w}_1)+b(\mathbf{v},\mathbf{w}_2)$$

and

$$b(\mathbf{v},\alpha\mathbf{w}) = \alpha^\sigma b(\mathbf{v},\mathbf{w}).$$

(The prefix "sesqui-" means "one-and-a-half".) If we need to emphasise the anti-automorphism σ, we say that b is σ-sesquilinear. If σ is the identity, then the form is *bilinear*.

The form b is *non-degenerate* if, $b(\mathbf{v},\mathbf{w}) = 0$ for all $\mathbf{w} \in V$ implies $\mathbf{v} = \mathbf{0}$ and, $b(\mathbf{v},\mathbf{w}) = 0$ for all $\mathbf{v} \in V$ implies $\mathbf{w} = \mathbf{0}$.

Theorem 3.1 *Any duality of* $\mathrm{PG}(n,F)$*, for* $n > 1$*, is induced by a non-degenerate* σ*-sesquilinear form on the underlying vector space, where* σ *is an automorphism of* F. ■

Conversely, any non-degenerate sesquilinear form on V induces a duality.

$$U \mapsto U^{\perp} := \{\mathbf{v} \in V : b(\mathbf{v},\mathbf{w}) = 0 \text{ for all } \mathbf{w} \in U\}.$$

Obviously, a duality applied twice is a collineation. The most important types of dualities are those whose square is the identity. A *polarity* of $\mathrm{PG}(n,F)$is a duality $\perp$ which satisfies $U^{\perp\perp} = U$ for all flats U of $\mathrm{PG}(n,F)$.

A sesquilinear form b is *reflexive* if $b(\mathbf{v},\mathbf{w}) = 0$ implies $b(\mathbf{w},\mathbf{v}) = 0$.

Proposition 3.2 *A duality is a polarity if and only if the sesquilinear form defining it is reflexive.*

Proof b is reflexive if and only if

$$\mathbf{v} \in \langle \mathbf{w} \rangle^{\perp} \Rightarrow \mathbf{w} \in \langle \mathbf{v} \rangle^{\perp}.$$

Hence, if b is reflexive, then $U \subseteq U^{\perp\perp}$ for all subspaces U. But by non-degeneracy, $\dim U^{\perp\perp} = \dim V - \dim U^{\perp} = \dim U$; and so $U = U^{\perp\perp}$ for all U. Conversely, given a polarity $\perp$, if $\mathbf{w} \in \langle \mathbf{v} \rangle^{\perp}$, then $\mathbf{v} \in \langle \mathbf{v} \rangle^{\perp\perp} \subseteq \langle \mathbf{w} \rangle^{\perp}$ (since inclusions are reversed). ■

The form b is said to be σ-*Hermitian* if $b(\mathbf{w},\mathbf{v}) = b(\mathbf{v},\mathbf{w})^{\sigma}$ for all $\mathbf{v},\mathbf{w} \in V$. This implies that, for any $\mathbf{v}$, $b(\mathbf{v},\mathbf{v})$ lies in the fixed field of σ. If σ is the identity, such a form (which is bilinear) is called *symmetric*.

A bilinear form b is called *alternating* if $b(\mathbf{v},\mathbf{v}) = 0$ for all $\mathbf{v} \in V$. This implies that $b(\mathbf{w},\mathbf{v}) = -b(\mathbf{v},\mathbf{w})$ for all $\mathbf{v},\mathbf{w} \in V$. (Expand $b(\mathbf{v}+\mathbf{w},\mathbf{v}+\mathbf{w}) = 0$, and note

that two of the four terms are zero.) Hence, if the characteristic is 2, then any alternating form is symmetric (but not conversely); but, in characteristic different from 2, only the zero form is both symmetric and alternating.

Clearly, an alternating or Hermitian form is reflexive. Conversely, we have the following:

Theorem 3.3 *A non-degenerate reflexive σ-sesquilinear form is either alternating, or a scalar multiple of a σ-Hermitian form. In the latter case, if σ is the identity, then the scalar can be taken to be* 1.

The proof of this theorem is quite lengthy and so is not included here. A partial proof can be found in Cameron ([2]).

If b is a non-zero reflexive σ-sesquilinear form then σ^2 is the identity. For every scalar α is a value of b, say $b(\mathbf{v},\mathbf{w}) = \alpha$; then

$$\alpha = b(\mathbf{v},\mathbf{w}) = b(\mathbf{w},\mathbf{v})^\sigma = b(\mathbf{v},\mathbf{w})^{\sigma^2} = \alpha^{\sigma^2}.$$

Let V be a vector space over F. A *quadratic form* on V is a function $f : V \to F$ satisfying

- $f(\lambda\mathbf{v}) = \lambda^2 f(\mathbf{v})$ for all $\lambda \in F$, $\mathbf{v} \in V$;
- $f(\mathbf{v}+\mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w}) + b(\mathbf{v},\mathbf{w})$, where b is bilinear.

Now, if the characteristic of F is not 2, then b is a symmetric bilinear form. Each of f and b determines the other, by

$$b(\mathbf{v},\mathbf{w}) = f(\mathbf{v}+\mathbf{w}) - f(\mathbf{v}) - f(\mathbf{w})$$

and

$$f(\mathbf{v}) = \tfrac{1}{2} b(\mathbf{v},\mathbf{v}),$$

the latter equation coming from the substitution $\mathbf{v} = \mathbf{w}$ in the second defining condition. So nothing new is obtained.

On the other hand, if the characteristic of F is 2, then b is an alternating bilinear form, and f cannot be recovered from b. Indeed, many different quadratic forms correspond to the same bilinear form.

We say that the bilinear form is obtained by *polarisation* of f.

Now, in characteristic different from 2, we can take either quadratic forms or symmetric bilinear forms. For consistency, we will take quadratic forms in this case too. This leaves us with three types of forms to study: alternating bilinear forms; σ-Hermitian forms where σ is not the identity; and quadratic forms.

We have to define the analogue of non-degeneracy for quadratic forms. Of course, we could require that the bilinear form obtained by polarisation is non-degenerate; but this is too restrictive. We say that a quadratic form f is *non-singular* if for all $\mathbf{w} \in V$ $b(\mathbf{v},\mathbf{w}) = 0$ and $f(\mathbf{v}) = 0$ implies $\mathbf{v} = \mathbf{0}$, where b is the associated bilinear form.

If the characteristic is not 2, then non-singularity is equivalent to non-degeneracy of the bilinear form.

Now suppose that the characteristic is 2, and let W be the radical of b. the space on which b is identically zero. The restriction of f to W satisfies

$$\begin{aligned} f(\mathbf{v}+\mathbf{w}) &= f(\mathbf{v}) + f(\mathbf{w}), \\ f(\lambda\mathbf{v}) &= \lambda^2 f(\mathbf{v}). \end{aligned}$$

The field F is called *perfect* if every element is a square. If F is a finite field of characteristic 2 then it is perfect. In this case, f is semilinear, and its kernel is a hyperplane of W. We conclude:

Theorem 3.4 *Let f be a non-singular quadratic form, which polarises to b, over a field F.*

(a) If the characteristic of F is not 2, then b is non-degenerate.

(b) If F is a perfect field of characteristic 2, then the radical of b has rank at most 1.

