Flocks, generalised quadrangles and translation planes from BLT-sets

Maska Law

This thesis is presented for the degree of
Doctor of Philosophy
of The University of Western Australia
Department of Mathematics & Statistics.
March, 2003

Abstract

The study of flocks of the quadratic cone in three dimensional finite projective space is a fascinatingly rich field within finite geometry. The diversity of the geometric structures intimately connected with flocks lends great appeal, and these connections play a major role in this thesis. In particular, we study the case of flocks over fields of odd characteristic, where we have available the construction of Bader, Lunardon and Thas of a set of flocks from a given flock, and the concept of a BLT-set.

Following a survey of finite projective spaces and finite polar spaces, we study translation planes arising from linespreads of three dimensional projective space via the constructions of André and of Bruck and Bose, and we study elation generalised quadrangles via the group coset geometry construction of Kantor. The construction of Thas and Walker of an ovoid of the Klein quadric from a flock of the quadratic cone connected the extensive theory of translation planes with the study of flocks. The introduction by Payne of the concept of a q-clan for use in the construction of Kantor provided the opportunity for Thas to describe the connection between flocks and elation generalised quadrangles. We survey these many connections, introducing the known infinite families as examples of the various structures. We also apply the so called Fundamental Theorem of q-clan geometry to the calculation of the automorphism group of an example.

The concept of a BLT-set, introduced by Bader, Lunardon and Thas, but named by Kantor, provided a more general model in which to study flocks over fields of odd order, since one BLT-set gives rise to a number of flocks, which may or may not be pairwise equivalent. By applying results of Bader, O'Keefe and Penttila, we are able to exploit some recent upgrades to the computer algebra system MAGMA in order to search for new examples of BLT-sets. We discuss the general ideas behind these searches, and present a total of 31 new BLT-sets of varying order, yielding 170 new flocks. Analysis of one of the new examples led to the construction of an infinite family of BLT-sets over fields of characteristic three. These have been shown by Payne to be new, and give rise to the first known infinite family of flocks with trivial automorphism group. As well as each of the known infinite families of BLT-sets, we present a complete list of all known BLT-sets not currently belonging to an infinite family, and hence cover all BLT-sets known at this time.

Contents

Preface

The concept of a BLT-set arose in the field of finite geometry in 1990 with the introduction by Bader, Lunardon and Thas of the process of derivation of flocks of the quadratic cone of $\mathrm{PG}(3, q)$. The study of such flocks had constituted a very active area of research for many years before this, due in large part to the connections with other extensive fields of research, namely, the studies of certain translation planes and elation generalised quadrangles. These connections are a major motivation behind the continued interest in flocks of the quadratic cone, and so the focus on BLT-sets in this thesis requires the wider context of flocks and their associated geometries. An attempt is made to cover some important parts of this wide setting, but no claims to completeness are made in any respect. The contents of Chapters 1-4 and 6 make up this wider context, and full references are given for all ideas covered therein. Perhaps, however, some topics are presented in a fashion other than that which has become standard in the literature; for example, most of the known infinite families are presented in the setting in which they were originally described, and then compiled into a list after the wider context has been covered. The exceptions are presented in the models which the author considers most suitable for their presentation, but this is, of course, a matter of taste.

The contribution to current knowledge claimed by this thesis forms the content of Chapters 7-9, where results and outcomes of computer searches for BLT-sets are presented. The ideas underlying these searches, which are discussed in Chapter 7, are those of the author's supervisor Tim Penttila. The successful searches, undertaken by the author and their supervisor during the years of the author's candidature, yielded a wealth of new examples of BLT-sets, and these are presented in Chapter 8. Analysis of one of these examples led to the construction of a new infinite family of BLT-sets, which is presented in Chapter 9. Along with the new examples of BLT-sets, all previously known infinite families and all previously known examples which do not yet belong to an infinite family are presented in this thesis, and in so doing, all presently known BLT-sets are covered (to the author's best knowledge).

The initial content of Chapter 5 is in some sense well known material also, however the calculation given here has not appeared in the literature. An equivalent calculation in a different model has been given elsewhere, but the theme of this chapter is to demonstrate an understanding of the difficult topic it covers, and as for the presentation of the wider context earlier, to present in detail an important topic related to flocks and their associated geometries.

Acknowledgements

I'd like to say a personal thankyou to those people who have made my time as a research student a very enjoyable and rewarding experience.

Thankyou to my supervisor Tim Penttila, for introducing me to the beautiful world of finite geometry, and for teaching me so much, albeit so little of your vast knowledge. Thankyou for all the opportunities you have provided me, and just for being a great supervisor. It has been a real pleasure talking and learning and hanging out with you over the years.

Thankyou to Christine O'Keefe for support at local and international conferences, and for the Adelaide workshops. To Stan Payne and Bill Cherowitzo in Denver, to Guglielmo Lunardon and Laura Bader in Napoli, and to Jef Thas and Frank De Clerck in Gent, thankyou all for your warm hospitality during my visits to your universities. It is a great encouragement to know there are so many nice people in this area. Particular thanks to Stan Payne for the lectures you gave whilst I was in Denver and for your enthusiastic interest in my work, and to Guglielmo Lunardon, Laura Bader, Nicola Durante and Tim Penttila for showing me how much fun collaboration can be.

Thankyou to my good friend Michel Lavrauw, for your encouraging words on mathematics, and life in general, and for enjoying a good laugh. To Nicholas Hamilton, Matt Brown, Leanne Holder, Nico Durante and Rocco Trombetti for some fun times in the name of mathematics and otherwise.

Thankyou to everyone in the Maths and Stats Department for being part of a productive, and sociable, working environment.

Thankyou to my wonderful family, Karla, Malcolm and Saskia, for always being there. Thankyou for our great times together, and for encouraging my education over the years. Thankyou Judit for always believing in me, and for your immense support during the difficult times. To all my fabulous friends, cheers for being the great people you are.

And finally, thanks to Barrett's Bread for making the best coffee around !

Preliminaries and background

In this thesis we will be studying finite geometries. Some good sources of reference for preliminaries and background include Artin (1957), Baer (1952), Beukenhout (Ed.) (1995), Cameron (year unknown), Dembowski (1968), Hirschfeld (1979, 1985, 1998), Hirschfeld and Thas (1991) and Taylor (1992).

1.1 Finite projective spaces and finite polar spaces

We will be concerned with finite dimensional projective geometries over finite fields. For a positive integer n and a prime power q, the subspaces of the n-dimensional **projective space** $\mathrm{PG}(n,q)$ are the subspaces of a vector space V of rank $\mathrm{rk} = n+1$ over the Galois field $GF(q)$ of order q. We view $\mathrm{PG}(n,q)$ as an incidence structure with symmetric inclusion as the incidence relation. So that we retain familiar geometric properties, the dimension of an element of a projective space is defined to be one less than its rank as a vector subspace. Thus the points of a projective space are the vector subspaces of rank 1, hence of dimension 0. Subspaces of codimension 1 are called **hyperplanes**.

Building on work of von Staudt and of Hilbert, Veblen and Young (1916) gave axioms for a projective geometry solely in terms of the points and lines of the space : for a set of points and a set of distinguished subsets of the set of points called lines, suppose

(i) any two points lie on a unique line;

(ii) any line contains at least three points;

(iii) any line which meets two sides of a triangle, not at a vertex, meets the third side also.

A **subspace** is a subset S of points such that for any two points P, Q in S, all points on the unique line PQ are also in S. The **projective geometry** is then the incidence structure of all nonempty subspaces satisfying these axioms, with incidence inclusion. A projective geometry has dimension d if there exists a chain of proper nonempty subspaces of length d, but not of length $d+1$.

In fact, any finite projective geometry of dimension at least 3 is isomorphic to $\mathrm{PG}(n,q)$ for some n and q. But for dimension 2, there exist numerous projective planes not isomorphic to $\mathrm{PG}(2,q)$, satisfying the first two axioms and the simpler condition that any two lines meet. The planes $\mathrm{PG}(2,q)$ are called **Desarguesian** as they are the only finite projective planes which satisfy the theorem of Desargues. For $n \geq 3$, $\mathrm{PG}(n,q)$ is always Desarguesian.

It follows from the axioms that any two lines of a projective geometry have the same number of points. Since, consider two lines l, l' which meet in some point P. Take a third line m meeting both l and l' in points other than P. By axiom (ii), there is a third point Q on m. Any line through Q which meets l in a point R will also meet l' in some point R', by axiom (iii). In this way, the points of l other than P are uniquely paired with the points of l' other than P. If on the other hand the lines l and l' do not meet in a point, take a point P on l and a point P' on l'. Then the unique line PP' has the same number of points as l by the above argument, but also has the same number of points as l', and so the result follows. If the number of points on a line of the projective geometry $\mathcal{PG}$ is $s+1$, we call s the **order** of $\mathcal{PG}$. The order of $\mathrm{PG}(n,q)$ is q.

As with many mathematical objects, we are interested in automorphisms of projective geometries, that is, structure-preserving bijections of the space. A **collineation** of a projective geometry is a permutation of the points which maps lines onto lines, and thus maps subspaces onto subspaces. So a collineation is an inclusion-*preserving* bijection of the space. The set of all collineations of a projective geometry $\mathcal{PG}$ forms a group under composition called the **collineation group** (or **automorphism group**) and is denoted by $\mathrm{Aut}\mathcal{PG}$.

A theme that will become very important in the following sections is that of transferring information between a projective space and the underlying vector space (in the Desarguesian case), and we begin this theme in the context of collineations.

For a vector space V over $GF(q)$, a transformation $T : V \to V$ is called **α-semilinear** if there exists a field automorphism α of $GF(q)$ such that

$$T(v+w) = T(v) + T(w) \quad \text{and} \quad T(cv) = \alpha(c)T(v)$$

for all $v, w \in V$ and $c \in GF(q)$. We call α the **companion automorphism** of T. Clearly, any semilinear transformation of V will map subspaces onto subspaces, and thus any invertible semilinear transformation will give rise to (or induce) a collineation of the associated projective space $\mathrm{PG}(n,q)$. The set of all invertible semilinear transformations forms a group under composition and is denoted by $\mathit{\Gamma L}(n+1,q)$.

Now the elements of $\mathit{\Gamma}L(n+1,q)$ which induce collineations fixing every point of $\mathrm{PG}(n,q)$ form the subgroup

$$Z = \{v \mapsto cv \mid c \in GF(q), c \neq 0\},$$

that is, the pointwise stabiliser of $\mathrm{PG}(n,q)$ is the set of collineations induced by the scalar maps. Thus the group of collineations of $\mathrm{PG}(n,q)$ induced by the invertible semilinear transformations is $P\mathit{\Gamma}L(n+1,q) = \mathit{\Gamma}L(n+1,q)/Z$, called the **projective semilinear group**.

Conversely, if the rank of V is at least 3, then it can be shown that every collineation of $\mathrm{PG}(n,q)$ has this form, that is, every collineation is induced by an invertible semilinear transformation of V. Thus we have the following result.

Theorem 1.1 (The Fundamental Theorem of Projective Geometry). *If the rank $n+1$ of V is at least 3, then $AutPG(n,q) = P\mathit{\Gamma}L(n+1,q)$.*

Proof : See Baer (1952), p44.

A very interesting feature of a projective geometry $\mathcal{PG}$ is that it satisfies a duality concept. A proposition concerning $\mathcal{PG}$ is often stated only in terms of subspaces and inclusion relations between them, for example, meet, join or dimension. The dual proposition is then obtained by inverting all inclusions, and hence replacing meet, join and dimension r with join, meet and dimension $n-1-r$, respectively (if $\mathcal{PG}$ has dimension n). This concept is referred to as the **Principle of Duality** : for a proposition which is true in all n-dimensional projective geometries, the dual proposition is also true in all n-dimensional projective geometries.

Motivated by the Principle of Duality, we introduce the concept of a **duality** (or **correlation**) of a projective geometry, that is, an inclusion-*reversing* bijection of the space. So a duality δ of a projective geometry $\mathcal{PG}$ is a permutation of the subspaces such that $S \subseteq T \Rightarrow S^\delta \supseteq T^\delta$, for all subspaces S and T of $\mathcal{PG}$. The product of two dualities is then a collineation, and the set of all dualities and collineations forms a group under composition, called the **correlation group** and denoted by $\mathrm{Cor}\mathcal{PG}$.

The most important type of duality is one of order 2, called a **polarity** of the projective geometry. The reason for their importance is that they give rise to particular geometries called polar spaces, which are similar in nature to projective geometries, yet rich in different types of structure.

Let ρ be a polarity of a Desarguesian projective space $\mathrm{PG}(n,q)$. A subspace S is **totally isotropic** with respect to ρ if $S \subseteq S^\rho$. The **polar space** $\Pi(\rho)$ arising from

ρ is the geometry whose subspaces are the totally isotropic subspaces of $\mathrm{PG}(n,q)$ with respect to ρ, with incidence inherited from $\mathrm{PG}(n,q)$. We call S^ρ the **polar subspace** of the subspace S with respect to ρ.

We return to our theme motivated by the Fundamental Theorem of Projective Geometry, and ask what information we can obtain by studying the transformations on the underlying vector space which give rise to polarities.

A **sesquilinear form** on a vector space V is a function $f : V \times V \to GF(q)$ which is linear in the first variable and semilinear in the second variable, that is, for which there exists a field automorphism α such that

$$f(v+v',w) = f(v,w) + f(v',w) \qquad f(cv,w) = cf(v,w)$$

$$f(v,w+w') = f(v,w) + f(v,w') \qquad f(v,cw) = \alpha(c)f(v,w),$$

for all $v, v', w, w' \in V$ and $c \in GF(q)$. We call α the **companion automorphism** of f, and say f is an α-sesquilinear form. If α is the identity, then the form is called **bilinear**.

The **radical** of a sesquilinear form f is

$$\mathrm{Rad}(f) = \{w \in V \mid f(v,w) = 0 \text{ for all } v \in V\}.$$

A sesquilinear form is **nondegenerate** if its radical is $\{0\}$.

Consider the vector space $V = GF(q)^n$. If A is an $n \times n$ matrix with entries from $GF(q)$ and $\alpha \in \mathrm{Aut}GF(q)$, then $f(v,w) = v^T A\alpha(w)$ is an α-sesquilinear form on V. Conversely, if f is an α-sesquilinear form on $V = GF(q)^n$, $X = \{x_1, \ldots, x_n\}$ is a basis for V, and $A = A(X,f)$ is the $n \times n$ matrix $A = (a_{ij})$ with $a_{ij} = f(x_i, x_j)$, then the isomorphism $GF(q)^n \to V$ taking $(a_1, \ldots, a_n)$ to $a_1x_1 + \cdots + a_nx_n$ identifies $(v,w) \mapsto v^T A\alpha(w)$ with f. The matrix $A = A(X,f)$ is called **the matrix of** f **with respect to the basis** X. Note that A (and α) uniquely determine the form f.

Lemma 1.1. *A sesquilinear form f on a vector space V is nondegenerate if and only if the matrix of f with respect to a basis of V is nonsingular.*

Proof : If A is the matrix of f with respect to some basis of V and α is the companion automorphism of f, then the radical of f corresponds to the kernel of the map $x \mapsto A\alpha(x)$. Since this map is a bijection, the kernel is $\{0\}$ if and only if A is nonsingular.