3.2 Classification of forms

As explained in the last section, we now consider a vector space V of finite rank equipped with a form of one of the following types: a non-degenerate alternating

bilinear form b; a non-degenerate σ-Hermitian form b, where σ is not the identity; or a non-singular quadratic form f. In the third case, we let b be the bilinear form obtained by polarising f; then b is alternating or symmetric according as the characteristic is or is not 2, but b may be degenerate. In the other two cases, we define a function $f : V \to F$ defined by $f(\mathbf{v}) = b(\mathbf{v},\mathbf{v})$ — this is identically zero if b is alternating.

We say that V is *anisotropic* if $f(\mathbf{v}) \neq 0$ for all $\mathbf{v} \neq 0$. Also, V is a *hyperbolic line* if it is spanned by vectors $\mathbf{v}$ and $\mathbf{w}$ with $f(\mathbf{v}) = f(\mathbf{w}) = 0$ and $b(\mathbf{v},\mathbf{w}) = 1$. (The vectors $\mathbf{v}$ and $\mathbf{w}$ are linearly independent, so V has rank 2; so, projectively, it is a "line".)

Theorem 3.5 *A space carrying a form of one of the above types is the direct sum of a number r of hyperbolic lines and an anisotropic space U.*

Proof If V is anisotropic, then there is nothing to prove. (V cannot contain a hyperbolic line.) So suppose that V contains a vector $\mathbf{v} \neq 0$ with $f(\mathbf{v}) = 0$.

We claim that there is a vector $\mathbf{w}$ with $b(\mathbf{v},\mathbf{w}) \neq 0$. In the alternating and Hermitian cases, this follows immediately from the non-degeneracy of the form. In the quadratic case, if no such vector exists, then $\mathbf{v}$ is in the radical of b; but $\mathbf{v}$ is a singular vector, contradicting the non-singularity of f.

Multiplying $\mathbf{w}$ by a non-zero constant, we may assume that $b(\mathbf{v},\mathbf{w}) = 1$.

Now, for any value of λ, we have $b(\mathbf{v},\mathbf{w}-\lambda\mathbf{v}) = 1$. We wish to choose λ so that $f(\mathbf{w}-\lambda\mathbf{v}) = 0$; then $\mathbf{v}$ and $\mathbf{w}$ will span a hyperbolic line. Now we distinguish cases. If b is alternating, then any value of λ works. If b is Hermitian, we have

$$\begin{aligned} f(\mathbf{w}-\lambda\mathbf{v}) &= f(\mathbf{w}) - \lambda b(\mathbf{v},\mathbf{w}) - \lambda^\sigma b(\mathbf{w},\mathbf{v}) + \lambda\lambda^\sigma f(\mathbf{v}) \\ &= f(\mathbf{w}) - (\lambda + \lambda^\sigma); \end{aligned}$$

and there exists λ with $\mathrm{Tr}(\lambda) = f(\mathbf{w})$. Finally, if f is quadratic, we have

$$\begin{aligned} f(\mathbf{w}-\lambda\mathbf{v}) &= f(\mathbf{w}) - \lambda b(\mathbf{w},\mathbf{v}) + \lambda^2 f(\mathbf{v}) \\ &= f(\mathbf{w}) - \lambda, \end{aligned}$$

so we choose $\lambda = f(\mathbf{w})$.

Now let W_1 be the hyperbolic line $\langle \mathbf{v}, \mathbf{w}-\lambda\mathbf{v}\rangle$, and let $V_1 = W_1^\perp$, where orthogonality is defined with respect to the form b. It is easily checked that $V = V_1 \oplus W_1$,

and the restriction of the form to V_1 is still non-degenerate or non-singular, as appropriate. Now the existence of the decomposition follows by induction. ■

The number r of hyperbolic lines is called the *polar rank* or *Witt index* of V. As in Cameron [2] we will call U the *germ* of V.

To complete the classification of forms over a given field, it is necessary to determine all the anisotropic spaces.

The alternating case is trivial:

Proposition 3.6 *The only anisotropic space carrying an alternating bilinear form is the zero space.* ■

In combination with Theorem 3.5, this shows that a space carrying a non-degenerate alternating bilinear form is a direct sum of hyperbolic lines.

Theorem 3.7 *(a) An anisotropic quadratic form in n variables over* $\mathrm{GF}(q)$ *exists if and only if* $n \leq 2$. *There is a unique form for each n except when* $n = 1$ *and q is odd, in which case there are two forms, one a non-square multiple of the other.*

(b) Let q be square and let σ *be the field automorphism* $\alpha \mapsto \alpha^{\sqrt{q}}$. *Then there is an anisotropic* σ*- Hermitian form in n variables if and only if* $n \leq 1$. *The form is unique in each case.*

Proof (a) Consider first the case where the characteristic is not 2. The multiplicative group of $\mathrm{GF}(q)$ is cyclic of even order $q-1$; so the squares form a subgroup of index 2, and if η is a fixed non-square, then every non-square has the form $\eta\alpha^2$ for some α. It follows easily that any quadratic form in one variable is equivalent to either x^2 or ηx^2.

Next, consider non-singular forms in two variables. By completing the square, such a form is equivalent to one of x^2+y^2, $x^2+\eta y^2$, $\eta x^2+\eta y^2$.

Suppose first that $q \equiv 1 \pmod 4$. Then -1 is a square, say $-1 = \beta^2$. Thus $x^2 + y^2 = (x+\beta y)(x-\beta y)$, and the first and third forms are not anisotropic. Moreover, any form in 3 or more variables, when converted to diagonal form, contains one of these two, and so is not anisotropic either.

Now consider the other case, $q \equiv -1 \pmod 4$. Then -1 is a non-square, so the second form is $(x+y)(x-y)$, and is not anisotropic. Moreover, the set of squares is not closed under addition (else it would be a subgroup of the additive group, but $\frac{1}{2}(q+1)$ doesn't divide q); so there exist two squares whose sum is a non-square. Multiplying by a suitable square, there exist β,γ with $\beta^2+\gamma^2=-1$. Then

$$-(x^2+y^2) = (\beta x+\gamma y)^2+(\gamma x-\beta y)^2,$$

and the first and third forms are equivalent. Moreover, a form in three variables is certainly not anisotropic unless it is equivalent to $x^2+y^2+z^2$, and this form vanishes at the vector $(\beta,\gamma,1)$; hence there is no anisotropic form in three or more variables.

The characteristic 2 case is an exercise.

(b) Now consider Hermitian forms. If σ is an automorphism of $\mathrm{GF}(q)$ of order 2, then q is a square and $\alpha^\sigma = \alpha^{\sqrt{q}}$. Every element of $\mathrm{GF}(\sqrt{q})$ has the form $\alpha\alpha^\sigma$.

In one variable, we have $f(x) = \mu x x^\sigma$ for some non-zero $\mu \in GF(\sqrt{q})$; writing $\mu = \alpha\alpha^\sigma$ and replacing x by αx, we can assume that $\mu = 1$.