We say two vectors v, w are **orthogonal** (with respect to f) if $f(v,w) = 0$. For a subset X of V, we define the **orthogonal complement** of X (with respect to f) to be

$$X^\perp = \{v \in V \mid f(x,v) = 0 \text{ for all } x \in X\},$$

where the symbol $\perp$ is read as 'perp'. So a subspace U of V is **nondegenerate** if the restriction of f to U is nondegenerate, or equivalently, if $U \cap U^\perp = \{0\}$.

For a nondegenerate sesquilinear form f on a vector space V, and U a subspace of V, other familiar properties also hold :
(i) rk U + rk $U^\perp$ = rk V;
(ii) U is nondegenerate if and only if $V = U \oplus U^\perp$;
(iii) $(U^\perp)^\perp = U$.

Thus the map $\mathrm{PG}(n,q) \to \mathrm{PG}(n,q)$ with $U \mapsto U^\perp$, for all subspaces U of V, is a duality of the projective space $\mathrm{PG}(n,q)$. We call such a duality **the duality arising from** f. It is determined up to a nonzero scalar multiple of f.

Theorem 1.2 (Birkhoff and von Neumann (1936)). *Every duality of $PG(n,q)$, $n \geq 2$, arises from a nondegenerate sesquilinear form on the underlying vector space, up to a nonzero scalar multiple.*

Proof : See Baer (1952), p102.

The previous theorem was first proved by Birkhoff and von Neumann in 1936 whilst attempting to provide a logical structure for such physical theories as quantum mechanics. As a consequence of the theorem we see that the study of dualities of a projective space is equivalent, up to a nonzero scalar multiple, to the study of nondegenerate sesquilinear forms on the underlying vector space.

A sesquilinear form f on V is **reflexive** if the orthogonality relation is symmetric, that is, if for all $v, w \in V$,

$$f(v,w) = 0 \Rightarrow f(w,v) = 0.$$

Lemma 1.2. *The duality arising from a nondegenerate sesquilinear form f is a polarity if and only if f is reflexive.*

Proof : Let δ be the duality arising from f, so that

$$\delta(\langle v \rangle) = v^\perp = \{w \mid f(v,w) = 0\}.$$

Then

$$
\begin{aligned}
\delta \text{ is a polarity} &\iff \delta^2 = 1 \\
&\iff (\langle v\rangle \subseteq \delta(\langle w\rangle) \equiv \langle w\rangle \subseteq \delta(\langle v\rangle)) \quad \forall v, w \in V \\
&\iff (f(w,v) = 0 \equiv f(v,w) = 0) \quad \forall v, w \in V \\
&\iff f \text{ is reflexive.}
\end{aligned}
$$

So in order to study polarities of a projective space, we need only concern ourselves with nondegenerate reflexive sesquilinear forms defined on the underlying vector space.

Before continuing our study of sesquilinear forms, we consider the question of isomorphism of vector spaces carrying such forms.

So let V_1, V_2 be vector spaces of the same dimension carrying the sesquilinear forms f_1, f_2, respectively. Let $T : V_1 \to V_2$ be an invertible semilinear transformation with companion automorphism α. Then T is called a **semisimilarity** if there exists $c \in GF(q) \setminus \{0\}$ with

$$f_2(T(v), T(w)) = c\alpha(f_1(v,w))$$

for all $v, w \in V_1$. If α is the identity, then T is linear and is called a **similarity**. A similarity for which the **constant of similitude** c is the multiplicative identity of $GF(q)$ is called an **isometry**. We say two spaces are **isometric** (**similar**) if there exists an isometry (similarity) between them. Note that an isometry preserves the sesquilinear forms on the spaces, whereas a similarity preserves only orthogonality of vectors.

Lemma 1.3. *A sesquilinear form g on V is similar to f if and only if there exists a basis $Y = \{y_1, \ldots, y_n\}$ of V with $A(Y,g) = cA(X,f)$ for some $c \in GF(q) \setminus \{0\}$. The forms are isometric precisely when c can be chosen to be 1.*

Proof : See Aschbacher (1986), p78.

The set of all semisimilarities from a vector space V with form X to itself forms a group under composition, called the **semisimilarity group** $\varGamma X(V)$ of V. It is clear from the definitions that the map from a semisimilarity to its companion automorphism is a homomorphism onto $\mathrm{Aut}GF(q)$ with kernel the **similarity group** $GX(V)$. Likewise, the map from a similarity to its constant of similitude c is a homomorphism onto $GF(q) \setminus \{0\}$ with kernel the **isometry group** $IX(V)$ (or simply $X(V)$).

An α-sesquilinear form f on a vector space V is called α-**hermitian** if $f(v,w) = \alpha(f(w,v))$ for all $v, w \in V$. α has order at most 2. If α is the identity, then f (which is bilinear) is called **symmetric**. A bilinear form f on V is called **alternating** if $f(v,v) = 0$ for all $v \in V$.

Theorem 1.3 (Classification of nondegenerate reflexive sesquilinear forms). *A nondegenerate reflexive sesquilinear form is either alternating, symmetric or similar to an α-hermitian form with $\alpha \neq 1$.*

Proof : See Baer (1952), or Cameron (year unknown).

Traditionally, a vector space carrying an alternating form is called **symplectic**, and the polarity arising from this space is a **symplectic** (or **null**) polarity. However, a short calculation (expand $f(v+w, v+w) = 0$) shows that an alternating bilinear form over a field of characteristic 2 is also symmetric, whereas a symmetric bilinear form need not be alternating. In order to distinguish these cases, over a field of characteristic 2, we call a polarity **symplectic** (or **null**) if it arises from an alternating symmetric bilinear form (as before), and **pseudo-symplectic** if it arises from a non-alternating symmetric bilinear form. For characteristic not 2, a vector space carrying a symmetric bilinear form is called **orthogonal** and gives rise to an **orthogonal** polarity. A vector space over an arbitrary field carrying a hermitian sesquilinear form is called **unitary** and gives rise to a **unitary** polarity. These names correspond to the names of the classical isometry groups associated with such spaces.

As we now know that every polarity arises from a nondegenerate reflexive sesquilinear form, we would like to construct the polar space arising from a polarity directly from the underlying vector space and form.

For a vector space V with nondegenerate sesquilinear form f we say a nonzero vector $v \in V$ is **isotropic** if $f(v,v) = 0$. A subspace U is **totally isotropic** if the restriction of f to U is trivial, that is, if any two vectors are orthogonal ($f(v,w) = 0$ for all $v, w \in U$). This is equivalent to saying that $U \subseteq U^{\perp}$, and so we see that this definition of totally isotropic is consistent with the earlier usage. A subspace is **anisotropic** if it contains no nonzero isotropic vectors. A subspace of the projective space arising from V is called **totally isotropic** if it is totally isotropic as a subspace of V.

The **polar space** arising from a vector space with nondegenerate reflexive sesquilinear form is the geometry whose subspaces are the totally isotropic subspaces of the associated projective space, with incidence inherited from the projective space.

Now this is not the only way in which these sorts of geometries arise. A geometry with properties akin to the above polar spaces can be constructed from a nondegenerate quadric of projective space, and as we shall see, is indeed one of these geometries in odd characteristic, but gives rise to new examples in characteristic 2.

A **quadratic form** on a vector space V is a function $Q : V \to GF(q)$ which satisfies

$$Q(cv) = c^2 Q(v)$$

for all $v \in V$ and all $c \in GF(q)$, and has associated with it a symmetric bilinear form, f_Q, where

$$f_Q(v, w) = Q(v + w) - Q(v) - Q(w)$$

for all $v, w \in V$. We say that f_Q is the **polar form** of Q or that Q **polarises** to f_Q.

The **singular radical** of a quadratic form Q is

$$\mathrm{SingRad}(Q) = \{v \in \mathrm{Rad}(f_Q) \mid Q(v) = 0\}.$$

A quadratic form is **nondegenerate** if its singular radical is $\{0\}$.

We note that the question of isomorphism of vector spaces with quadratic forms is analogous with that of spaces carrying sesquilinear forms, and results carry over naturally from the earlier discussion.

A **quadric** $\mathcal{Q}$ of $\mathrm{PG}(n, q)$ arising from the quadratic form Q is the set of points $\langle v \rangle$ such that $Q(v) = 0$. We say a quadric is **nondegenerate** if the defining quadratic form is nondegenerate.

The **polar space** $\Pi(\mathcal{Q})$ arising from a nondegenerate quadric $\mathcal{Q}$ is the geometry whose subspaces are the subspaces of $\mathrm{PG}(n, q)$ contained in $\mathcal{Q}$, with incidence inherited from $\mathrm{PG}(n, q)$.

Again, we can construct the polar space arising from a quadric directly from the underlying vector space and quadratic form.

For a vector space V with nondegenerate quadratic form Q, we say a nonzero vector $v \in V$ is **singular** if $Q(v) = 0$. A subspace U is **totally singular** if the restriction of Q to U is trivial, that is, if $Q(v) = 0$ for all $v \in U$. If a subspace is totally singular, then it is clear that the subspace is also totally isotropic with respect to the polar form of the quadratic form, since the quadratic form uniquely determines its polar form. A subspace is **anisotropic** if it contains no nonzero singular vectors.

A subspace of the projective space arising from V is called **totally singular** if it is totally singular as a subspace of V.

The **polar space** $\Pi(Q)$ arising from a nondegenerate quadratic form Q on a vector space is the geometry whose subspaces are the totally singular subspaces of the associated projective space.

It was mentioned above that, under certain circumstances, this type of polar space actually coincides with the case of a polar space arising from a polarity. For the polar form f_Q of a quadratic form Q, we have that $f_Q(v, v) = 2Q(v)$ for $v \in V$. So if the characteristic of $GF(q)$ is not 2, the quadratic form Q is uniquely determined by f_Q, and so the study of quadratic forms is equivalent to the study of symmetric bilinear forms. However, if the characteristic of $GF(q)$ is 2, the polar form of a quadratic form is alternating, and so for quadrics in characteristic 2 we get the polar spaces arising from symplectic polarities, but not those arising from pseudo-symplectic polarities. Furthermore, we cannot recover the quadratic form from the polar form. Indeed, there are many quadratic forms which could give rise to a given alternating symmetric bilinear form as its polar form.

For this reason, we intend to no longer consider vector spaces carrying symmetric bilinear forms, except when they arise as the polar form of a quadratic form. Thus for characteristic 2 we intend to exclude the possibility of a pseudo-symplectic polarity. However, it turns out that the polar space arising from a pseudo-symplectic polarity is isomorphic to the polar space arising from a symplectic polarity in dimension one less. Hence in general we will only consider the following cases :

(i) a nondegenerate alternating bilinear form (giving rise to a symplectic polarity)

(ii) a nondegenerate α-hermitian sesquilinear form with $\alpha \neq 1$ (giving rise to a unitary polarity)

(iii) a nondegenerate quadratic form with symmetric bilinear polar form (giving rise to an orthogonal polarity for characteristic not 2, and a symplectic polarity for characteristic 2).

For uniformity, a vector space carrying a form of one of these types will be called a **space with form**, of type **symplectic, unitary** or **orthogonal**, respectively, and the families of polar spaces arising in these situations are called the **classical polar spaces**.

Now we investigate more closely the structure of the finite classical polar spaces, by studying the underlying spaces with form.

The following is a powerful result from the theory of categories, first proved by Witt in 1937 for symmetric and hermitian forms over fields of characteristic not 2.

Theorem 1.4 (Witt (1937)). *Suppose V is a space with form, U is a subspace of V and the map $T : U \to V$ is an isometry. Then T extends to an isometry of V.*

Proof : See Aschbacher (1986), p81.

As a consequence of Witt's theorem, we can define an invariant of spaces with form. Consider two maximal totally isotropic subspaces M and N of a vector space V. Without loss of generality, suppose that rk $M \leq$ rk N. Then there is an isomorphism S of M into N, and this isomorphism is in fact an isometry since M and N are totally isotropic. So by Witt's theorem, there is an extension of S to an isometry T of V onto V. Then $M \subseteq T^{-1}(N)$; but $T^{-1}(N)$ is totally isotropic. Thus $M = T^{-1}(N)$, and so rk $M =$ rk N. Hence all maximal totally isotropic subspaces have the same rank. This constant rank is called the **Witt index** of the space, and since a totally isotropic subspace is one which is contained in its perp, the Witt index can be at most half the rank of the underlying vector space. A similar argument holds for maximal totally singular subspaces, and so in this case, the Witt index will be equal to one more than the dimension of a maximal subspace contained in the quadric.

With this invariant of a space with form we are able to completely describe the structure of these spaces, and hence describe all classical polar spaces of this type. Firstly, we require some more geometric concepts.

A pair of vectors (u, v) in V such that u and v are isotropic, and $Q(u) = Q(v) = 0$ in the orthogonal case, is called a **hyperbolic pair** if $f(u, v) = 1$. The line $\langle u, v\rangle$ in $\mathrm{PG}(n, q)$ is then called a **hyperbolic line**.

If $V = U \oplus W$ and $f(u, w) = 0$ for all $u \in U$ and $w \in W$, we write $V = U \perp W$ and say that V is the **orthogonal direct sum** of U and W.

Lemma 1.4. *Suppose that l is a nondegenerate subspace of V of rank 2 which contains an isotropic vector u with respect to the sesquilinear form f. Then $l = \langle u, v\rangle$, where (u, v) is a hyperbolic pair.*

Proof : See Taylor (1992), p56.

Lemma 1.5. *(i) Any two symplectic hyperbolic lines over the same field are isometric.*
(ii) Any two unitary hyperbolic lines over the same field are isometric.
(iii) Any two orthogonal hyperbolic lines over the same field are isometric.

Proof : The matrix of an alternating or hermitian form f with respect to the basis $\{u, v\}$ of the hyperbolic line $l = \langle u, v\rangle$ is

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

For a quadratic form Q, we have $Q(au + bv) = 0$. Since these remarks hold for any form and any hyperbolic line, the result follows from Lemma 1.3 and the analogous result for spaces with quadratic forms.

Lemma 1.6. *For vector spaces U_1, U_2, W_1, W_2, if U_1 is isometric to U_2 and W_1 is isometric to W_2, then the orthogonal direct sum $U_1 \perp W_1$ is isometric to the orthogonal direct sum $U_2 \perp W_2$.*

Proof : This follows immediately from the definition of orthogonal direct sum.

The following result describes completely the structure of a vector space with form in terms of the previous concepts.

Theorem 1.5. *Let V be a space with form. Then V is an orthogonal direct sum of r hyperbolic lines and an anisotropic space U, where r is the Witt index of V. U is determined up to isometry.*

Proof : (Existence) We show existence of an orthogonal direct sum of the required form by induction on the Witt index r. If $r = 0$, then V has no maximal totally isotropic subspaces other than $\{0\}$, so V is anisotropic by definition. So suppose that $r > 0$. Then since there is a maximal totally isotropic subspace of rank $r > 0$, totally isotropic points must exist. Consider such a point P. Then $P^\perp$ is a hyperplane, and so there exists a line l on P with $l \not\subseteq P^\perp$. Let $R = l \cap l^\perp$ and take $x \in R$. Then since $x \in l^\perp$, $l \subseteq x^\perp$, and so $P \subseteq x^\perp$. Thus $x \in P^\perp$. Now $l \not\subseteq P^\perp$, so $l \cap P^\perp = P$. So we have $x \in P$. But if $x \neq 0$, then $x^\perp = P^\perp$; and $l \subseteq x^\perp$, so $l \subseteq P^\perp$. This contradicts the original assumption, so $x = 0$. Thus $R = \{0\}$, that is, l is nondegenerate. So nondegenerate lines on totally isotropic points exist. By Lemma 1.4, all such lines are hyperbolic, and so hyperbolic lines exist. Now consider $l^\perp$ for a hyperbolic line

l on a totally isotropic point P. Since $l^\perp \cap (l^\perp)^\perp = l^\perp \cap l = \{0\}$, we see that $l^\perp$ is nondegenerate.