In two variables, we can similarly take the form to be $xx^\sigma + yy^\sigma$. Now $-1 \in \mathrm{GF}(\sqrt{q})$, so $-1 = \lambda\lambda^\sigma$; then the form vanishes at $(1,\lambda)$. It follows that there is no anisotropic form in any larger number of variables either. ■

3.3 Classical polar spaces

Polar spaces describe the geometry of vector spaces carrying a reflexive sesquilinear form or a quadratic form in much the same way as projective spaces describe the geometry of vector spaces.

The polar spaces associated with the three types of forms (alternating bilinear, Hermitian, and quadratic) are referred to by the same names as the groups associated with them: *symplectic*, *unitary*, and *orthogonal* respectively. Of what do these spaces consist?

Let V be a vector space carrying a form of one of our three types. Recall that as well as a sesquilinear form b in two variables, we have a form f in one variable (either f is defined by $f(\mathbf{v}) = b(\mathbf{v},\mathbf{v})$, or b is obtained by polarising f) and we make use of both forms. A subspace of V on which b vanishes identically is called

a *totally isotropic subspace*, while a subspace on which f vanishes identically is called a *totally singular subspace*. Every totally isotropic subspace is totally singular, but the converse is false. In the case of alternating forms, every subspace is totally singular.

The *classical polar space* (or simply the *polar space*) associated with a vector space carrying a form is the geometry whose flats are the totally isotropic or totally singular subspaces (in the above sense). Note that, if the form is anisotropic, then the only member of the polar space is the zero subspace. The *polar rank* of a classical polar space is the largest vector space rank of any totally isotropic or totally singular subspace; it is zero if and only if the form is anisotropic. Where there is no confusion, polar rank will be called simply *rank*. We use the terms *point, line, plane*, etc., just as for projective spaces.

The rank of the polar space is the same as the polar rank of V. Consider V as the direct sum of r hyperbolic lines and an anisotropic space. By Theorem 3.5 any totally isotropic or totally singular subspace meets each hyperbolic line in at most a point and meets the anisotropic subspace in the zero subspace; so it's rank is at most r.

In a polar space G, for any set S of points, we let $S^\perp$ denote the set of points which are perpendicular to (that is, collinear with) every point of S. For any set S, the set $S^\perp$ is a (linear) subspace of G (that is, if two points of $S^\perp$ are collinear, then the line joining them lies wholly in $S^\perp$). Moreover, for any point x, $x^\perp$ is a hyperplane of G (that is, a subspace which meets every line).

Polar spaces have good inductive properties. Let G be a classical polar space. There are two natural ways of producing a "smaller" polar space from G:

(a) Take a point x of G, and consider the quotient space $x^\perp/x$, the space whose points, lines, ... are the lines, planes, ... of G containing x.

(b) Take two non-perpendicular points x and y, and consider $\{x,y\}^\perp$.

In each case, the space constructed is a classical polar space, having the same germ as G but with polar rank one less than that of G. (Note that, in (b), the span of x and y in the vector space is a hyperbolic line.) There are more general versions. For example, if S is a flat of dimension $d-1$, then $S^\perp/S$ is a polar space of rank $r-d$ with the same germ as G. We will see how this inductive process can be used to obtain information about polar spaces.

The classification of finite classical polar spaces was achieved by Theorem 3.5 and Theorem 3.7. We subdivide these spaces into six families according to their germ, viz., one symplectic, two unitary, and three orthogonal. (Forms which differ only by a scalar factor obviously define the same polar space.) The following table gives some information about them. In the table, r denotes the polar space rank, n the vector space rank. The significance of the parameter ε will emerge shortly. This number, depending only on the germ, carries numerical information about all spaces in the family. Note that, in the unitary case, the order of the finite field must be a square.

Type	n	ε	Group		Label
Symplectic	$2r$	0	$Sp(n,q)$		$W_{n-1}(q)$
Unitary	$2r$	$-\frac{1}{2}$	$U(n,q)$		$H_{n-1}(q)$
Unitary	$2r+1$	$\frac{1}{2}$	$U(n,q)$		$H_{n-1}(q)$
Orthogonal	$2r$	-1	$O^+(n,q)$	Hyperbolic	$Q^+_{n-1}(q)$
Orthogonal	$2r+1$	0	$O(n,q)$	Parabolic	$Q_{n-1}(q)$
Orthogonal	$2r+2$	1	$O^-(n,q)$	Elliptic	$Q^-_{n-1}(q)$

Table 3.1: Finite classical polar spaces

Theorem 3.8 *The number of points in a finite polar space of rank* 1 *is* $q^{1+\varepsilon}+1$, *where* ε *is given in Table 3.1.*

Proof Let V be a vector space carrying a form of rank 1 over GF(q). Then V is the orthogonal direct sum of a hyperbolic line L and an anisotropic germ U of dimension k (say). Let n_k be the number of points.

Suppose that $k > 0$. If p is a point of the polar space, then p lies on the hyperplane $p^\perp$; any other hyperplane containing p is non-degenerate with polar rank 1 and having germ of dimension $k-1$. Consider a parallel class of hyperplanes in the affine space whose hyperplane at infinity is $p^\perp$. Each such hyperplane contains $n_{k-1}-1$ points, and the hyperplane at infinity contains just one, namely p. So we have

$$n_k - 1 = q(n_{k-1}-1),$$

from which it follows that $n_k = 1+(n_0-1)q^k$. So it is enough to prove the result for the case $k = 0$, that is, for a hyperbolic line.

In the symplectic case, each of the $q+1$ projective points on a line is isotropic.

Consider the unitary case. We can take the form to be

$$b(\mathbf{x},\mathbf{y}) = x_1 y_1^{\sqrt{q}} + x_2 y_2^{\sqrt{q}}.$$

So the isotropic points satisfy $x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} = 0$, and a hyperbolic line is incident with $\sqrt{q}+1$ projective points.

Finally, consider the orthogonal case. The quadratic form is equivalent to x_1x_2, and has two singular points, $\langle(1,0)\rangle$ and $\langle(0,1)\rangle$. ∎

Theorem 3.9 *In a finite polar space of rank r, there are $(q^r-1)(q^{r+\varepsilon}+1)/(q-1)$ points, of which $q^{2r-1+\varepsilon}$ are not perpendicular to a given point.*

Proof We let $F(r)$ be the number of points, and $G(r)$ the number not perpendicular to a given point. (We do not assume that $G(r)$ is constant; this constancy follows from the induction that proves the theorem.)

Take a point x, and count pairs (y,z), where $y \in x^\perp$, $z \notin x^\perp$, and $z \in y^\perp$. Choosing z first, there are $G(r)$ choices; then $\langle x,z\rangle$ is a hyperbolic line, and y is a point in $\langle x,z\rangle^\perp$, so there are $F(r-1)$ choices for y. On the other hand, choosing y first, the lines through y are the points of the rank $r-1$ polar space $x^\perp/x$, and so there are $F(r-1)$ of them, with q points different from x on each, giving $qF(r-1)$ choices for y; then $\langle x,y\rangle$ and $\langle y,z\rangle$ are non-perpendicular lines in $y^\perp$, i.e., points of $y^\perp/y$, so there are $G(r-1)$ choices for $\langle y,z\rangle$, and so $qG(r-1)$ choices for z. Thus

$$G(r)\cdot F(r-1) = qF(r-1)\cdot qG(r-1),$$

from which it follows that $G(r) = q^2G(r-1)$.

Since $G(1) = q^{1+\varepsilon}$, it follows immediately that $G(r) = q^{2r-1+\varepsilon}$, as required.

The points perpendicular to x lie on lines that are points of $x^\perp/x$ and the remaining points are not perpendicular to x. Hence $F(r) = 1 + qF(r-1) + G(r)$.

Now it is just a matter of calculation that the function $(q^r-1)(q^{r+\varepsilon}+1)/(q-1)$ satisfies the recurrence and correctly reduces to $q^{1+\varepsilon}+1$ when $r=1$. ∎

Theorem 3.10 *The number of maximal flats in a finite polar space of rank r is*

$$\prod_{i=1}^{r}(1+q^{i+\varepsilon}).$$

Proof Let $H(r)$ be this number. Count pairs (x,U), where U is a maximal flat and $x \in U$. We find that

$$F(r) \cdot H(r-1) = H(r) \cdot (q^r - 1)/(q-1),$$

so

$$H(r) = (1 + q^{r+\varepsilon})H(r-1).$$

Now the result is immediate. ■

3.4 The polar geometries of finite fields

We consider polar geometries in finite fields as was done in Section 1.4 for the projective and affine spaces. The field $GF(q^n)$ is the vector space of rank n over $GF(q)$ carrying a form.

The polynomial in two variables defined by

$$b(x,y) = \sum_{i=0}^{n-1} Tr_{q^n \to q}(\alpha_i y^{q^i} x)$$

is a bilinear form. The total number of bilinear forms (including degenerate ones) is q^{n^2} and there are exactly this many possibilities for $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$. Hence we conclude that any bilinear form on $GF(q^n)$ can be written as above.

Let us consider first the alternating case, $n = 2r$ and $b(x,y) = -b(y,x)$. The coefficients satisfy

$$\alpha_0 = -\alpha_0 \text{ and } \alpha_{n-j} = -\alpha_j^{q^{n-j}}.$$

If the form is degenerate then there exists a $y \in GF(q^n)$ such that

$$\sum_{i=0}^{n-1} \alpha_i y^{q^i} = 0.$$

We saw in Section 1.4 that this is the equation defining a hyperplane of $PG(n-1,q)$ and that the matrix $B = (b_{ij})$ defined by $b_{ij} = \alpha_{j-i}^{q^i}$, where the indices are taken modulo n, does not have full rank, i.e. the determinant of B is zero. We can choose a canonical form for a non-degenerate alternating form by setting $\alpha_j = 0$ for $j \neq r$ and then

$$b(x,y) = Tr_{q^n \to q}(\gamma y^{q^r} x)$$

where $\gamma^{q^r} = -\gamma$. Note that when q is even we can choose $\gamma = 1$.

The polynomial

$$b(x,y) = \sum_{i=0}^{n-1} Tr_{q^n \to q}(\alpha_i x y^{q^{i+1/2}})$$

is a Hermitian form if $b(x,y) = b(y,x)^{q^{1/2}}$. The coefficients satisfy

$$\alpha_{n-i-1} = \alpha_i^{q^{n-i-1/2}}.$$

The form is degenerate if there exists a $y \in GF(q^n)$ such that

$$\sum_{i=0}^{n-1} \alpha_i y^{q^{i+1/2}} = 0.$$

As in the alternating case this implies that the matrix B has zero determinant. If $n = 2r+1$ then we can choose a canonical form for a non-degenerate Hermitian form by setting $\alpha_j = 0$ for $j \neq r$ and $\alpha_r = 1$ and then

$$b(x,y) = Tr_{q^n \to q}(y^{q^{r+1/2}} x).$$

If $n = 2r$ then we choose a canonical form for a non-degenerate Hermitian form by setting $\alpha_j = 0$ for $j \neq r-1, r$ and $\gamma = \alpha_r = \alpha_{r-1}^{q^{r+1/2}}$ where γ is chosen so that $\gamma^{q^{r-1/2}} y^{q^{r-1/2}} + \gamma y^{q^{r+1/2}} = 0$ has no solutions in $GF(q^n)$. Let $z = y^{q^{r-1/2}}$ then $\gamma^{q^{r-1/2}} z + \gamma z^q = 0$ which we saw in Section 1.4 has solutions if and only if

$$\gamma^{(q^{r-1/2}-1)(1+q+q^2+\ldots+q^{n-1})} = 1.$$

Hence we choose γ so that $\gamma^{(q^{r-1/2}-1)(1+q+q^2+\ldots+q^{n-1})} \neq 1$ and a non-degenerate Hermitian form

$$b(x,y) = Tr_{q^n \to q}(\gamma^{q^{r-1/2}} y^{q^{r-1/2}} + \gamma y^{q^{r+1/2}} x).$$

The polynomial

$$f(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} Tr_{q^n \to q}(\alpha_i x^{q^i+1})$$

defines a quadratic form over $GF(q)$. If n is even then the coefficient of $x^{q^{n/2+j}+q^j}$ is $\alpha_{n/2}^{q^j} + \alpha_{n/2}^{q^{j+n/2}} \in GF(q^{n/2})$. If n is odd the number of quadratic forms that can

be written like this is $q^{\binom{n}{2}}$ and if q is even it is also $q^{n(n/2-1)+n/2} = q^{\binom{n}{2}}$. This is the total number of quadratic forms and so any quadratic form can be written as above. The bilinear form associated to the quadratic form is

$$b(x,y) = \sum_{i=0}^{\lfloor n/2 \rfloor} Tr_{q^n \to q}(\alpha_i(x^{q^i}y + y^{q^i}x)).$$

By the definition in Section 3.1 the form f is degenerate if there is an x such that

$$\alpha_i x^{q^i} + \alpha_i^{q^{n-i}} x^{q^{n-1}} = 0$$

for $i = 1,2,\ldots,\lfloor n/2 \rfloor$ **and** $f(x) = 0$.

If $n = 2r+1$ then we choose $\alpha_j = 0$ for $j \neq r$ and $\alpha_r = 1$ and hence

$$f(x) = Tr_{q^n \to q}(x^{q^r+1}).$$

We have to check non-singularity. If the form is singular then there exists an x such that $b(x,y) \equiv 0$ and $f(x) = 0$.

$$b(x,y) = Tr_{q^n \to q}(x^{q^r}y + y^{q^r}x) = Tr_{q^n \to q}(x^{q^r} + x^{q^{r+1}})y) \equiv 0$$

if and only if $x^q + x = 0$. The form $f(x)$ on these elements is equal to $(-1)^r x^2 \neq 0$. Note that when q is even the set of x satisfying $x^q = -x$ is a point of $PG(n-1,q)$; this is the nucleus.