Our next step is to show that the Witt index of $l^\perp$ is $r-1$: Firstly, since $P \nsubseteq l^\perp$, the span of P and any totally isotropic subspace of $l^\perp$ will give a totally isotropic subspace of V with rank at most r. So the Witt index of $l^\perp$ is not greater than $r-1$. Secondly, let M be a maximal totally isotropic subspace of V on P. Take $w \in l$ such that $w \notin P$. Then $M \cap l^\perp \subseteq M \cap w^\perp$. Now suppose $P = \langle v \rangle$ and so $l = \langle v, w \rangle$. Consider $u \in M \cap w^\perp$. Then since M is totally isotropic, $M \subseteq M^\perp$; and since $P \subseteq M$, we have that $M \subseteq P^\perp$. So $f(u,v) = 0$ for the defining form f. Also, since $u \in w^\perp$, $f(u,w) = 0$. So we have that $f(u, \lambda v + \mu w) = 0$, and so $u \in l^\perp$. Thus $M \cap w^\perp \subseteq M \cap l^\perp$. Hence $M \cap l^\perp = M \cap w^\perp$. Now $w^\perp$ is a hyperplane, and if $M \subseteq w^\perp$ then $f(v,w) = 0$; but $f(v,w) \neq 0$ since $l = \langle v, w \rangle$ is a hyperbolic line, and so $M \nsubseteq w^\perp$. Hence the rank of M is one more than the rank of $M \cap w^\perp$, that is, $rkM = r = 1 + rk(M \cap w^\perp)$. Thus $rk(M \cap l^\perp) = r-1$. So a maximal totally isotropic subspace of $l^\perp$ must have rank not less than $r-1$. Thus the Witt index of $l^\perp$ is $r-1$.

Now since l is nondegenerate, $V = l \oplus l^\perp$. Our inductive hypothesis says that the result holds for a nondegenerate space of Witt index $r-1$; in particular, for $l^\perp$. That is, $l^\perp$ is an orthogonal direct sum of $r-1$ hyperbolic lines and an anisotropic subspace. Hence $V = l \oplus l^\perp$ will be an orthogonal direct sum of r hyperbolic lines (since l is hyperbolic) and an anisotropic subspace.

(Uniqueness) By Lemmas 1.5 and 1.6 any two orthogonal direct sums of r hyperbolic lines of V are isometric. By Witt's theorem, there is an isometry T of V taking the first U_1 of these sums to the second U_2. So T will take $(U_1)^\perp$ to $(U_2)^\perp$. Since each of these sums is nondegenerate, we have that $V = U_1 \perp (U_1)^\perp$ and $V = U_2 \perp (U_2)^\perp$. So $(U_1)^\perp$ and $(U_2)^\perp$ are in fact the anisotropic spaces related to each of the sums. Thus any two anisotropic spaces are isometric.

Note that the hyperbolic lines play a similar role here to an orthonormal basis in a real inner product space. If a space is just an orthogonal direct sum of hyperbolic lines, that is, the anisotropic part is just the zero subspace, then we call it a **hyperbolic** space. Our final step to describing completely the structure of our spaces with form is to determine all possible anisotropic parts of a given space.

Lemma 1.7. *An anisotropic symplectic space has rank 0.*

Proof : All nonzero vectors are isotropic under an alternating form.

Corollary 1.1. *A symplectic space is isometric to an orthogonal direct sum of r hyperbolic lines, and thus has even rank $2r$, where r is the Witt index. This space is denoted by $Sp(2r, q)$.*

Lemma 1.8. *An anisotropic unitary space has rank at most 1, and all anisotropic unitary spaces of rank 1 are isometric.*

Proof : See Taylor (1992), p116, or Cameron (year unknown), pp76-77.

Corollary 1.2. *A unitary space of even rank $2r$ over the field $GF(q^2)$ is isometric to an orthogonal direct sum of r hyperbolic lines, where r is the Witt index, and is denoted by $U(2r, q^2)$. A unitary space of odd rank $2r+1$ over the field $GF(q^2)$ is isometric to an orthogonal direct sum of r hyperbolic lines and an anisotropic subspace of rank 1, where r is the Witt index, and is denoted by $U(2r+1, q^2)$.*

Lemma 1.9. *(i) An anisotropic orthogonal space over $GF(q)$ has rank at most 2.*
(ii) All anisotropic orthogonal spaces of rank 2 over $GF(q)$ are isometric.
(iii) If q is even, all anisotropic orthogonal spaces over GF(q) of rank 1 are isometric.
(iv) If q is odd, all anisotropic orthogonal spaces over GF(q) of rank 1 are similar, but there are two isometry classes.

Proof : See Taylor (1992), pp138-139, or Cameron (year unknown), p76.

Corollary 1.3. *An orthogonal space of even rank $2r$ over $GF(q)$ is either isometric to an orthogonal direct sum of r hyperbolic lines, where r is the Witt index, and denoted by $O^+(2r, q)$ and called hyperbolic, or is isometric to an orthogonal direct sum of $r-1$ hyperbolic lines and an anisotropic space of rank 2, where $r-1$ is the Witt index, and denoted by $O^-(2r, q)$ and called elliptic. An orthogonal space of odd rank $2r+1$ over $GF(q)$ is isometric to an orthogonal direct sum of r hyperbolic lines and an anisotropic space of rank 1, where r is the Witt index. If q is even, this determines the space up to isometry, while if q is odd, this determines the space up to similarity, but there are two isometry classes of such spaces. In any case we denote the space by $O(2r+1, q)$ and call it parabolic.*

The two isometry classes in the odd rank orthogonal case for characteristic not 2 clearly give rise to the same polar space, however, care must be taken when such a polar space is embedded in a polar space of higher polar rank. In this case, a choice is made when considering the smaller polar space, as highlighted in the paper of Bader, Durante, Lunardon, Penttila and the present author ([8]). We will study this further in the next section, where discriminants are used to distinguish isometry classes of orthogonal spaces, and will also see this in the context of BLT-sets later.

The problem of axiomatising polar spaces was solved by Tits (1974) (building on work of Veldkamp (1959)).

An **abstract polar space** of **polar rank** r is a set of points together with a set of distinguished subsets called **subspaces** such that :

(i) any subspace, together with the subspaces it contains, is a projective space of dimension at most $r-1$;

(ii) the intersection of any two subspaces is a subspace;

(iii) given a subspace H of dimension $r-1$ and a point P not in H, there exists a unique subspace M containing P such that $M \cap H$ has dimension $r-2$ and M contains all points of H collinear with P;

(iv) there exist two disjoint subspaces of dimension $r-1$.

Axiom (iii) will be refered to as **Tits' polar space axiom** in later sections.

These axioms were somewhat simplified by Buekenhout and Shult (1974), in the spirit of the Veblen-Young axioms for a projective geometry. They provided a set of axioms for an abstract polar space solely in terms of the points and lines of the space, from which all subspaces could be reconstructed. So for a set of **points** $\mathcal{P}$ together with a non-empty set of subsets called **lines** :

BS(i) every line has at least three points;

BS(ii) no point is collinear with all other points;

BS(iii) if a point P is not on a line l, then either P is collinear with exactly one point of l or P is collinear with all points of l.

A subset S of points is called a **subspace** if every pair of distinct points of S is collinear, and if whenever a line l contains two distinct points of S, all points of l are in S. Then if such a set of points $\mathcal{P}$ does not contain an infinite chain of distinct subspaces, Buekenhout and Shult showed that $\mathcal{P}$ together with its sets of subspaces satisfies the set of axioms given by Tits above. The polar rank is then one more than the size of a maximal subspace. Axiom BS(iii) will be refered to as the **all-or-one axiom** in later sections.

All projective spaces of dimension ≥ 3 are Desarguesian, whereas there exist projective planes which are non-Desarguesian. Similarly, a complete classification theorem of polar spaces of polar rank ≥ 3 was given by Tits (1974). For the case of finite polar spaces, this classification amounts to the following :

Theorem 1.6 (Tits (1974)). *A finite polar space of polar rank ≥ 3 is a classical polar space.*

Thus we have seen how to construct all finite polar spaces of polar rank ≥ 3. The polar spaces of rank 2, containing only points and lines, are called **generalised quadrangles**, and we will come to these later. Just as with projective planes, not all generalised quadrangles arise from polarities or from quadrics as the higher rank polar spaces do. (Rank 1 polar spaces are considered trivial structures.)

The six families of finite classical polar spaces can be summarised as in the following table. We use the more familiar geometric notation for these polar spaces in this thesis, so the dimensions in the table are projective dimensions, r is the polar rank, and e, depending only on the anisotropic space, carries information about all spaces in the family. (Note that for the unitary case, the finite field must have order a square, to ensure the existence of a nonidentity companion automorphism.)

Type	Notation	e
symplectic	$W(2r-1,q)$	0
unitary	$H(2r-1,q^2)$	$-\frac{1}{2}$
unitary	$H(2r,q^2)$	$\frac{1}{2}$
orthogonal	$Q^+(2r-1,q)$	-1
orthogonal	$Q(2r,q)$	0
orthogonal	$Q^-(2r+1,q)$	1

We list here some combinatorial results for finite polar spaces, proofs of which can be found, for example, in Cameron (year unknown) or Buekenhout (1995). The notation follows that of the above table.

Theorem 1.7. *The number of points in a finite polar space of rank 1 is $q^{1+e}+1$.*

Theorem 1.8. *In a finite polar space of rank r, there are $(q^r-1)(q^{r+e}+1)/(q-1)$ points, of which q^{2r-1+e} are not orthogonal to a given point.*

Theorem 1.9. *The number of maximal subspaces in a finite polar space of rank r is*

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

In particular, if $r = 2$ (so the polar space is a generalised quadrangle), each line has $q+1$ points, and each point lies on $q^{1+e}+1$ lines. In terms of the parameters we shall use later for generalised quadrangles, $s = q$ and $t = q^{1+e}$.

The full collineation groups of the classical polar spaces are, in general, induced by the semisimilarity groups of the underlying spaces with form in the same manner as for projective spaces, that is, by factoring out the scalar maps. These groups are denoted as follows :

(i) symplectic : $P\Gamma Sp(2r, q)$

(ii) unitary : $P\Gamma U(2r, q^2)$, $P\Gamma U(2r+1, q^2)$

(iii) orthogonal : $P\Gamma O^+(2r, q)$, $P\Gamma O(2r+1, q)$, $P\Gamma O^-(2r+2, q)$.

The exceptional case is that of the polar space arising from the hyperbolic quadric $Q^+(3, q)$ in $\mathrm{PG}(3, q)$. Note that this example is in fact a generalised quadrangle, and when considered as such there exist automorphisms permuting the lines in ways not possible when considered as a polar space for fields of order at least 4.

1.2 Orthogonal spaces and quadrics

The situation for orthogonal polar spaces is somewhat more involved than that for the other examples, and so we study them closer here.

Firstly, we justify the use of the superscripts + and − to distinguish isometry classes of orthogonal spaces of even rank, and introduce the concept of a discriminant when q is odd to distinguish the two isometry classes arising in general.

Consider the orthogonal direct sum of two nondegenerate orthogonal spaces U and W, each of even rank. If U and W are both hyperbolic, then $U \perp W$ is hyperbolic by definition. If, without loss of generality, U is elliptic and W is hyperbolic, then $U \perp W$ is elliptic by definition. However, if both U and W are elliptic, it is not so clear whether their orthogonal direct sum is hyperbolic or elliptic. Suppose $V = U \perp W$ is elliptic. Since U is nondegenerate, $V = U \perp U^\perp$, and so by the classification above, W is isometric to $U^\perp$. But we know from the previous case that $U^\perp$ must be hyperbolic when U and V are elliptic, and so $U \perp W$ must be hyperbolic.

Thus we can determine the isometry type of an even rank orthogonal space if we can decompose the space into an orthogonal direct sum of nondegenerate even rank subspaces for which we know the isometry type of each.

For q odd, consider two nondegenerate orthogonal spaces V_1, V_2 over $GF(q)$ with quadratic forms Q_1, Q_2 respectively, and suppose they are isometric with respect to some isometry T. Let X_i be a basis for V_i and let B_i be the nonsingular matrix of f_{Q_i} with respect to X_i, for $i = 1, 2$. Let P be the nonsingular transition matrix corresponding to T. Then $B_2 = P^T B_1 P$. So $\det(B_2) = \det(P)^2.\det(B_1)$. Thus, up to a nonzero square multiple, the determinants of the matrices of any bases of isometric orthogonal spaces are equivalent.

Let $F^* = GF(q)\backslash\{0\}$ be the multiplicative group of $GF(q)$, q odd. Then $\square = \{t^2 | t \in F^*\}$ is a subgroup of F^* of index 2. Let $\boxtimes$ be the other coset of $\square$ in F^*, so that $F^*/\square = \{\square, \boxtimes\}$.

Let V be a nondegenerate orthogonal space over $GF(q)$, q odd, with quadratic form Q, and let B be the nonsingular matrix of some basis X of V with respect to the polar form f_Q of Q. Define the **discriminant of** Q as $\mathrm{disc}(Q) = \det(B)\square \in F^*/\square$. From the discussion above, it is clear that the discriminant is an invariant of nondegenerate orthogonal spaces over finite fields of odd order, up to isometry. In other words, such spaces are isometric if and only if they have the same discriminant.

Suppose V is the orthogonal direct sum of two nondegenerate orthogonal spaces U and W, with repsect to the quadratic form Q. Let A, B, C be matrices of V, U, W respectively. Then $A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$, and so $\mathrm{disc}(Q) = \det(A)\square = (\det(B)\det(C))\square = (\det(B)\square)(\det(C)\square) = \mathrm{disc}(Q|_U)\mathrm{disc}(Q|_W)$, where $Q|_U$ is the quadratic form obtained by restricting Q to the subspace U.

Motivated by this, the use of the superscripts $+$ and $-$ for the two isometry classes of nondegenerate orthogonal spaces of even rank is then familiar with the notion of multiplying positive and negative integers : "minus times minus is plus" corresponds to the orthogonal direct sum of two elliptic spaces being hyperbolic, as we saw earlier.

Let V be a nondegenerate orthogonal space of even rank $2r$ over $GF(q)$, q odd, arising from the quadratic form Q. Suppose V is hyperbolic, that is, $V = l_1 \perp \ldots \perp l_r$ for some hyperbolic lines l_i. Now l_j has matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to f_Q restricted to l_j. So $\mathrm{disc}(Q|_{l_j}) = (-1)\square$. Thus from above, $\mathrm{disc}(Q) = ((-1)\square)^r = (-1)^r\square$.