If $n = 2r+2$ and we wish to find an elliptic form then we choose $\alpha_j = 0$ for $j \neq r+1$ and $\alpha_{r+1} = \gamma$ where $\gamma + \gamma^{q^{r+1}} = 1$. If the form is singular then there exists an x such that

$$b(x,y) = Tr_{q^n \to q}(\gamma(x^{q^{r+1}}y + y^{q^{r+1}}x)) = Tr_{q^n \to q}(\gamma x^{q^{r+1}} + \gamma^{q^{r+1}}x^{q^{r+1}})y) \equiv 0.$$

However by assumption $\gamma + \gamma^{q^{r+1}} = 1$. We can check that the form is elliptic by checking the number of distinct zeros of f. The degree of f is $q^{2r+1} + q^r$ and the leading term is of degree $q^{r+1}+1$. Therefore the number of zeros of f is at most $(q^{r+1}+1)(q^r-1)$ and the number of points in the polar space defined by f is at most $(q^{r+1}+1)(q^r-1)/(q-1)$. However the hyperbolic polar space has more points than this and indeed this is equal to the number of points in the elliptic polar space.

Type	n	ε	Canonical form	Condition
Alternating	$2r$	0	$Tr_{q^n\to q}(\gamma y^{q^r}x)$	$\gamma^{q^r}=-\gamma$
Hermitian	$2r$	$-\frac{1}{2}$	$Tr_{q^n\to q}(\gamma y^{q^{r+1/2}}x+\gamma^{q^{r-1/2}}y^{q^{r-1/2}}x)$	see notes
Hermitian	$2r+1$	$\frac{1}{2}$	$Tr_{q^n\to q}(y^{q^{r+1/2}}x)$	
Quadratic$^+$	$2r$	-1	$Tr_{q^n\to q}(\alpha x^{q^{r-1}+1}+\gamma x^{q^r+1})$	see notes
Quadratic	$2r+1$	0	$Tr_{q^n\to q}(x^{q^r+1})$	
Quadratic$^-$	$2r+2$	1	$Tr_{q^n\to q}(\gamma x^{q^{r+1}+1})$	$\gamma^{q^{r+1}}+\gamma=1$

Table 3.2: The sesquilinear and quadratic forms on $GF(q^n)$

If $n=2r$ and we wish to find a hyperbolic form then we choose $\alpha_j=0$ for $j\neq r-1,r$, $\alpha_{r-1}=\alpha$ and $\alpha_r=\gamma$. The form is non-singular if there is no x such that both $b(x,y)\equiv 0$ and $f(x)=0$. If

$$b(x,y)=Tr_{q^n\to q}(\alpha(x^{q^{r-1}}y+y^{q^{r-1}}x)+\gamma(x^{q^r}y+y^{q^r}x))=$$

$$Tr_{q^n\to q}(\alpha x^{q^{r-1}}+\alpha^{q^{r+1}}x^{q^{r+1}}+\gamma x^{q^r}+\gamma^{q^r}x^{q^r})y)\equiv 0$$

then

$$\alpha^{q^{r+1}}x+(\gamma+\gamma^{q^r})x^q+\alpha^{q^2}x^{q^2}=0.$$

Now we have to select α and γ so that this equation has no zeros. If $n=4$ one can choose $\gamma=0$ and $\alpha^{q^3+q}\neq\alpha^{q^2+1}$.

3.5 *m*-systems

An *partial m-system* $\mathcal{M}$ of a finite classical polar space $\mathcal{G}$ of rank r is a set of totally singular (projective) m-spaces of $\mathcal{G}$ with the property that any totally singular subspace of rank r (projective $(r-1)$-space) containing an element of $\mathcal{M}$ is disjoint from any other element of $\mathcal{M}$.

The set $\mathcal{M}_0$ is the set of points that are incident with an element of $\mathcal{M}$.

Theorem 3.11 *A partial m-system $\mathcal{M}$ of a finite classical polar space $\mathcal{G}$ of rank r and type ε satisfies $|\mathcal{M}| \leq q^{r+\varepsilon}+1$.*

Proof We assume $m < r-1$ since for $m = r-1$ the bound is obvious from Theorem 3.9.

For every point $p_i \in \mathcal{G} \setminus \mathcal{M}_0$ let t_i be the number of totally singular $(m+1)$-spaces of $\mathcal{G}$ containing p_i and an element of $\mathcal{M}$.

The number of ordered pairs (p_i, ξ) where ξ is a totally singular $(m+1)$-space containing p_i and an element of $\mathcal{M}$ is

$$\sum t_i = |\mathcal{M}| q^{m+1} F(r-m-1),$$

where $F(r)$ is number of points in a polar space of rank r as in Theorem 3.9.

The number of triples (p_i, ξ, ξ') where ξ and ξ' are totally singular $(m+1)$-spaces containing p_i and an element of $\mathcal{M}$ is

$$\sum t_i(t_i-1) = |\mathcal{M}|(|\mathcal{M}|-1)F(r-m-1).$$

The number N of points $p_i \in \mathcal{G} \setminus \mathcal{M}_0$ is

$$F(r) - |\mathcal{M}|(q^{m+1}-1)/(q-1).$$

Apply the inequality $N\sum t_i^2 - (\sum t_i)^2 \geq 0$ to the above equations and use Theorem 3.9 to conclude that

$$(|\mathcal{M}| - q^{r+\varepsilon} - 1)(1 - |\mathcal{M}| - q^r) \geq 0.$$

■

We call a partial m-system of size $q^{r+\varepsilon}+1$ an *m-system*. If we have an m-system then the inequality in the proof is in fact an equality which implies that every point not in $\mathcal{M}_0$ lies on a constant number of totally singular $(m+1)$-spaces that contain an element of $\mathcal{M}$. It is a simple matter to calculate this constant and we have the following.

Theorem 3.12 *Let $\mathcal{M}$ be an m-system of a finite classical polar space of rank r, with $m < r-1$ and let $\mathcal{M}_0$ be the set of points that are incident with an element of $\mathcal{M}$. A point that is not in $\mathcal{M}_0$ is incident with precisely $q^{r-m-1+\varepsilon}+1$ totally singular $(m+1)$-spaces that contain an element of $\mathcal{M}$.*

A 0-system is called an *ovoid* and an $(r-1)$-system is called a *spread*.

Theorem 3.13 *Let $\mathcal{M}$ be an m-system of a finite classical polar space and let $\mathcal{M}_0$ be the set of points that are incident with an element of $\mathcal{M}$. Every maximal totally isotropic subspace is incident with precisely $(q^{m+1}-1)/(q-1)$ points of $\mathcal{M}_0$.*

Proof Let t_i be the number of points of $\mathcal{M}_0$ incident with a maximal totally isotropic subspace γ_i. The quotient space of each isotropic point is a polar space of rank one less and so

$$\sum t_i = |\mathcal{M}_0|H(r-1),$$

where $H(r)$ is as in Theorem 3.10. We shall count triples (x,y,γ_i) where x and y are elements of $\mathcal{M}_0$ incident with γ_i. Let $\perp$ denote the polarity. The points x and y are orthogonal $y \in x^\perp$, and either lie in the same element of the m-system or not. In both cases the number of maximal totally isotropic subspaces is equal to the number of maximal totally isotropic subspaces in their quotient space. The hyperplane $x^\perp$ meets every element of the m-system, excepting that which is incident with x, in an $(m-1)$-dimensional subspace. Hence

$$\sum t_i(t_i-1) = |\mathcal{M}_0|H(r-2)(q(q^m-1)/(q-1)+q^{r+\varepsilon}(q^m-1)/(q-1)).$$

Now we can calculate

$$H(r)\sum t_i^2 - (\sum t_i)^2$$

and conclude that this is zero. Hence the $t_i = t$ are constant,

$$H(r)t = |\mathcal{M}_0|H(r-1),$$

and substituting from Theorem 3.10 concludes the proof. ∎

A symplectic spread of $PG(2n-1,q)$ is a spread of the symplectic polar space of $V(2n,q)$. The translation plane constructed from the spread as in Proposition 2.1 is called a *symplectic translation plane*. The Hamilton-Quinn-Thas construction of maximal arcs in symplectic translation planes require the existence of certain m-systems of the symplectic polar space.

Theorem 3.14 *Let V be a vector space of rank $2n$ with an alternating form, let $W_{2n-1}(q)$ denote the associated symplectic polar space and let $PG(2n-1,q)$ denote the (ambient) projective space. Let $\mathcal{M}$ be an m-system of $W_{2n-1}(q)$ with the*

property that each element of $\mathcal{M}$ is contained in an element of $\mathcal{S}$, an $(n-1)$-system (a spread) of $W_{2n-1}(q)$. Embed $PG(2n-1,q)$ in $PG(2n,q)$ and choose a point $x \in PG(2n,q) \setminus PG(2n-1,q)$, and let $\mathcal{K}$ be the set of affine points on the cone with vertex x and base $\mathcal{M}_0$. The set $\mathcal{K}$ defines a maximal arc of degree q^{m+1} in the translation plane of order q^n associated to the spread $\mathcal{S}$.

Proof We have to show that every subspace Σ' of $PG(2n,q)$ of dimension n that contains an element S of $\mathcal{S}$ is incident with either 0 or q^{m+1} points of $\mathcal{K}$. If Σ' is incident with x then Σ' contains the affine part of the cone with vertex x and base M_S, where M_S is the element of the m-system contained in S. Hence Σ' is incident with q^{m+1} points of $\mathcal{K}$. From now on assume that Σ' is not incident with x. We have to show that Σ, the projection of Σ from x, a subspace of $PG(2n-1,q)$ of dimension n that contains an element $S \in \mathcal{S}$, is incident with either 0 or q^{m+1} points of $\mathcal{M}_0 \setminus S$.

Let $\perp$ be the polarity of $W_{2n-1}(q)$. The subspace $\Sigma^\perp$ is a subspace of dimension $n-2$ contained in Σ. If $\Sigma^\perp \supset M_S$ then $(\Sigma^\perp)^\perp = \Sigma \subset M_S^\perp$ and Σ is incident with no point of $\mathcal{M}_0 \setminus S$ since by definition the perp-space of an element of an m-system is disjoint from all the other elements of the m-system. If $\Sigma^\perp$ does not contain M_S then $\Sigma^\perp \cap M_S$ is a subspace of dimension $m-1$. Let $\mathcal{A}$ be the set of $q+1$ totally isotropic subspaces of dimension $n-1$ such that $A \in \mathcal{A}$ implies $\Sigma^\perp \subset \mathcal{A} \subset \Sigma$, and note $S \in \mathcal{A}$. Every subspace in $\mathcal{A} \setminus \{S\}$ is incident with exactly $(q^m-1)/(q-1)$ points of M_S, the points of the subspace $\Sigma^\perp \cap M_S$. By Theorem 3.13 the totally isotropic subspaces of dimension $n-1$ are incident with $(q^{m+1}-1)/(q-1)$ points of $\mathcal{M}_0$. Hence the subspaces in $\mathcal{A} \setminus \{S\}$ are incident with $((q^{m+1}-1)-(q^m-1))/(q-1) = q^m$ points of $\mathcal{M}_0 \setminus S$. Moreover the sets $\mathcal{A} \setminus S$ are disjoint and cover $\Sigma \setminus S$ and so Σ is incident with $q.q^m = q^{m+1}$ points of $\mathcal{M}_0 \setminus S$. ∎

For applications of the Hamilton-Quinn-Thas construction see [6]. An up-to-date survey of m-systems can be found in [10].

4

Generalised quadrangles

4.1 Axioms

Consider a rank 2 geometry with the following properties.

(Q1) Every two points are incident with at most one line;

(Q2) For all anti-flags (p, L) (the point p is not incident with the line L) there is exactly one point incident with L and collinear with p.

We have already seen these axioms in Section 2.4. A generalised quadrangle is a partial geometry with $\alpha = 1$ which satisfies a further axiom.

(Q3) There is no point collinear with all others.

The axioms (Q1)–(Q3) are self-dual; so the dual of a generalised quadrangle is also a generalised quadrangle.

Two simple classes of examples are provided by the *complete bipartite graphs*, whose points fall into two disjoint sets (with at least two points in each, and whose lines consist of all pairs of points containing one from each set), and their duals, the *grids*. Any generalised quadrangle in which lines have just two points is a complete bipartite graph, and dually. We note that any line contains at least two points, and dually: if L were a singleton line $\{p\}$, then every other point would be collinear with p (by (Q2)), contradicting (Q3).

Apart from complete bipartite graphs and grids, all generalised quadrangles have orders. The following is analogous to Proposition 2.17 for $\alpha = 1$.

Proposition 4.1 *Let G be a generalised quadrangle in which there is a line incident with at least three points and a point incident with at least three lines. Then the number of points incident with a line, and the number of lines incident with a point, are constants.*

Proof First observe that, if lines L_1 and L_2 are disjoint, then they have the same cardinality; for collinearity sets up a bijection between the points on L_1 and those on L_2.

Now suppose that L_1 and L_2 intersect. Let p be a point on neither of these lines. Then one line through p meets L_1, and one meets L_2. We want to show that there a line L_3 disjoint from both L_1 and L_2. The points on L_1 and L_2 together with p generate a grid using axioms (Q1) and (Q2). However there is a point on 3 lines by assumption so there is a line L_3 disjoint from both L_1 and L_2. It follows that L_1 and L_2 both have the same cardinality as L_3.

The other assertion is proved dually. ■

We say G is a generalised quadrangle of order s, t if every line is incident with $s+1$ points and every point is incident with $t+1$ lines.

The classical generalised quadrangles are the classical polar spaces of rank 2 over $\mathrm{GF}(q)$. The parameters are $s = q$ and $t = q^{1+\varepsilon}$, where ε is given in Table 3.1.

We have already seen a way to construct generalised quadrangles that are not classical. In Section 2.4 $T_2^*(\mathcal{H})$, where $\mathcal{H}$ is a hyperoval is a generalised quadrangle with parameters $s = q-1$ and $t = q+1$, $q = 2^h$. There are many other constructions of non-classical generalised quadrangles known. See for example [5] or [7].

Theorem 4.2 *Let G be a finite GQ with orders s,t.*

(a) G has $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines.

(b) $s+t$ divides $st(s+1)(t+1)$;

(c) if $s > 1$, then $t \leq s^2$;

(d) if $t > 1$, then $s \leq t^2$.

Proof (a) is proved by elementary counting. (b) is shown by an argument involving eigenvalues of matrices. (c) is proved by elementary counting and (d) is dual to (c). ■

4.2 The symplectic generalised quadrangle

The symplectic generalised quadrangle and the orthogonal parabolic generalised quadrangle have the same parameters $s = t = q$. Indeed there is an isomorphism between the dual of $W_3(q)$ and $Q_4(q)$. Before we prove this isomorphism we introduce the Klein correspondence.