Now $-1 \in \square$ if and only if $q \equiv 1 (\mathrm{mod}\ 4)$, so we have the following for a hyperbolic space :

$$\operatorname{disc}(Q) = \begin{cases} \square, \text{if } q \equiv 1 (\text{mod } 4) \text{ or } r \text{ is even} \\ \boxtimes, \text{if } q \equiv 3 (\text{mod } 4) \text{ and } r \text{ is odd} \end{cases}$$

So depending upon q and r, the value of the discriminant completely determines the isometry type of a nondegenerate orthogonal space of even rank $2r$ over a finite field of odd order; that is, the discriminant is a complete invariant of such spaces, up to isometry.

For nondegenerate orthogonal spaces of odd rank $2r+1$, there are also two isometry classes. If, for q odd, we can show that both values of the discriminant do occur, then as the discriminant is an invariant up to isometry, it will be a complete invariant of such spaces, up to isometry.

So consider the following two nondegenerate quadratic forms over $GF(q)$:

$$Q_1 : x_0x_{2r} + x_1x_{2r-1} + \ldots + x_{r-1}x_{r+1} - x_r^2;$$

$$Q_n : x_0x_{2r} + x_1x_{2r-1} + \ldots + x_{r-1}x_{r+1} - nx_r^2.$$

Calculating the discriminant of each we have :

$$\operatorname{disc}(Q_1) = \begin{cases} -1\square, \text{ if } r \text{ is even} \\ 1\square, \text{ if } r \text{ is odd} \end{cases} ; \operatorname{disc}(Q_n) = \begin{cases} -n\square, \text{ if } r \text{ is even} \\ n\square, \text{ if } r \text{ is odd} \end{cases} .$$

Now if $q \equiv 1 \pmod 4$, then $-1 \in \square$, and so $\operatorname{disc}(Q_1) \in \square$ for all r, and $\operatorname{disc}(Q_n) \in \boxtimes$ for all r.

If $q \equiv 3 \pmod 4$, then $-1 \in \boxtimes$, and we can choose $n = -1$. Then

$$\operatorname{disc}(Q_1) = \begin{cases} \boxtimes, \text{ if } r \text{ is even} \\ \square, \text{ if } r \text{ is odd} \end{cases} ; \operatorname{disc}(Q_n) = \begin{cases} \square, \text{ if } r \text{ is even} \\ \boxtimes, \text{ if } r \text{ is odd} \end{cases} .$$

So in general, the discriminant is a complete invariant of nondegenerate orthogonal spaces over finite fields of odd order, up to isometry.

Of course, for q even, $\square = F^*$, and so the discriminant as defined has little meaning in this case.

We now study in more detail some quadrics of low-dimensional (Desarguesian) projective spaces, which will appear in many sections of material later.

From above, we know that all nondegenerate quadrics in PG$(2, q)$ are similar. Such a quadric is called a **conic**. If the defining quadratic form is $Q : x_1^2 - x_0x_2$, a conic may be parametrised as follows :

$$\mathcal{C} = \{\langle(t^2, t, 1)\rangle | t \in GF(q)\} \cup \{\langle(1, 0, 0)\rangle\}.$$

Thus a conic consists of $q + 1$ points. Our analysis of the discriminant for parabolic spaces shows that the other isometry class of conics may be represented by the quadratic form $Q' : nx_1^2 - x_0x_2$, for some nonsquare $n \in \boxtimes$.

Let l be a line of PG(n, q) and suppose l contains three distinct points $P = \langle u\rangle, P' = \langle v\rangle, R = \langle u + av\rangle$ of some quadric $\mathcal{Q}$, defined by the quadratic form Q. Then $f_Q(u, v) = 0$ (expand $Q(u + av) = 0$), and so for any point $X = \langle u + bv\rangle$ on l we have $Q(u + bv) = 0$. That is, if a line l contains three distinct points of the quadric $\mathcal{Q}$, then l is a line of $\mathcal{Q}$.

As the Witt index for a conic is 1, a conic contains no lines, and so no three points of a conic are collinear. This property motivates the general definition of a k**-arc** of a projective plane as a set of k points, no three collinear. The largest possible k-arc of a projective plane of order n has size $n+2$ and is called a **hyperoval**. Hyperovals exist only when n is even. A k-arc of size $n + 1$ is called an **oval**, and so a conic in PG$(2, q)$ is an oval. For q odd, the converse is also true.

Theorem 1.10 (Segre (1955)). *If q is odd, every oval in PG$(2, q)$ is a conic.*

For q even, there exist examples of ovals which are not conics. We also mention that a degenerate quadric in PG$(2, q)$ is either a single point, a single line, or two intersecting lines, i.e., a subspace or the union of two hyperplanes.

Now consider PG$(3, q)$. From above, we know there are two isometry classes of nondegenerate quadrics in PG$(3, q)$, called hyperbolic and elliptic.

Let $\mathcal{H}$ be a nondegenerate hyperbolic quadric in PG$(3, q)$. Then $\mathcal{H}$ has Witt index 2, and so contains both points and lines.

Let $\mathcal{R}$ be a nonempty set of mutually **skew** lines of PG$(3, q)$, that is, no two distinct lines of $\mathcal{R}$ have a point in common. A line l is called a **transversal** of $\mathcal{R}$ if it meets each line of $\mathcal{R}$ in exactly one point. If through each point of each line of $\mathcal{R}$ there is a transversal of $\mathcal{R}$, and through each point of a transversal of $\mathcal{R}$ there is a line of $\mathcal{R}$, then we call $\mathcal{R}$ a **regulus**. The set $\mathcal{R}'$ of all transversals of the regulus $\mathcal{R}$ forms a regulus, called the **opposite regulus** of $\mathcal{R}$. Any regulus contains exactly $q+1$ lines, and through any three distinct mutually skew lines, there is exactly one regulus.

The points of a nondegenerate hyperbolic quadric $\mathcal{H}$ in $\mathrm{PG}(3,q)$ are the points on some regulus $\mathcal{R}$, and the lines of $\mathcal{H}$ are the lines of $\mathcal{R}$ together with the lines of the opposite regulus $\mathcal{R}'$. This can easily be seen by considering the three mutually skew lines

$$l_1 = \langle(1,0,0,0),(0,1,0,0)\rangle, l_2 = \langle(0,0,1,0),(0,0,0,1)\rangle, l_3 = \langle(1,0,1,0),(0,1,0,1)\rangle.$$

The points $\langle(x_0,x_1,x_2,x_3)\rangle$ on the unique regulus through l_1,l_2,l_3 satisfy the nondegenerate quadratic equation $Q(x) = x_0x_3 - x_1x_2 = 0$, which has $\mathrm{disc}(Q) = \Box$.

The number of points on a nondegenerate hyperbolic quadric in $\mathrm{PG}(3,q)$ is then $(q+1)^2$.

Just as the lines of $\mathcal{H}$ fall naturally into two classes, in general for hyperbolic spaces, the maximal totally singular subspaces form two distinct classes. Suppose that V is a hyperbolic orthogonal space of Witt index $m > 0$, and consider two maximal totally singular subspaces M, N of V. If we define a relation on the set of all maximal totally singular subspaces by considering for M and N the parity of the corank of their intersection in each, then we find that this defines an equivalence relation on the set of all maximal totally singular subspaces. There will be two equivalence classes, and subspaces are in the same class if and only if the corank of their intersection in each is even. It is clear that this relation is reflexive and symmetric, but the fact that it is also transitive is not so clear. See Cameron (year unknown) or Beutelspacher and Rosenbaum (1998) for a proof.

Now let $\mathcal{E}$ be a nondegenerate elliptic quadric in $\mathrm{PG}(3,q)$. Then $\mathcal{E}$ has Witt index 1, and so contains only points. Thus no three points of $\mathcal{E}$ are collinear.

Let $p(x) \in GF(q)[x]$ be an irreducible polynomial of degree 2 over $GF(q)$, and suppose $p(x) = ax^2 + bx + c$. Define the nonconcurrent lines $l = \langle(1,0,0,0),(0,0,0,1)\rangle$ and $m = \{(0,x_1,x_2,0) | ax_1^2 + bx_1x_2 + cx_2^2 \neq 0\}$ of $\mathrm{PG}(3,q)$. Then, with respect to the quadratic form $Q(x) = x_0x_3 + ax_1^2 + bx_1x_2 + cx_2^2$, l is a hyperbolic line and m is an anisotropic line. We know from the classification of such spaces above that $\mathcal{E}$ is an orthogonal direct sum of a hyperbolic line and an anisotropic line, and so the points $\langle x\rangle = \langle(x_0,x_1,x_2,x_3)\rangle$ of $\mathrm{PG}(3,q)$ such that $Q(x) = 0$ form an elliptic quadric $\mathcal{E}$. The only point on $\mathcal{E}$ with $x_3 = 0$ is $\langle(1,0,0,0)\rangle$. If $x_3 \neq 0$, then, without loss of generality, take $x_3 = 1$. Then $x_0 = -ax_1^2 - bx_1x_2 - cx_2^2$, and so $\langle(-as^2 - bst - ct^2, s, t, 1)\rangle$ is a point on $\mathcal{E}$ for all $s, t \in GF(q)$. Hence the number of points on a nondegenerate elliptic quadric in PG$(3, q)$ is $q^2 + 1$.

A **k-cap** of PG$(3, q)$ is a set of k points, no three collinear. The largest possible k-cap for $q > 2$ has size $q^2 + 1$ and is called an **ovoid**. So an elliptic quadric in PG$(3, q)$ is an ovoid. For q odd, the converse is also true.

Theorem 1.11 (Barlotti (1955), Panella (1955)). *If q is odd, every ovoid in $PG(3, q)$ is an elliptic quadric.*

Now let $\mathcal{C}$ be a conic in PG$(2, q)$, and embed PG$(2, q)$ as a hyperplane π of PG$(3, q)$. For a point P not on π, take the lines through P which meet $\mathcal{C}$ in a point. There are necessarily $q+1$ such lines, and the set of (q^2+q+1) points on these lines form a **quadratic cone**. The point P is called the **vertex** of the quadratic cone $\mathcal{K}$, and $\mathcal{K}$ is said to **project** the conic $\mathcal{C}$.

The pointwise stabiliser of π in $P\Gamma L(4, q)$ is transitive on points not on π, and $P\Gamma L(4, q)_\pi$ induces $P\Gamma L(3, q)$ on π. Since all conics of PG$(2, q)$ are equivalent under $P\Gamma L(3, q)$, it follows that all quadratic cones of PG$(3, q)$ are equivalent under $P\Gamma L(4, q)$.

Suppose π is the plane $x_3 = 0$ of PG$(3, q)$, and take $P = \langle(0, 0, 0, 1)\rangle$ not on π. Consider the quadric $\mathcal{Q}$ of PG$(3, q)$ defined by the quadratic form $Q : x_1^2 - x_0x_2$. Then $\mathcal{Q}$ is the quadratic cone with vertex P meeting π in the conic $\mathcal{C} = \{\langle(t^2, t, 1, 0)\rangle | t \in GF(q)\} \cup \{\langle(1, 0, 0, 0)\rangle\}$. Clearly $\mathcal{Q}$ is degenerate, since the point P is collinear with all points of $\mathcal{Q}$; in fact, the singular radical of Q is $\{(0, 0, 0, a) : a \in GF(q)\} = P$.

In PG$(3, q)$ we also have the generalised notion of an **oval cone**, that is, a cone projecting an oval of some hyperplane of PG$(3, q)$. Of course, for q odd, an oval cone is a quadratic cone, but for q even there exist examples of oval cones which are not quadratic cones. The other types of degenerate quadrics in PG$(3, q)$ are a subspace or the union of two hyperplanes.

Note that restricting a quadratic form defining some quadric $\mathcal{Q}$ in PG(n, q) to a subspace S of PG(n, q) will define a quadric $\mathcal{Q}_S$ of S. If $\mathcal{Q}$ is an elliptic quadric, a hyperbolic quadric or a quadratic cone in PG$(3, q)$, and π is a plane, then $\mathcal{Q}_\pi$ is a quadric of π. In the following chapters we will be interested in studying plane sections of these three quadrics which are conics.

1.2.1 The Klein correspondence The classical correspondence between projective 3-space and a nondegenerate hyperbolic quadric in projective 5-space is often referred to as the *Klein correspondence*, after the German mathematician Felix Klein (1849-1925), who first studied the correspondence over the complex numbers in his dissertation of 1868 (reprinted in his collected works). The correspondence is valid over an arbitrary field, and arises from defining a simple set of homogeneous coordinates for points in projective 5-space, called *Plücker coordinates* after the Prussian geometer and physicist Julius Plücker (1801-1868).

For a line l in $\mathrm{PG}(3,q)$ through the points $\langle u\rangle = \langle(u_0,\ldots,u_3)\rangle$ and $\langle v\rangle = \langle(v_0,\ldots,v_3)\rangle$, define a point $P = \langle(p_{01}(u,v), p_{02}(u,v), p_{03}(u,v), p_{12}(u,v), p_{31}(u,v), p_{23}(u,v))\rangle$ of $\mathrm{PG}(5,q)$, where $p_{ij}(u,v) = u_iv_j - u_jv_i$ are the Plücker coordinates of l. Then P is a point on the nondegenerate hyperbolic quadric $Q^+(5,q)$ of $\mathrm{PG}(5,q)$ defined by the quadratic form $Q : x_0x_5 + x_1x_4 + x_2x_3$. The bijective mapping from the set of all lines of $\mathrm{PG}(3,q)$ to the set of all points of $Q^+(5,q)$ is often called the *Klein mapping* (or *Plücker mapping*) and $Q^+(5,q)$ is called the **Klein quadric**. This mapping determines a complete correspondence between $\mathrm{PG}(3,q)$ and $Q^+(5,q)$.

Concurrence of lines of $\mathrm{PG}(3,q)$ corresponds to collinearity (in a line of $Q^+(5,q)$) of points of $Q^+(5,q)$, and so a maximal set of pairwise concurrent lines of $\mathrm{PG}(3,q)$ corresponds to a maximal set of pairwise collinear points of $Q^+(5,q)$. A set of pairwise concurrent lines of $\mathrm{PG}(3,q)$ can be either a set of lines all through a common point, or a set of lines all in a common plane. A set of pairwise collinear points of $Q^+(5,q)$ is a set of points on a maximal subspace of $Q^+(5,q)$, that is, on a plane of $Q^+(5,q)$. As $Q^+(5,q)$ is a hyperbolic quadric, the planes fall into two classes, and these two classes correspond to the two possibilities for a maximal set of pairwise concurrent lines of $\mathrm{PG}(3,q)$, that is, to the points and the planes of $\mathrm{PG}(3,q)$. We label the planes of $Q^+(5,q)$ corresponding to points of $\mathrm{PG}(3,q)$ as type I planes, and planes of $Q^+(5,q)$ corresponding to planes of $\mathrm{PG}(3,q)$ as type II planes. Two planes of the same type intersect in a point, since two points (planes) of $\mathrm{PG}(3,q)$ lie on a unique line. Two planes of different types intersect in a line or are disjoint according to whether the corresponding point-plane pair of $\mathrm{PG}(3,q)$ is incident or nonincident, respectively. So the lines of $Q^+(5,q)$ correspond to incident point-plane pairs of $\mathrm{PG}(3,q)$, and a line of $Q^+(5,q)$ lies in one plane of type I and one plane of type II. Note that the arbitrary labelling of the planes of $Q^+(5,q)$ is permitted, due to the principle of duality in projective spaces, and hence explains why the correspondence cannot be strengthened to an isomorphism of structures.

Consequently, the correlation group of $\mathrm{PG}(3,q)$ is isomorphic to $P\Gamma O^{+}(6,q)$, the full collineation group of $Q^{+}(5,q)$.

For a detailed list of substructures of $\mathrm{PG}(3,q)$ and $Q^{+}(5,q)$ which Klein correspond, see Hirschfeld (1985).

Theorem 1.12. *The dual of the polar space arising from the nondegenerate quadric $Q(4,q)$ is isomorphic to the polar space arising from the nondegenerate symplectic space $Sp(4,q)$.*

Proof : Since all nondegenerate symplectic spaces of a given rank are isometric, we may take any alternating form as the underlying form on the space. The canonical form is $f : x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$, so for all points $\langle x\rangle, \langle y\rangle$ on lines of the symplectic polar space $\Pi(Sp(4,q))$ we have

$$x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 = 0.$$

Thus the Plücker coordinates of the lines of $\Pi(Sp(4,q))$ satisfy $p_{12} + p_{34} = 0$. Now if we apply the Klein correspondence to these lines, the images will as usual lie on the Klein quadric, but they will now satisfy a quadratic equation in five variables, namely,

$$Q \ : \ -p_{12}^2 + p_{13}p_{42} + p_{14}p_{23} = 0.$$

Thus the lines of $\Pi(Sp(4,q))$ correspond to the points of $\Pi(Q(4,q))$ defined by Q. All lines of $\Pi(Sp(4,q))$ on a point of $\Pi(Sp(4,q))$ are pairwise concurrent and so their images under the Klein correspondence are pairwise collinear in totally singular lines, and hence in the same totally singular line, since $Q(4,q)$ does not contain planes. Hence the points of $\Pi(Sp(4,q))$ correspond to the lines of $\Pi(Q(4,q))$, and the polar spaces are dual to one another.

Theorem 1.13. *The dual of the polar space arising from the nondegenerate quadric $Q^{-}(5,q)$ is isomorphic to the polar space arising from the nondegenerate unitary space $U(4,q^2)$.*

Proof : Let $\tau \in P\Gamma O^{+}(6,q^2)$ be a collineation of $Q^{+}(5,q^2)$ of order two, whose fixed points are the points of the subgeometry $Q^{-}(5,q)$. (Such collineations exist, and are often called *Baer involutions*.) Then for any line l of $Q^{+}(5,q^2)$ which meets $Q^{-}(5,q)$ in a subline (fixed by τ), the plane of type I on l must be mapped by τ to the plane of type II on l. Hence τ interchanges the two classes of planes on $Q^{+}(5,q^2)$, and so Klein corresponds to a duality of $\mathrm{PG}(3,q^2)$. Since τ has order two, the corresponding duality is a polarity π of $\mathrm{PG}(3,q^2)$. The number of points of $Q^-(5,q)$ is $(q+1)(q^3+1)$, by Theorem 1.8, and so τ fixes this number of points of $Q^+(5,q^2)$. Hence π fixes $(q+1)(q^3+1)$ totally isotropic lines of $\mathrm{PG}(3,q^2)$. Thus the polar rank of the polar space arising from π is at least two, and from the classification of such spaces in the previous section, it can be at most two. Hence, by Theorem 1.9, the polar space arising from π must be the polar space arising from the nondegenerate unitary space $U(4,q^2)$. Thus the points of $\Pi(Q^-(5,q))$ correspond to the lines of $\Pi(U(4,q^2))$, and so from the Klein correspondence, the lines of $\Pi(Q^-(5,q))$ correspond to the points of $\Pi(U(4,q^2))$.

The above theorems can be found in Payne and Thas (1984). The second result appears in Thas and Payne (1976) and in Bruen and Hirschfeld (1978).

Translation planes and elation generalised quadrangles

The previous chapter displays a strong analogy between projective spaces and polar spaces; especially with respect to the projective spaces of dimension 2 and the polar spaces of polar rank 2. The reason for this analogy is that these classes of "point-line" incidence structures can be viewed in a wider setting. We briefly discuss some of these ideas before focussing on the individual topics of interest.

An **incidence structure** $\mathcal{I} = (\mathcal{P}, \mathcal{L}, \mathtt{I})$ is a set of *points* $\mathcal{P}$ and a set of *lines* $\mathcal{L}$, where $\mathcal{P}$ and $\mathcal{L}$ are disjoint, nonempty sets, and $\mathtt{I} \subseteq \mathcal{P} \times \mathcal{L}$ defines incidence. Noting that the incidence graph of $\mathcal{I}$ is bipartite, we define a particularly nice class of incidence structures known as *generalised polygons.* A **generalised** n**-gon** is a bipartite graph of diameter n and girth $2n$. To avoid trivial cases, we assume that $n \geq 3$, and if the degree of each vertex is at least 3, a generalised n-gon is called **thick**. Then Feit and Higman (1964) proved that any finite, thick generalised n-gon has $n \in \{3, 4, 6, 8\}$. The generalised 3-gons are the projective planes, and the generalised 4-gons are the generalised quadrangles. For $n = 6$ they are called **generalised hexagons**, and for $n = 8$ they are called **generalised octagons**.

Generalised polygons were introduced by Tits (1959) while studying finite simple groups of Lie type in prime characteristic. They arose through the following observation.

Consider an incidence structure $\mathcal{I} = (\mathcal{P}, \mathcal{L}, \mathtt{I})$. An element (P, l) of $\mathtt{I}$ is called a **flag**. If a subgroup G of automorphisms of $\mathcal{I}$ acts transitively on the set $\mathtt{I}$ of flags, then G is said to be **flag-transitive**. Now suppose H and K are subgroups of some group G. Take $\mathcal{P} = (G : H)$ to be the set of cosets of H in G, $\mathcal{L} = (G : K)$ to be the set of cosets of K in G, and $\mathtt{I} = \{(Hg, Kl) \subseteq \mathcal{P} \times \mathcal{L} : Hg \cap Kl \neq \emptyset\}$ to be nonempty intersection of cosets. Then $\mathcal{I} = (\mathcal{P}, \mathcal{L}, \mathtt{I})$ is an incidence structure on which the subgroup G of automorphisms of $\mathcal{I}$ acts flag-transitively. Tits (1956) observed the remarkable fact that every flag-transitive incidence structure is of this form, for some group G.

If G is a finite simple group of Lie type in characteristic p, p prime, then take U to be a Sylow p-subgroup of G, and let $B = N_G(U)$ be the normaliser of U in G. Let $M_1, \ldots, M_r$ be the maximal subgroups of G containing B. Then r is the Lie rank of G, and if $r = 2$, the incidence structure with points $(G : M_1)$, lines $(G : M_2)$ and incidence as nonempty intersection is a flag-transitive generalised polygon. The generalised polygons arising are essentially the *classical* examples within each class; that is, for example, the generalised 3-gons arising (from $PSL(3,q)$) are the Desarguesian projective planes $\mathrm{PG}(2,q)$, and the generalised 4-gons arising are (essentially) the finite classical polar spaces of polar rank 2. (If $r > 2$ we (essentially) obtain the finite Desarguesian projective spaces of dimension r and the finite classical polar spaces of polar rank r.)

The aim of this chapter is to introduce the study of two classes of generalised polygons which are intimately connected with our central topic, namely, translation projective planes and elation generalised quadrangles. In some sense, we weaken the concept of flag-transitivity in the above coset geometry construction, and instead act regularly on the elements furthest from some fixed element in the incidence graph of the generalised polygon. The somewhat natural approach for the projective planes motivates the analogous concepts for the generalised quadrangles. Furthermore, translation projective planes and elation generalised quadrangles represent most known examples of these two types of generalised polygons. For a complete study of all generalised polygons see, for example, van Maldeghem (1998). For recent surveys on topics in the theory of generalised polygons, see [42].

As many examples of these incidence structures are not naturally embedded in projective spaces, we cannot consider equivalence of such structures under the automorphism group of some projective geometry. As mentioned earlier, mathematical equivalence is considered to be structure-preserving, and so two point-line incidence structures $\mathcal{I}_1 = (\mathcal{P}_1, \mathcal{L}_1, \mathtt{I}_1)$ and $\mathcal{I}_2 = (\mathcal{P}_2, \mathcal{L}_2, \mathtt{I}_2)$ are said to be **isomorphic** if and only if there exist bijective mappings from $\mathcal{P}_1$ onto $\mathcal{P}_2$, $\mathcal{L}_1$ onto $\mathcal{L}_2$ and $\mathtt{I}_1$ onto $\mathtt{I}_2$.

2.1 Projective planes

We begin with a short discussion of projective and affine planes. From the axioms for a projective space given earlier, a **projective plane** is an incidence structure consisting of a set of points and a set of distinguished subsets called lines, which satisfies the following three conditions :

(i) any two points lie on a unique line;

(ii) any line contains at least three points;

(iii) any two lines meet in a unique point.

Recall that the **order** of a projective plane is defined to be one less than the number of points on a line, which we saw earlier is a constant for any projective geometry.

Thus the order of a projective plane is at least 2.

An **affine plane** is a point-line incidence structure satisfying the following three conditions :

(i) any two points lie on a unique line;

(ii) if l is a line and P is a point, then there is a unique line containing P and parallel to (i.e., equal to or disjoint from) l;

(iii) there exist three noncollinear points.

Note that the first two conditions imply that parallelism is an equivalence relation on the set of lines, and that each equivalence class partitions the set of points. The number of points on a line of an affine plane is the **order** of the affine plane.

The connection between projective and affine planes is simple : by removing a line l and all of its points from a projective plane $\mathbf{P}$, one obtains an affine plane $\mathbf{A} = \mathbf{P}^l$. Conversely, given an affine plane, adjoin a 'point at infinity' corresponding to each parallel class of lines, which is incident with every line of the class, and adjoin a 'line at infinity' incident with all points at infinity. The structure obtained is a projective plane, sometimes called the **projective completion** of the affine plane. Hence an affine plane is equivalent to a projective plane with a distinguished line.

This concept naturally generalises to projective and affine spaces, where we remove a hyperplane and all of its subspaces from a projective space to obtain an affine space.

For a Desarguesian projective space we have a natural coordinate system arising from the choice of some basis for the underlying vector space. Since points of the projective space are represented by vector subspaces of rank one, these coordinates are *homogeneous* in that they are defined up to a scalar multiple. For non-Desarguesian projective planes, coordinates can be introduced by fixing an (ordered) quadrangle, that is, a set of four points, no three collinear. With respect to this quadrangle, coordinates can be defined in the affine plane arising from some line of the quadrangle, by setting up a one-to-one correspondence between the points of the affine plane and the ordered pairs of elements of some set $\mathcal{T}$ of cardinality equal to the order of the affine plane. A ternary operation can be defined on such a set $\mathcal{T}$ representing an arbitrary line of the affine plane, and satisfying certain properties arising from the axioms for the projective plane. Such a set $\mathcal{T}$ is called a *ternary field* (or *planar* *ternary ring*), and from any such ternary field, an affine plane may be constructed, so that there is a canonical correspondence between ternary fields and projective planes with distinguished ordered quadrangles. If the ternary operation is written as $a \cdot b \circ c$ for $a, b, c \in \mathcal{T}$, then *addition* in $\mathcal{T}$ is defined as $a + b = a \cdot 1 \circ b$ and multiplication as $ab = a \cdot b \circ 0$, where 0 and 1 are two distinct elements of $\mathcal{T}$. Coordinates for points can then be given in the forms $(0,0,1), (0,1,a), (1,a,b)$ for $a, b \in \mathcal{T}$ and coordinates for lines in the forms $[0,0,1], [0,1,a], [1,a,b]$ for $a, b \in \mathcal{T}$. These *homogeneous* coordinates have the property that the point (x_0, x_1, x_2) is incident with the line $[y_0, y_1, y_2]$ if and only if $y_0x_2 = x_1 \cdot y_1 \circ x_0y_2$. The projective plane is Desarguesian if and only if the ternary field is a skew field, and so in the finite case, as we have seen, if and only if the ternary field is $GF(q)$. For more details and precise definitions of ternary fields, see Dembowski (1968), pp127-131. A good reference for the theory of projective planes in general is Hughes and Piper (1973).

2.1.1 Translation planes A collineation of a projective geometry was defined earlier. For an affine geometry, it is the same concept, that is, a permutation of the points which maps lines onto lines, and hence maps subspaces onto subspaces.

A point P is a **centre** of the collineation ϕ if all subspaces containing P are fixed by ϕ. A hyperplane H is an **axis** of ϕ if every point of H is fixed by ϕ. We call a collineation **central** or **axial** if it has a centre or an axis, respectively. Nontrivial collineations can have at most one centre and at most one axis, and a collineation of a projective geometry has a centre if and only if it has an axis. A central collineation is called an **elation** or a **homology** if it has an incident or nonincident centre-axis pair, respectively.

Let $\mathbf{A}$ be an affine plane and $\mathbf{P}$ the corresponding projective plane, so that $\mathbf{A} = \mathbf{P}^l$ for some line l of $\mathbf{P}$. A collineation of $\mathbf{A}$ is called a **translation** if, when considered as a collineation of $\mathbf{P}$, it is an elation with axis l. The set of all translations of an affine plane $\mathbf{A}$ forms a group T under composition, and we call $\mathbf{A}$ a **translation affine plane** if T is transitive on the points of $\mathbf{A}$. The projective completion $\mathbf{P}$ of $\mathbf{A}$ is then called a **translation plane**. We may rephrase this by saying that a projective plane π is a translation plane if and only if there is a line l of π and a subgroup G of Autπ, which fixes every point on l, and acts regularly on the set of points not on l. The group G is called the **translation group**, and l the **translation line**.

Let $\mathbf{A}$ be a translation affine plane and T be its full translation group. Suppose $\mathbf{A} = \mathbf{P}^l$ and consider T as the group of all elations with axis l of the projective plane $\mathbf{P}$. If we define $G(P,l)$ to be the set of all collineations of $\mathbf{P}$ with centre P and axis l, then $G(P,l)$ is a subgroup of the full collineation group of $\mathbf{P}$, and so $T = \bigcup_{P\mathrm{I}l} G(P,l)$. As the $P\mathrm{I}l$ are just the parallel classes of $\mathbf{A}$, we can write $T = \bigcup_i T_i$, where T_i denotes the subgroup of T which fixes every line of the i-th parallel class of $\mathbf{A}$. Since the centre and axis of a nontrivial collineation are unique, it follows that $T_i \cap T_j = 1$ for $i \neq j$, otherwise there would exist a nontrivial collineation fixing two distinct parallel classes linewise, and thus fix linewise two distinct points of l. Thus the T_i form a partition of T, and furthermore, this is a **congruence partition** of T in the sense that if $i \neq j$ then $T_iT_j = T$.