Let $\mathbf{x}, \mathbf{y} \in V(4,q)$. The *Plücker coordinates* are defined for $1 \leq i < j \leq 4$ by

$$p_{ij} = x_i y_j - y_i x_j.$$

The vector $\mathbf{p} = (p_{13}, p_{24}, p_{14}, p_{23}, p_{12}, p_{34}) \in V(6,q)$ is a zero of the quadratic form $f(\mathbf{x}) = x_1x_2 - x_3x_4 + x_5x_6$. Moreover the Plücker coordinates for $(\mathbf{x}, \mathbf{y})$ are the same as those for $(\mathbf{x}, \mathbf{y} + \lambda\mathbf{x})$ for $\lambda \in F$. Hence there is a correspondence (the *Klein correspondence*) between the rank 2 subspaces of $V(4,q)$ and the zeros of a hyperbolic quadratic form on $V(6,q)$. Projectively this is a correspondence between the lines of $PG(3,q)$ and the points of the hyperbolic quadric $Q_5^+(q)$, which is known as the *Klein quadric*.

Theorem 4.3 *The dual of the symplectic generalised quadrangle is isomorphic to the parabolic generalised quadrangle, dual of $W_3(q) \cong Q(4,q)$, and vice-versa.*

Proof Let $W_3(q)$ denote the symplectic generalised quadrangle with an alternating form given by

$$b(\mathbf{x}, \mathbf{y}) = x_1y_2 - y_1x_2 + x_3y_4 - y_3x_4 = p_{12} + p_{34}.$$

The Plücker coordinates of the totally isotropic lines (the lines of $W_3(q)$) satisfy $p_{12} = -p_{34}$. Hence these lines correspond to the zeros of the form on $V(5,q)$ given by $g(\mathbf{x}) = x_1x_2 - x_3x_4 - x_5^2$. ■

We can also look at the symplectic generalised quadrangle in the finite field $GF(q^4)$. Firstly a point of the symplectic generalised quadrangle is a point of $PG(3,q)$ and in Section 1.4 we saw that

$$\{x \in GF(q^4) \mid x^q - ax = 0\}$$

is a point of $PG(3,q)$ if and only if $a^{q^3+q^2+q+1} = 1$. Hence it makes sense to replace x^{q-1} by x and to take for the set of points of the symplectic generalised quadrangle the set

$$\{x \in GF(q^4) \mid x^{q^3+q^2+q+1} = 1\}.$$

In Section 3.4 we calculated a canonical form for an alternating form on $GF(q^4)$,

$$b(x,y) = Tr_{q^4 \to q}(\gamma x^{q^2} y)$$

where $\gamma^{q^2} = -\gamma$. In Section 1.4 (Exercise 1) a line $\mathcal{L}$ of $PG(3,q)$ is

$$\{x \in GF(q^4) \mid x^{q^2} + cx^q + ex = 0\}$$

where $e^{q^3+q^2+q+1} = 1$ and $c^{q+1} = e^q - e^{q^2+q+1}$. Let x and y be orthogonal, the form $b(x,y) = 0$, and satisfy $x^{q^2} + cx^q + ex = 0$ and $y^{q^2} + cy^q + ey = 0$. We can deduce that

$$(x^q y - y^q x)e = x^{q^2} y^q - y^{q^2} x^q \quad \text{and} \quad (x^q y - y^q x)c = -(x^{q^2} y - y^{q^2} x)$$

and

$$(\gamma c + \gamma^q e c^q)(x^q y - y^q x) = b(x,y) = 0.$$

The points of $Sp(4,q)$ were taken to be the (q^3+q^2+q+1)-st roots of unity and again to find the lines we replace x^{q-1} by x. A totally isotropic line of the form $b(x,y)$ is

$$\{x \mid x^{q+1} + cx + e = 0\}$$

where $\gamma c = -\gamma^q e c^q$ as well as $e^{q^3+q^2+q+1} = 1$ and $c^{q+1} = e^q - e^{q^2+q+1}$.

Let $\eta = \gamma^{1-q}$. In the case when $c = 0$ there are q^2+1 lines where each totally isotropic line is given by

$$\{x \mid x^{q+1} + e = 0\}$$

where $e^{q^2+1} = 1$. In the case c is non-zero let $d = c^{-1}$ and so $e = -\eta d^{q-1}$ and

$$\eta d^{q^3+q} - \eta^{-1} d^{q^2+1} + 1 = 0.$$

For each d satisfying this equation there is a totally isotropic line which is given by

$$\{x \mid dx^{q+1} + x - \eta d^q = 0\}.$$

When q is even the alternating form is also symmetric and we can assume that $\gamma = 1$, and hence $\eta = 1$. The equations $c^{q+1} = e^q + e^{q^2+q+1}$ and $c = ec^q$ imply that $c^2 = e^{q+1}(e^{q^2+1} + 1)$ and by taking square roots that $c = e^{(q+1)/2} + e^{(q^2+q+2)/2}$. Thus we have that the totally isotropic lines of $W_3(q)$ when q is even are given by

$$\mathcal{L}_e := \{x \mid x^{q+1} + (e^{(q+1)/2} + e^{(q^2+q+2)/2})x + e = 0\} \subset \{x \mid x^{q^3+q^2+q+1} = 1\}$$

where $e^{q^3+q^2+q+1} = 1$. A short manipulation shows that

$$x^{q+1} + (e^{(q+1)/2} + e^{(q^2+q+2)/2})x + e = 0$$

if and only if

$$e^{q+1} + (x^{q^2+q} + x^{q-1})e + x^{2q} = 0.$$

Hence $x \in \mathcal{L}_e$ if and only if $e \in \mathcal{L}_{x^{2q}}$. Hence we see that $W_3(q)$ is self-dual when q is even.

Let π be the duality of $W_3(q)$ where π maps the point x to the line $\mathcal{L}_{x^\sigma}$ where σ is an automorphism of $GF(q^4)$. Since π is incidence-preserving π induces a map on the lines given by π^* which takes the line $\mathcal{L}_e$ to the point $e^{\sigma/2q}$. Now π is a polarity if $\pi^*\pi$ is the identity. That is if, for all $x \in GF(q^4)$, $(x^\sigma)^{\sigma/2q} = x$. Hence we have a polarity if q is not a square and we choose $\sigma = \sqrt{2q}$ or $\sigma = q^2\sqrt{2q}$.

4.3 Ovoids and spreads

In Section 3.5 we defined an ovoid and a spread of a polar space to be a 0-system and an $(r-1)$-system respectively. In general we define an *ovoid* O of a generalised quadrangle $\mathcal{G}$ to be a set of points with the property that every line is incident with exactly one point of O. A *spread* $\mathcal{S}$ of a generalised quadrangle is a set of lines with the property that every point is incident with exactly one line of $\mathcal{S}$. The dual of an ovoid is a spread in the generalised quadrangle dual to $\mathcal{G}$ and vice-versa. One can check that this definition coincides with the definition of an ovoid and a spread for the classical generalised quadrangles given in Section 3.5.

It is a simple matter to deduce the following proposition.