Conversely, if T is an abstract group possessing a nontrivial congruence partition, i.e., a set of subgroups T_i such that $T = \bigcup_i T_i$, $T_i \cap T_j = 1$ and $T_iT_j = T$ for $i \neq j$, then T may be regarded as the full translation group of a translation affine plane. The incidence structure with points the elements of T, with lines the cosets of the T_i in T, and with incidence as set theoretic inclusion, is a translation affine plane with T as its full translation group.

Hence there is a canonical correspondence between translation affine planes and congruence partitions of groups, that is, the isomorphism classes of translation affine planes can be put into a one-to-one correspondence with the isomorphism classes of groups with congruence partitions. This was first proved by André (1954).

The **kernel** of the translation affine plane $\mathbf{A}$ is the set $K(\mathbf{A})$ of all endomorphisms α of the translation group T such that $T_i^\alpha \subseteq T_i$ for all i parallel classes. With usual addition and multiplication of endomorphisms, $K(\mathbf{A})$ is a ring, and in fact André (1954) showed it is also a skew field, and hence in the finite case, $GF(q)$. As translations commute with one another, the translation group T of a translation affine plane is abelian, and in fact, T is elementary abelian. Thus regarding T as a vector space over some finite field $F \subseteq K(\mathbf{A})$, we see that the subgroups T_i of the congruence partition are in fact subspaces of T. Hence in the corresponding projective geometry $\mathrm{PG}(T)$ arising from the vector space T, these subgroups form a collection of mutually disjoint subspaces covering all of $\mathrm{PG}(T)$. Such a collection $\mathcal{S}$ is called a **spread** of $\mathrm{PG}(T)$, and furthermore, $\mathcal{S}$ has the property that any two distinct subspaces of $\mathcal{S}$ span the whole of $\mathrm{PG}(T)$. Conversely, every spread of $\mathrm{PG}(V)$ with this property defines a congruence partition of the additive group of the underlying vector space V, and hence defines a translation affine plane, as above. Thus we have in the finite case :

Theorem 2.1 (André (1954)). *For a finite field F of order q and positive integer*

t, there is a canonical correspondence between the translation affine planes $\mathbf{A}$ of order q^{t+1} with $F \subseteq K(\mathbf{A})$, and the t-dimensional subspace spreads of $PG(2t+1, q)$.

This was first proved by André (1954) in more generality, and then later rediscovered independently by Bruck and Bose (1964) and by Segre (1964). In fact, most known finite projective planes are either translation planes or closely related to them. See Kallaher (1982), Lüneburg (1980) and Ostrom (1970) for more on translation planes.

The coordinatising ternary field of a translation affine plane is known as a *quasifield*. As an example, we will consider a certain type of quasifield known as a *semifield*. Let S be a finite set, with two binary operations "+" and "·" such that

(i) $S(+)$ is an abelian group, with identity 0;

(ii) both distributive laws hold in S;

(iii) there exists a multiplicative identity 1;

(iv) $x \cdot y = 0$ if and only if $x = 0$ or $y = 0$.

Then S is called a (finite) **semifield**, and if multiplication is not associative, so that S is not a field, S is called a **proper** semifield. The **middle nucleus** $N = \{n \in S : (xn)y = x(ny), \forall x, y \in S\}$ of S is a field, and S may be regarded as a vector space over N. Clearly, a proper semifield has $N \neq S$. A finite semifield necessarily has prime power order, and proper finite semifields exist for all orders $q = p^h$, where $h \geq 2$ if p is odd and $h \geq 4$ if $p = 2$. A translation plane coordinatised by a semifield is called a **semifield translation plane**.

Let S be a (multiplicatively) commutative semifield of order q^2 whose middle nucleus is $GF(q)$, so that S may be regarded as a vector space of rank 2 over $GF(q)$. Then $S = \{t\alpha + \beta : \alpha, \beta \in GF(q)\}$ for some $t \in S \backslash GF(q)$. Let addition in S be component-wise, and multiplication be defined as follows :

$$(t\alpha + \beta)(t\gamma + \delta) = t(t(\alpha\gamma)) + t(\beta\gamma) + t(\alpha\delta) + \beta\delta.$$

If we write $t(tx)) = tf(x) + g(x)$ for all $x \in GF(q)$, where $f, g : GF(q) \to GF(q)$, then we have :

$$(t\alpha + \beta)(t\gamma + \delta) = t[f(\alpha\gamma) + \beta\gamma + \alpha\delta] + [g(\alpha\gamma) + \beta\delta].$$

With respect to this form of the multiplication, considering both distributive laws and the existence of zero divisors yields the following result.

Lemma 2.1 (Cohen and Ganley (1982)). *The above multiplication involving the maps f and g yields a semifield if and only if*

(i) f and g are linear maps from $GF(q)$ to $GF(q)$, and

(ii) $xy^2 + f(x)y - g(x) \neq 0$ for all $x, y \in GF(q)$, with $x \neq 0$.

The maps $f(x) = \alpha x$ and $g(x) = \beta x$, where $\alpha, \beta \in GF(q)$ and $w^2 + \alpha w - \beta$ is irreducible over $GF(q)$, yield an improper finite semifield of order q^2, namely $GF(q^2)$. Surprisingly, we have the following for $p = 2$.

Theorem 2.2 (Cohen and Ganley (1982)). *There is no proper commutative semifield of even order which is of rank 2 over its middle nucleus.*

For q odd however, there exist examples of proper commutative semifields of rank 2 over their middle nuclei.

Example (The Ganley semifields [Ganley (1981)]) Let $q = 3^h$, $h \geq 2$, and fix a nonsquare n of $GF(q)$. Define the following linear maps from $GF(q)$ to $GF(q)$:

$$f(x) = nx^3 \quad \text{and} \quad g(x) = nx^9 + n^3x.$$

To check the second condition in the above lemma, we must show that $f^2(x)+4xg(x)$ is a nonsquare of $GF(q)$ for all $x \neq 0$. Then

$$\begin{aligned} & f^2(x) + 4xg(x) \\ = \; & n^2x^6 + nx^{10} + n^3x^2 \\ = \; & nx^2(nx^4 + x^8 + n^2) \\ = \; & nx^2(x^4 - n)^2 \end{aligned}$$

and we have a proper commutative semifield of order q^2.

2.2 Generalised quadrangles

The finite classical polar spaces of polar rank 2 consist of points and lines. Each line has $q + 1$ points, and each point lies on $q^{1+e} + 1$ lines, where e is as in the table of finite classical polar spaces earlier.

Consider also Tits' polar space axiom from earlier. For polar spaces of polar rank 2 this says the following : given a line l and a point P not on l, there exists a unique subspace M containing P such that $M \cap l$ is a point and M contains all points of l

collinear with P. So M must be a line, and with respect to the all-or-one axiom of Buekenhout and Shult, this says that for polar spaces of rank 2, the 'all' alternative does not occur.

A **generalised quadrangle** is an incidence structure of points and lines with a symmetric incidence relation I satisfying

(i) each point is incident with a constant number $t+1$ of lines, and two distinct points are incident with ≤ 1 line;

(ii) each line is incident with a constant number $s+1$ of points, and two distinct lines are incident with ≤ 1 point;

(iii) for a non-incident point-line pair (P, l) there is a unique point Q and a unique line m such that $P \mathrm{I} m \mathrm{I} Q \mathrm{I} l$.

We will often abbreviate generalised quadrangle as GQ. We call (s,t) the **order** of a GQ, and if $s = t$, we say the GQ has order s. For a GQ $\mathbf{X}$ of order (s,t), the incidence structure with points the lines of $\mathbf{X}$ and lines the points of $\mathbf{X}$ is a GQ of order (t,s), called the **dual** GQ of $\mathbf{X}$. If $s > 1$ and $t > 1$, a GQ of order (s,t) is called **thick**; otherwise **thin**, and is an example of a **grid** (if $t = 1$) or a **dual grid** (if $s = 1$).

For a GQ $\mathbf{X} = (\mathcal{P}, \mathcal{L}, \mathrm{I})$, we often write $P \sim Q$ for $P, Q \in \mathcal{P}$ if P and Q are collinear (in a line of $\mathbf{X}$); $P^{\perp}$ for $\{Q \in \mathcal{P} | P \sim Q\}$; $\{P,Q\}^{\perp}$ for $P^{\perp} \cap Q^{\perp}$; $\{P,Q\}^{\perp\perp}$ for $\cap_{R \in \{P,Q\}^{\perp}} R^{\perp}$; and use the obvious dual notation.

Fix a line l of a GQ $\mathbf{X}$ of order (s,t). Each point P of $\mathbf{X}$ not on l lies on a unique line m concurrent with l, say in the point Q. There are $s+1$ points Q on l, each lying on t lines $m \neq l$, each containing s points $P \neq Q$, so the number of points not on l is $(s+1)st$. Hence the number of points of a GQ of order (s,t) is $(s+1)(st+1)$. The dual of a GQ of order (s,t) is a GQ of order (t,s), and so the number of lines of a GQ of order (s,t) is $(t+1)(st+1)$.

Theorem 2.3 (Higman (1974)). *If* $\mathbf{X}$ *is a GQ of order* (s,t) *with* $s > 1$ *and* $t > 1$*, then* $s \leq t^2$*, and dually,* $t \leq s^2$.

For these and many more results concerning finite generalised quadrangles we refer to the detailed monograph of Payne and Thas (1984).

2.2.1 The classical generalised quadrangles We list here the generalised quadrangles arising as classical polar spaces of polar rank 2.

1. W(q)=W($3,q$)=$\Pi(\rho)$ where ρ is a null polarity of PG($3,q$) is a GQ of order q.

2. Q($3,q$)=Q$^+$($3,q$) $=\Pi(\mathcal{Q}^+)$ where $\mathcal{Q}^+$ is a hyperbolic quadric of PG($3,q$) is a GQ of order $(q,1)$.

3. Q($4,q$)=$\Pi(\mathcal{Q})$ where $\mathcal{Q}$ is a parabolic quadric of PG($4,q$) is a GQ of order q.

4. Q($5,q$)=Q$^-$($5,q$)=$\Pi(\mathcal{Q}^-)$ where $\mathcal{Q}^-$ is an elliptic quadric of PG($5,q$) is a GQ of order (q,q^2).

5. H($3,q^2$)=$\Pi(\rho)$ where ρ is a unitary polarity of PG($3,q^2$) is a GQ of order (q^2,q).

6. H($4,q^2$)=$\Pi(\rho)$ where ρ is a unitary polarity of PG($4,q^2$) is a GQ of order (q^2,q^3).

The GQ Q($3,q$) of order $(q,1)$ is a thin GQ (or a grid), which is often considered a trivial structure, though being a hyperbolic quadric in PG($3,q$), often plays a very nontrivial role in much beautiful mathematics.

Recall from earlier the duality between W(q) and Q($4,q$) (Theorem 1.12), and the duality between Q($5,q$) and H($3,q^2$) (Theorem 1.13). Both of these pairs of dual structures will be very important in the following chapters.

The GQ H($4,q^2$) will not play a role in this thesis.

2.2.2 The constructions of Tits Some of the first examples of nonclassical GQs were given by Tits (and first appeared in Dembowski (1968)), presumably generalising the classical examples arising from quadrics.

Observe that by fixing a point P of a GQ, we can partition both the set of points other than P and the set of lines into subsets determined by their incidence relationship with P. That is, the points other than P are either collinear or noncollinear with P, and the lines are either incident or nonincident with P. This can be represented by the following diagram :

P	lines on P	points collinear with P	lines not on P	points not collinear with P
$\bullet$	$\odot$	$\odot$	$\odot$	$\odot$

1. $\mathbf{T}_2(\mathcal{O})$ - generalising $\mathbf{Q}(4,q)$

Let P be a point of $\mathrm{Q}(4,q)$. Project from P onto a hyperplane $\mathrm{PG}(3,q)$ not on P. Then $P^{\perp}\cap$ $\mathrm{PG}(3,q)$ is a plane π. The lines through P project a conic $\mathcal{C}$ of π. Every line through P not in $P^{\perp}$ is secant to the parabolic quadric $\mathcal{Q}$ defining $\mathrm{Q}(4,q)$, so the points not collinear with P project the whole of $\mathrm{PG}(3,q)\backslash\pi$. The lines not on P project to lines l of $\mathrm{PG}(3,q)$ with $l\cap\pi$ a point of $\mathcal{C}$. The points collinear with P are in one-to-one correspondence with their tangent spaces, which project to planes π' meeting π in a tangent line to $\mathcal{C}$.

This motivates the following construction, as a conic is an oval.

Let $\mathcal{O}$ be an oval of $\mathrm{PG}(2,q)$. Embed $\mathrm{PG}(2,q)$ as a plane π of $\mathrm{PG}(3,q)$. Define the incidence structure $\mathrm{T}_2(\mathcal{O})$ by :

(∞)	lines on (∞)	points collinear with (∞)	lines not on (∞)	points not collinear with (∞)
$\bullet$	$\odot$	$\odot$	$\odot$	$\odot$
(∞)	points of $\mathcal{O}$	planes meeting π in a tangent line to $\mathcal{O}$	lines meeting π in a point of $\mathcal{O}$	points not on π

with (∞) on all points of $\mathcal{O}$, and all other incidences inherited from $\mathrm{PG}(3,q)$.

Theorem 2.4 (Tits (unpublished, first appeared in Dembowski (1968))). *$T_2(\mathcal{O})$ is a GQ of order q. $T_2(\mathcal{O})\cong Q(4,q)\Leftrightarrow\mathcal{O}$ is a conic.*

2. $\mathbf{T}_3(\Omega)$ - generalising $\mathbf{Q}(5,q)$

If we repeat our analysis of $\mathrm{Q}(4,q)$ working out from a point with $\mathrm{Q}(5,q)$, since a tangent hyperplane to an elliptic quadric in $\mathrm{PG}(5,q)$ meets the quadric in a cone projecting an elliptic quadric of $\mathrm{PG}(3,q)$, and an elliptic quadric is an ovoid, we are led to the following :

Let Ω be an ovoid of $\mathrm{PG}(3,q)$. Embed $\mathrm{PG}(3,q)$ as a hyperplane Σ of $\mathrm{PG}(4,q)$. Define an incidence structure $\mathrm{T}_3(\Omega)$ with special point (∞), lines on (∞) being points of Ω, points collinear with (∞) being hyperplanes of $\mathrm{PG}(4,q)$ meeting Σ in a tangent plane to Ω, lines not on (∞) being lines of $\mathrm{PG}(4,q)$ meeting Σ in a point of Ω, and points not collinear with (∞) being points of $\mathrm{PG}(4,q)$ not on Σ.

(∞)	lines on (∞)	points collinear with (∞)	lines not on (∞)	points not collinear with (∞)
$\bullet$	$\odot$	$\odot$	$\odot$	$\odot$
(∞)	points of Ω	hyperplanes meeting Σ in a tangent plane to Ω	lines meeting Σ in a point of Ω	points not on Σ

Theorem 2.5 (Tits (unpublished, first appeared in Dembowski (1968))). *$T_3(\Omega)$ is a GQ of order (q,q^2). $T_3(\Omega)$ is isomorphic to $Q(5,q) \Leftrightarrow \Omega$ is an elliptic quadric.*

2.2.3 Elation generalised quadrangles A **collineation** of a generalised quadrangle is a permutation of the points which maps lines onto lines. A collineation fixing every line incident with some point P is called a **whorl about** P. A whorl about P, which is either the identity collineation or which fixes no point not collinear with P, is called an **elation about** P. Motivated by the study of translation planes, we consider those GQ for which there exists a set of elations about some point P which forms a group acting transitively on the set of points not collinear with P.