Proposition 4.4 *An ovoid of a GQ of order (s,t) has $st+1$ points and a spread of a GQ of order (s,t) has $st+1$ lines.*

In Section 2.3 we defined an ovoid of $PG(3,q)$. There is a connection between ovoids of $PG(3,q)$ and ovoids of GQ's and it comes from the following proposition.

Proposition 4.5 *If q is even, an ovoid O of $W_3(q)$ is an ovoid of $PG(3,q)$.*

Proof The totally isotropic lines incident with a point $x \in O$ lie in a plane and are all tangents to the ovoid. Therefore it is only necessary to prove that the hyperbolic lines (the lines of $PG(3,q)$ that are not totally isotropic) are incident with either 0 or 2 points of O. Let l be a hyperbolic line incident with a point x of O and let $\perp$ be the polarity defining $W_3(q)$. Then $l^\perp \subset x^\perp$ and so $l^\perp$ is incident with no points of O. There are $q^2(q^2+1)$ hyperbolic lines and so there is a set N of $q^2(q^2+1)/2$ hyperbolic lines that contains all the hyperbolic lines incident with a point of O. Let n_i be the number of lines of N that are incident with i points of O. Counting in two ways the pairs (x,l) where $x \in O$ and $l \in N$ we get

$$\sum in_i = (q^2+1)q^2.$$

Counting in two ways the unordered triples (x,y,l) where x and $y \in O$ and $l \in N$ we get

$$\sum i(i-1)n_i = (q^2+1)q^2.$$

Hence $\sum i(i-2)n_i = 0$ and every hyperbolic line is incident with 0 or 2 points of O. ■

Now we shall prove that a polarity of a GQ gives an ovoid. A *self-conjugate point* of a polarity π is a point x with the property that x is incident with $\pi(x)$. A *self-conjugate line* of a polarity π is a line l with the property that l is incident with $\pi^{-1}(l)$.

Proposition 4.6 *Let x be a non self-conjugate point and $e = \pi(x)$. The point x' of e adjacent to x is the point $\pi^{-1}(e')$ where e' is the line joining x and x'; in particular, x' and e' are self conjugate.* ■

Proof The line $\pi(x')$ meets $\pi(x)$ and is incident with x.

Proposition 4.7 *Every line is incident with a unique self-conjugate point and every point is incident with a unique self-conjugate line.*

Proof The two statements are dual so it is sufficient to prove the first. If $\pi^{-1}(e) \in e$, $\pi^{-1}(e)$ is self-conjugate and if there exists another self-conjugate point $y \in e$, the line $\pi(y)$ is incident with y and $\pi^{-1}(e)$ and therefore $\pi(y) = e$. Suppose on the contrary that $\pi^{-1}(e) \notin e$. The point $x \in e$ adjacent to $\pi^{-1}(e)$ is self-conjugate (c.f. Proposition 4.6). If $x \in e$ is self-conjugate, $\pi(x)$ is incident with x and $\pi^{-1}(e)$ and is adjacent to $\pi^{-1}(e)$. ■

This implies immediately that the set of self-conjugate points of a polarity is an ovoid and the set of self-conjugate lines is a spread. In the previous section we saw a polarity of $Sp(4,q)$ with q even and not a square. This was discovered by Tits who constructed the ovoid and showed that it's stabiliser group is the Suzuki group, see [11]. The self-conjugate points given by this polarity have the property that x is incident with the line $\mathcal{L}_{x^\sigma}$, where $\sigma = \sqrt{2q}$. That is

$$x^{q+1} + (x^{\sigma(q^2+q+2)/2} + x^{\sigma(q+1)/2})x + x^\sigma = 0.$$

The zeros of this equation are the *Tits ovoid* of $W_3(q)$. A small calculation shows that these zeros are elements of the set

$$\mathcal{T} := \{x \in GF(q^4) \mid x^{q^2+1} + x^{\sigma q - q + 1} + x^{q-\sigma+1} + 1 = 0\}.$$

The set of self-conjugate lines dual to the Tits ovoid is called the *Lüneburg spread*.

The only other known ovoid of $W_3(q)$ when q is even is that given by the isotropic points of the orthogonal elliptic form, the elliptic quadric. As we have seen such a quadratic form polarises to an alternating form when q is even. In Section 3.4 we calculated a non-degenerate orthogonal elliptic form over $GF(q^4)$ to be

$$f(x) = Tr_{q^4 \to q}(\gamma x^{q^2+1}) = x^{q^2+1} + x^{q^3+q}$$

where $\gamma^{q^2} + \gamma = 1$. Note that $b(x,y) = f(x+y) - f(x) - f(y) = Tr_{q^4 \to q}(y^{q^2}x)$. The zeros of f satisfy $x^{q^2+1} = x^{q^3+q}$ and again we replace x^{q-1} by x to find the zeros corresponding to projective points. The set

$$\mathcal{E} := \{x \in GF(q^4) \mid x^{q^2+1} + 1 = 0\}$$

is an ovoid of $Sp(4,q)$ and it is called the *elliptic quadric*.

Bibliography

[Che] C. Chevalley, *The Algebraic Theory of Spinors and Clifford Algebras* (Collected Works Vol. 2), Springer, Berlin, 1997.

[Hir] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford, 1998.

[HT] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geomtries*, Oxford, 1991

[HP] D. R. Hughes and F. C. Piper *Projective planes*, Springer, 1973.

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1983.

[Tay] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992.

---

[1] M. Brown, (Hyper)ovals and ovoids in projective spaces, available from
`http://cage.rug.ac.be/~fdc/intensivecourse2/brown_2.pdf`

[2] P. J. Cameron, *Projective and Polar Spaces*, available from
`http://www.maths.qmw.ac.uk/~pjc/pps/`

[3] P. J. Cameron, *Classical Groups*, available from
`http://www.maths.qmw.ac.uk/~pjc/class_gps/`

[4] W. Cherowitzo, Hyperoval page, available from

`http://www-math.cudenver.edu/~wcherowi/research/hyperoval/hypero.html/`

[5] F. De Clerck, J. A. Thas and H. van Maldeghem, *Generalized Polygons and Semipartial Geometries*, available from
`http://www.cage.rug.ac.be/~fdc/`

[6] N. Hamilton and C. T. Quinn, *m*-systems of polar spaces and maximal arcs in projective planes, *Bull. Belg. Math. Soc. Simon Stevin*, **7**, (2000), 237–248.

[7] M. Law and T. Penttila, *Flocks, ovals and generalised quadrangles (Four Lectures in Napoli, June 2000)*, available from
`thysanotus.maths.uwa.edu.au/research/reports/`

[8] T. Penttila and G. Royle, Sets of type (m,n) in the affine and projective planes of order 9, *Des. Codes Cryptogr.*, **6**, (1995), 229–245.

[9] B. Segre, Sulle ovali nei piani lineari finiti, *Atti Accad. Naz. Lincei Rendic.* **17** (1954), 141–142.

[10] J. A. Thas, Ovoids, spreads and *m*-systems of finite classical polar spaces: A survey, in: *Surveys in Combinatorics 2001*, British Combinatorial Conference, Sussex 2001, to appear.

[11] J. Tits, Ovoïdes et groupes de Suzuki, *Arch. Math.* **13** (1962), 187–198.