A generalised quadrangle $\mathbf{X}$ is called an **elation generalised quadrangle** (EGQ) if for some point P of $\mathbf{X}$ there is a subgroup G of the automorphism group $\mathrm{Aut}\mathbf{X}$ of $\mathbf{X}$ which fixes each line on P and acts regularly on the set of points not collinear with P. The group G is called the **elation group**, and P the **base point**.

Example ($\mathrm{T}_2(\mathcal{O})$ is an EGQ)
The set G of all elations of $\mathrm{PG}(3,q)$ with axis the plane π is a group which acts regularly on the set of all points of $\mathrm{PG}(3,q)$ not on π. G also fixes every point of $\mathcal{O}$, and acts naturally on the set of planes meeting π in a tangent line to $\mathcal{O}$, and on the set of lines meeting π in a point of $\mathcal{O}$. By defining $(\infty)g = (\infty)\ \forall g \in G$, we identify G with a subgroup of $\mathrm{Aut}\mathrm{T}_2(\mathcal{O})$ which fixes (∞), every line of $\mathrm{T}_2(\mathcal{O})$ on (∞) and acts regularly on the set of points of $\mathrm{T}_2(\mathcal{O})$ not collinear with (∞).

We saw earlier that given a particular system of subgroups of an abstract group T, namely a congruence partition of T, it is possible to define an incidence structure in terms of cosets of these subgroups which is a translation affine plane, having T as its full translation group. A similar approach via a group coset geometry also exists for EGQs.

Given an EGQ $\mathbf{X}$ of order (s,t) with an elation group G and base point P, fix a point Q, not collinear with P. Then for every point R not collinear with P, there is a unique element g of G with $Qg = R$, since G acts regularly on the set of points not collinear with P. Identifying R with g, we see that the points not collinear with P can be identified with the elements of G (with Q being the identity of G). As there are s^2t points not collinear with P, G must have size s^2t.

Now consider a point P' collinear with P. There is a unique line l on P and P' and $\forall g \in G\ lg = l$. Let P'' be a point of l with $P \neq P''$. There exist points Q' and Q'', not collinear with P, with Q' collinear with P' and Q'' collinear with P''. So there exists $g \in G$ with $Q'g = Q''$. Since $lg = l$, and P' is the unique point on l collinear with Q', and P'' is the unique point on l collinear with Q'', it follows that $P'g = P''$. So G acts transitively on the set of points on l, other than P. There are s of these points, so, by the orbit-stabiliser theorem, the stabiliser $G_{P'}$ of P' in G has order st. The points on l, other than P, can then be identified with the cosets $G_{P'}g$ of $G_{P'}$ in G $(g \in G)$. So to reconstruct in G all of the points collinear with P, we will need one point P_i' on each of the $t+1$ lines l_i on P, giving rise to $t+1$ subgroups $S_0^*, \ldots, S_t^*$ of G, each of order st. Now the points collinear with P can be identified with the cosets S_i^*g, $g \in G$, $i \in \{0, \ldots, t\}$. We choose P_i' to be the point on l_i collinear with Q.

Now consider a line l' not on P. There is a unique line l and a unique point P' with P incident with l incident with P' incident with l'. Consider another line l'' not on P, but concurrent with l. Then there are points Q', Q'' not collinear with P with Q' on l' and Q'' on l''. So there exists $g \in G$ with $Q'g = Q''$. Since l is on P, $lg = l$, and so $l'g = l''$, as l' is the unique line on Q' concurrent with l and l'' is the unique line on Q'' concurrent with l. So G acts transitively on the set of lines concurrent with l, but not on P. There are st of these lines, so, by the orbit-stabiliser theorem, the stabiliser $G_{l'}$ of l' in G has order s. The lines concurrent with l, but not on P, can then be identified with the cosets $G_{l'}g$ of $G_{l'}$ in G $(g \in G)$. So to reconstruct in G all of the lines not on P, we will need one line l_i' concurrent with each of the $t+1$ lines l_i on P, giving rise to $t+1$ subgroups $S_0, \ldots, S_t$ of G, each of order s. Now the lines not on P can be identified with the cosets $S_i g$, $g \in G$, $i \in \{0, \ldots, t\}$. We choose l'_i incident with P'_i, so that the stabiliser S_i of l'_i fixes P'_i, that is, $S_i \leq S^*_i$, for all $i \in \{0, \ldots, t\}$. We also choose l'_i to be incident with Q.

Now we have a group G of order $s^2 t$ with $t+1$ subgroups $S_0, \ldots, S_t$ of order s and $t+1$ subgroups $S^*_0, \ldots, S^*_t$ of order st such that $S_i \leq S^*_i$. Let $\mathcal{J} = \{S_0, \ldots, S_t\}$ and $\mathcal{J}^* = \{S^*_0, \ldots, S^*_t\}$.

We define the incidence structure $\mathcal{S}(G, \mathcal{J}, \mathcal{J}^*)$ as follows :

Points : (iii) a symbol (∞)
(ii) cosets $S^*_i g$ $(g \in G, i \in \{0, \ldots, t\})$
(i) elements of G

Lines : (b) symbols $[S_i]$, $i \in \{0, \ldots, t\})$
(a) cosets $S_i g$ $(g \in G, i \in \{0, \ldots, t\})$

The point (∞) is incident with all lines $[S_i]$ of type (b). A line $[S_i]$ of type (b) is incident with (∞) and with all points $S^*_i g$ of type (ii) with the same i. A point $S^*_i g$ of type (ii) is incident with the line $[S_i]$ of type (b) with the same i and with each line $S_i h$ of type (a) with the same i such that $S_i h \subseteq S^*_i g$. A line $S_i h$ of type (a) is incident with the point $S^*_i g$ of type (ii) with the same i such that $S_i h \subseteq S^*_i g$ and with each point $g' \in G$ of type (i) such that $g' \in S_i h$. A point g of type (i) is incident with each line $S_i g$ of type (a).

Note that we use the same labelling of the points and lines of $\mathcal{S}(G, \mathcal{J}, \mathcal{J}^*)$ which has become standard, but reverse the order of presentation to emphasise that we have constructed $\mathcal{S}(G, \mathcal{J}, \mathcal{J}^*)$ by working out from a point in the incidence graph of $\mathcal{S}(G, \mathcal{J}, \mathcal{J}^*)$.

If $\mathbf{X}$ is an EGQ of order (s, t) with elation group G and base point P, $l_0, \ldots, l_t$ are lines of $\mathbf{X}$ on P, P'_i is a point on l_i $(\neq P)$ for $i \in \{0, \ldots, t\}$, l'_i is a line on P'_i $(\neq l_i)$ for $i \in \{0, \ldots, t\}$, $S_i = G_{l'_i}$, $S^*_i = G_{P'_i}$, $\mathcal{J} = \{S_0, \ldots, S_t\}$ and $\mathcal{J}^* = \{S^*_0, \ldots, S^*_t\}$, then $\mathbf{X}$ is isomorphic to $\mathcal{S}(G, \mathcal{J}, \mathcal{J}^*)$.

However, if we don't construct subgroups of G in this way from a known GQ, what conditions on $\mathcal{J}$ and $\mathcal{J}^*$ are necessary for $\mathcal{S}(G, \mathcal{J}, \mathcal{J}^*)$ to be a GQ ? The following example illustrates the answer.

Example ($\mathrm{T}_2(\mathcal{O})$ as a group coset geometry)
The elation group G of $\mathrm{T}_2(\mathcal{O})$ can be naturally identified with the vector space $GF(q)^3$, considered as an additive group. We can also think of this as $\mathrm{AG}(3, q)$.

The plane at infinity of $\mathrm{AG}(3,q)$ is identified with the plane π. We identify Q with the origin $O(0,0,0)$ (i.e., with the identity of G). Now lines of $\mathrm{AG}(3,q)$ through Q correspond to 1-dimensional subspaces of $GF(q)^3$, and so to points of π. Thus $l'_0,\ldots,l'_q$, the lines through Q, correspond to $S_0,\ldots,S_q$, each of which is a point of π. Also, $l'_i \cap \pi$ is a point of $\mathcal{O}$. So $\mathcal{J}$ is $\mathcal{O}$. Now planes of $\mathrm{AG}(3,q)$ through Q correspond to 2-dimensional subspaces of $GF(q)^3$, and so to lines of π. Thus $P'_0,\ldots,P'_q$, the points collinear with Q and collinear with (∞), correspond to $S^*_0,\ldots,S^*_q$, each of which is a line of π. Also, these planes of $\mathrm{PG}(3,q)$ meet π in a tangent line to $\mathcal{O}$. So $\mathcal{J}^*$ is $\mathcal{O}^*$, the set of all tangent lines to $\mathcal{O}$.

Now no three points of $\mathcal{O}$ are collinear, so $PQ \cap R = \{0\}$ for distinct P,Q,R in $\mathcal{O}$. Thus

$$\text{(K1)} \quad S_iS_j \cap S_k = 1$$

for distinct i,j,k, where $S_iS_j = \{gh | g \in S_i, h \in S_j\}$.

Also, no point P of $\mathcal{O}$ lies on a tangent line to another point Q of $\mathcal{O}$, i.e., $\forall P_i \in \mathcal{O}$ $\forall l_j \in \mathcal{O}^*$ $i \neq j \Rightarrow P_i \cap l_j = \{0\}$, giving

$$\text{(K2)} \quad S_i \cap S^*_j = \{1\}$$

for distinct i,j.

A system $\mathcal{J}$, $\mathcal{J}^*$ of subgroups is called a **Kantor (4-gonal) family** if it satisfies the conditions (K1) and (K2). This construction of EGQs is originally due to Kantor (1980).

Theorem 2.6 (Kantor (1980)). *$\mathcal{S}(G,\mathcal{J},\mathcal{J}^*)$ is a GQ if and only if $\mathcal{J}$, $\mathcal{J}^*$ is a 4-gonal family. In this case, $\mathcal{S}(G,\mathcal{J},\mathcal{J}^*)$ is an EGQ of order (s,t) with elation group G and base point (∞).*

We remark that there exist examples of generalised quadrangles which do not occur in any of the models we have thus far considered. These examples, due first to Ahrens and Szekeres (1969) for all prime powers q and independently to Hall Jr. (1971) for q even, but later included in a more general construction by Payne (1971), are of order $(q-1,q+1)$. They are the only known examples, with $s>1$ and $t>1$, in which s and t are not powers of the same prime.

Flocks of circle planes

We will now focus on quadrics of $\mathrm{PG}(3,q)$, in particular, on elliptic quadrics, hyperbolic quadrics, and quadratic cones. These three families of quadrics are examples of certain incidence structures known as circle planes, namely inversive (or Möbius) planes, Minkowski planes and Laguerre planes, respectively. Indeed, each of these classes of circle planes, or Benz planes as they are also known, is a generalisation of the model of the plane sections of the quadric which are conics. The three families of quadrics are known as the Miquelian circle planes, in that they satisfy the theorem of Miquel, an incidence theoretic result somewhat analogous to the theorem of Pappus in projective planes. The generalised concepts of ovoid and oval cone in $\mathrm{PG}(3,q)$ also give rise to circle planes, modelling the plane sections which are ovals, and these examples are not Miquelian (unless, of course, the ovoid is an elliptic quadric or the oval cone is a quadratic cone).

The general theory of circle planes is very beautiful, however we do not have the time to delve into it here. Instead, we have mentioned this wider setting in order to introduce historically the main problem of this thesis. Circle planes are incidence structures arising from a set of points, a set of subsets of points called circles, and either 0,2 or 1 sets of equivalence classes of points called lines, for inversive, Minkowski or Laguerre planes respectively. For an inversive plane $\mathbf{I}$, Dembowski (1968) introduced the concept of a *flock* as a set $\mathcal{F}$ of mutually disjoint circles such that, with the exception of precisely two points, every point of $\mathbf{I}$ is on a (necessarily unique) circle of $\mathcal{F}$. In other words, a flock of $\mathbf{I}$ is a partition of all but two points of $\mathbf{I}$ into pairwise disjoint circles. This concept naturally extends to the other circle planes, and has generated a great deal of interest in many parts of geometry.

This thesis is concerned with the problem of flocks of the Miquelian circle planes, i.e., with flocks of elliptic quadrics, hyperbolic quadrics, and quadratic cones of $\mathrm{PG}(3,q)$. We discuss these separately here.

For the case of elliptic quadrics, we may discuss the more general situation of flocks of ovoids of $\mathrm{PG}(3,q)$. A **flock** of an ovoid of $\mathrm{PG}(3,q)$ is a partition of all but two points of the ovoid into pairwise disjoint ovals, and we speak of the planes of a flock as the set of planes containing the ovals. Then two planes of a flock must meet in a line external to the ovoid. If all planes of a flock meet in the same external line, we call the flock **linear**.

Theorem 3.1 (Orr (1973) (q odd), Thas (1973) (q even)). *Any flock of an ovoid of $PG(3,q)$ is linear.*

A **flock** of a hyperbolic quadric of $\mathrm{PG}(3,q)$ is a partition of the points of the quadric into pairwise disjoint conics. Again, we speak of the planes of a flock as the set of planes containing the conics. Two planes of a flock must meet in an external line, and if all planes of a flock meet in the same external line, we call the flock **linear**.

Theorem 3.2 (Thas (1975)). *Any flock of a hyperbolic quadric of $PG(3,q)$, q even, is linear.*

For hyperbolic quadrics over fields of odd order, there exist examples of flocks which are not linear.

Example (The Thas flocks [Thas (1975)]) Let q be odd, V be $GF(q)^4$ and $Q : V \to GF(q)$ be a nondegenerate quadratic form of plus type, so that $\mathcal{Q}^+ = \{\langle v\rangle : Q(v) = 0\}$ is a hyperbolic quadric of $\mathcal{P}V = \mathrm{PG}(3,q)$. Let l be an external line to $\mathcal{Q}^+$ and m be the polar line to l, so that $m = l^\perp = \{v \in V | f(v,u) = 0 \ \forall u \in l\}$ where $f(x,y) = Q(x+y) - Q(x) - Q(y)$ is the polar form of Q. Let

$$\mathcal{F} = \{\langle v\rangle^\perp | v \in l \text{ and } Q(v)\square = \square \text{ or } v \in m \text{ and } Q(v)\square = -\boxtimes\}.$$

Then $\mathcal{F}$ is a flock of $\mathcal{Q}$, which is called a **Thas flock**. (This follows from the fact that the discriminant of Q restricted to $\langle u,v\rangle$ for $\langle u\rangle^\perp, \langle v\rangle^\perp \in \mathcal{F}$ is $-\boxtimes$.)

Example (The exceptional flocks [Baker and Ebert (1987) (orders 11,23), Bader (1988), Bonisoli (1988), Johnson (1989), see also Durante (1992)]) There are 3 exceptional flocks of the hyperbolic quadric of $\mathrm{PG}(3,q)$, one each for $q = 11, 23$ and 59 associated with the irregular nearfields of Dickson (1905) of orders $11^2, 23^2$ and 59^2.

Theorem 3.3 (Bader and Lunardon (1989), Thas (1991)). *Any flock of a hyperbolic quadric of $PG(3,q)$, q odd, is linear, Thas or exceptional.*

A different approach to these hyperbolic flocks has been given by Bader, Durante, Lunardon, Penttila and the present author ([7]), where they are shown to be the smallest member in each of three infinite families of partial flocks of sizes 12,24 and 60 of the hyperbolic quadric of $\mathrm{PG}(3,q)$, for $q \equiv -1$ modulo 12, 24, 60 respectively, by the use of root systems of the Euclidean space $\mathbb{R}^4$.

Thus the problem of flocks of nondegenerate quadrics of $\mathrm{PG}(3,q)$ is completely solved. But in the wider setting of circle planes, we also have the problem of flocks of Miquelian Laguerre planes, i.e., flocks of quadratic cones of $\mathrm{PG}(3,q)$. There exists a number of different examples of flocks of quadratic cones, and although much of the general theory holds for all q, the situation is somewhat different for q odd and for q even. The problem of classification of these flocks is still very much open for both cases, and one of the aims of this thesis is to contribute towards the case of q odd by constructing new examples. We mention here that the problem of flocks of circle planes arising from oval cones for q even is also still open. When the oval is a translation oval, see Cherowitzo (1998) for the study of these so called α-flocks. Flocks of other oval cones are yet to be considered.

3.1 Flocks of quadratic cones

A **flock** of a quadratic cone $\mathcal{K}$ of $\mathrm{PG}(3,q)$ is a partition of the points of $\mathcal{K}$ minus the vertex V into pairwise disjoint conics. We may talk of the conics of the flock, as well as the planes of the flock, namely, those planes of $\mathrm{PG}(3,q)$ containing the conics of the flock. There are necessarily q conics (planes) of the flock. As the conics of a flock are pairwise disjoint, the planes of the flock necessarily meet pairwise in lines exterior to the cone. If all planes of a flock meet in the same external line, then this flock is called **linear**.

Suppose two flocks $\mathcal{F} = \{\mathcal{C}_1, \ldots, \mathcal{C}_q\}$ and $\mathcal{F}' = \{\mathcal{C}'_1, \ldots, \mathcal{C}'_q\}$ of the quadratic cone $\mathcal{K}$ have $s > \frac{q-1}{2}$ conics in common. Without loss of generality, say $\mathcal{C}_i = \mathcal{C}'_i$ for $i = 1, \ldots, s$. If $s < q$, then there exists a conic $\mathcal{C}'_j$ of $\mathcal{F}'$ such that $\mathcal{C}'_j \notin \mathcal{F}$. Let π'_j be the plane of $\mathcal{C}'_j$ and π_i be the plane of $\mathcal{C}_i$ for $i = s+1, \ldots, q$. Now π'_j meets π_i in a line, and so $\mathcal{C}'_j$ meets $\mathcal{C}_i$ in at most two points, for $i = s+1, \ldots, q$. Since the conics of $\mathcal{F}$ are pairwise disjoint, the size of $\mathcal{C}'_j$ can be at most $2(q-s)$, that is, $q+1 \leq 2(q-s)$, whence $s \leq \frac{q-1}{2}$, a contradiction. Thus $s = q$, and we see that if two flocks share more than $\frac{q-1}{2}$ conics, they are equal (Thas (1987)).

In Fisher and Thas (1979) there is presented an example of a flock of a quadratic cone for all odd q due to Fisher. The geometric construction is very detailed, so we choose to delay presentation of this example until later. Instead we mention only that the example of Fisher has the property that *exactly* $\frac{q-1}{2}$ planes of the flock meet in a common line, and that Payne and Thas (1991) [99] have characterised this example as the unique nonlinear flock with this property. (Furthermore, the remaining $\frac{q+1}{2}$ planes meet in a common point, which is not on the common line of the first $\frac{q-1}{2}$ planes.)

We have seen earlier that all quadratic cones of PG$(3,q)$ are equivalent under the action of $P\Gamma L(4,q)$. Thus we define the quadratic cone $\mathcal{K}$ having equation

$$x_1^2 = x_0x_2,$$

so that $\mathcal{K} = \{(x_0,x_1,x_2,x_3)|x_1^2 = x_0x_2\}$. The vertex of $\mathcal{K}$ is the point $V(0,0,0,1)$.

Any plane of a flock $\mathcal{F}$ of $\mathcal{K}$ will have an equation of the form $ax_0+bx_1+cx_2+x_3 = 0$, and we denote these planes by $[a,b,c,1]^T$, so that

$$\mathcal{F} = \{[a_t,b_t,c_t,1]^T : t \in GF(q)\}.$$

If we project from V onto the plane $\pi : x_3 = 0$, then $\mathcal{K}$ projects the conic $\mathcal{C} : x_1^2 = x_0x_2$ in π. The intersection of the planes $[a_s,b_s,c_s,1]^T$ and $[a_t,b_t,c_t,1]^T$ for $s \neq t$ projects onto the line $[a_s-a_t, b_s-b_t, c_s-c_t]^T$ of π, which must be external to $\mathcal{C}$.

Thus for $\mathcal{F}$ to be a flock of $\mathcal{K}$, the following two equations must have no nontrivial solution (x_0,x_1,x_2) :

$$(a_s-a_t)x_0 + (b_s-b_t)x_1 + (c_s-c_t)x_2 = 0$$

$$x_1^2 = x_0x_2.$$

By making the appropriate substitutions, the following equation must have no non-trivial solution X :

$$(a_s-a_t)^2X^2 + [2(a_s-a_t)(c_s-c_t) - (b_s-b_t)^2]X + (c_s-c_t)^2 = 0.$$

Using the quadratic formula when q is odd and using the absolute trace equation when q is even, we arrive at the following important theorem.

Theorem 3.4 (Thas (1987)).

$$\mathcal{F} = \{[a_t,b_t,c_t,1]^T : t \in GF(q)\} \text{ is a flock of } \mathcal{K}$$

$$\iff \begin{cases} (b_s-b_t)^2 - 4(a_s-a_t)(c_s-c_t) = \boxtimes & \forall s \neq t \ (q \ odd) \\ b_s \neq b_t \ and \ trace\left(\frac{(a_s+a_t)(c_s+c_t)}{(b_s+b_t)^2}\right) = 1 & \forall s \neq t \ (q \ even) \end{cases}$$

The following example of an infinite family of flocks of the quadratic cone was first given by Walker (1976) in the context of translation planes and then by Fisher and Thas (1979) explicitly as flocks.

Example (The Fisher-Thas/Walker flocks [Walker (1976), Fisher and Thas (1979)]) With notation as above, let $\mathcal{F} = \{[t, 3t^2, 3t^3, 1]^T : t \in GF(q)\}$ be a set of q planes of PG$(3, q)$. Then $\mathcal{F}$ is a flock of the quadratic cone $\mathcal{K}$ if and only if $q \equiv -1 \pmod 3$. We prove this using the above theorem.

For q odd,

$$\begin{aligned} & (b_s - b_t)^2 - 4(a_s - a_t)(c_s - c_t) \\ = \; & (3s^2 - 3t^2)^2 - 4(s - t)(3s^3 - 3t^3) \\ = \; & 9(s - t)^2(s + t)^2 - 12(s - t)^2(s^2 + st + t^2) \\ = \; & (s - t)^2(-3s^2 + 6st - 3t^2) \\ = \; & -3(s - t)^4 \end{aligned}$$

Now $GF(q)$ has a primitive cube root of unity if and only if $3|q-1$, so $q \equiv -1 \pmod 3$ if and only if there is no cube root of unity in $GF(q)$, if and only if $x^2 + x + 1$ is irreducible over $GF(q)$, if and only if $\Delta = 1 - 4 = -3$ is a non-square in $GF(q)$. Hence $(b_s - b_t)^2 - 4(a_s - a_t)(c_s - c_t)$ is a nonsquare for $s \neq t$ if and only if $q \equiv -1 \pmod 3$.

For q even,

$$\begin{aligned} & \mathrm{trace}\left(\tfrac{(a_s+a_t)(c_s+c_t)}{(b_s+b_t)^2}\right) \\ = \; & \mathrm{trace}\left(\tfrac{(s+t)(s^3+t^3)}{(s^2+t^2)^2}\right) \\ = \; & \mathrm{trace}\left(1 + \tfrac{s^3t+st^3}{s^4+t^4}\right) \\ = \; & \mathrm{trace}\left(1 + \tfrac{(st+s^2)}{(s^2+t^2)} + \left(\tfrac{st+s^2}{s^2+t^2}\right)^2\right) \end{aligned}$$

Now $\mathrm{trace}(x + x^2) = 0$ for all $x \in GF(q), q = 2^h$, and $\mathrm{trace}(1) = 1$ if and only if h is odd, if and only if $q \equiv -1 \pmod 3$. Note that $s^2 + t^2 \neq 0$ for $s \neq t$ as $x \mapsto x^2$ is one-to-one.

This flock is linear if and only if $q = 2$.

For the rest of this thesis we will only be concerned with flocks of the quadratic cone, and so we may often call them simply flocks, and drop the reference to the quadratic cone. A central aim of this thesis is to discover new examples of flocks of the quadratic cone. Thus we need to know just what 'new' means, that is, we must have a concept of equivalence of flocks. Being partitions of the quadratic cone of PG$(3, q)$, flocks are substructures of PG$(3, q)$, and so naturally we consider equivalence under $P\Gamma L(4, q)$. Thus two flocks $\mathcal{F}_1$ and $\mathcal{F}_2$ of the quadratic cone $\mathcal{K}$ of PG$(3, q)$ are **isomorphic** if and only if there exists an element of $P\Gamma L(4, q)$ which fixes $\mathcal{K}$ and maps $\mathcal{F}_1$ onto $\mathcal{F}_2$. We will discuss the question of isomorphism in more detail later.

Associated geometries

The study of flocks of the quadratic cone in PG$(3, q)$ is a fascinatingly rich area of research. One of the most appealing aspects is the wide diversity of geometric structures connected with flocks. In this chapter we investigate some of these connections. For recent surveys of this wide area see Payne's survey [96] in [42] and Johnson and Payne (1997).

4.1 Translation planes arising from linespreads

We saw earlier that translation planes of order q^{t+1} are intimately connected with t-spreads of PG$(2t+1, q)$. In the following sections we will be interested in the case $t = 1$, so we now present this result in the geometric manner of Bruck and Bose (1964).

A 1-spread of PG$(3, q)$ is a partition of the points into lines, and so is referred to as a **linespread**. Equivalently, it is a set of $q^2 + 1$ lines, no 2 intersecting. From now on we will only be concerned with linespreads of PG$(3, q)$, and we may refer to them simply as **spreads**.

Embed PG$(3, q)$ as a hyperplane of PG$(4, q)$, and let $\mathcal{S}$ be a linespread of PG$(3, q)$. Define an incidence structure $\mathcal{A}(\mathcal{S})$ with **points** the points of PG$(4, q)$ not in PG$(3, q)$, **lines** the planes of PG$(4, q)$ meeting PG$(3, q)$ only in a line of $\mathcal{S}$, and with **incidence** inherited from PG$(4, q)$.

Theorem 4.1 (Bruck and Bose (1964)). *$\mathcal{A}(\mathcal{S})$ is a translation affine plane of order q^2.*

Each line l of $\mathcal{S}$ corresponds to a class of parallel lines of $\mathcal{A}(\mathcal{S})$, so adjoining each such line of $\mathcal{S}$ to $\mathcal{A}(\mathcal{S})$ as a 'point at infinity', and adjoining $\mathcal{S}$ to $\mathcal{A}(\mathcal{S})$ as a 'line at infinity' defines a projective plane $\mathcal{P}(\mathcal{S})$, which is a translation plane of order q^2.

Let $\mathcal{S}$ be a linespread of PG$(3, q)$. If, for any three distinct lines l_1, l_2, l_3 of $\mathcal{S}$, all lines of the unique regulus through l_1, l_2, l_3 are contained in $\mathcal{S}$, then $\mathcal{S}$ is called a **regular** linespread. For $q = 2$, the regulus through any three lines contains only the three lines, that is, every linespread of PG$(3, 2)$ is regular.

Theorem 4.2 (Bruck and Bose (1966)). *With respect to the André/Bruck-Bose constructions, a linespread of PG$(3, q)$ is regular if and only if the corresponding translation plane is Desarguesian.*

We say two linespreads $\mathcal{S}_1$ and $\mathcal{S}_2$ of PG$(3,q)$ are **isomorphic** if and only if there exists an element of $P\Gamma L(4,q)$ which maps $\mathcal{S}_1$ onto $\mathcal{S}_2$ linewise; and so, with respect to the André/Bruck-Bose constructions, two linespreads of PG$(3,q)$ are isomorphic if and only if the corresponding translation planes are isomorphic.

We remark however that not all translation planes of order q^2 arise from linespreads of PG$(3,q)$, if q is not prime. Consider the case for translation planes of order $16 = 4^2 = 2^4$. These can arise from linespreads of PG$(3,4)$ $(t=1)$, but also from solidspreads of PG$(7,2)$ $(t=3)$. We wish to consider only the case of translation planes arising from linespreads of PG$(3,q)$. In the finite case, the kernel of a translation plane is a field, and so if the largest subfield of the kernel is $GF(q)$, the kernel itself will be $GF(q)$. Thus if we stipulate that the largest subfield of the kernel is $GF(q)$, the translation plane arising from a linespread of PG$(3,q)$ is of order q^2 with kernel $GF(q)$, in other words, it is of dimension 2 over its kernel. These are precisely the translation planes we will consider in this thesis. Note that the translation planes arising from solidspreads of PG$(7,2)$ would then be of order 16, but of dimension 4 over their kernel.

Let $F = GF(q)$, where $q > 3$ and $q = p^h$ for some prime $p \neq 3$. A function $L : F \to F$ is **likeable** if it satisfies the following conditions :

(i) $L(x+y) = L(x) + L(y)$ for all $x, y \in F$ (i.e., L is additive); and

(ii) if $y^2 = x^2 y - \frac{1}{3}x^4 + xL(x)$ then $x = y = 0$.

This concept and the following ideas were introduced by Kantor (1982) [68]. Consider $f(x,y) = xy - \frac{1}{3}x^3 + L(x)$, where L is a likeable function on $GF(q)$. Then

$$G(L) = \left\{ M(x,y) = \begin{pmatrix} 1 & x & y & f(x,y) \\ 0 & 1 & x & y \\ 0 & 0 & 1 & x \\ 0 & 0 & 0 & 1 \end{pmatrix} : x, y \in GF(q) \right\}$$

is an abelian group of order q^2. Define the following set of q^2+1 lines of PG$(3,q)$:

$$\mathcal{S}(L) = \left\{ l_M = \langle (x_0, x_1, 0, 0)M \rangle : M \in G(L) \right\} \cup \left\{ l_\infty = \langle (0,0,x_2,x_3) \rangle \right\}.$$

Clearly l_∞ does not intersect any other line of $\mathcal{S}(L)$, and since $G(L)$ is abelian, to check if two distinct lines l_M, l_N of $\mathcal{S}(L) \backslash l_\infty$ are skew, we can take $M = M(0,0)$, the identity element of $G(L)$, and $N = N(t,u)$ where at least one of t,u is nonzero. Then we must have that the following two equations :

$$x_0u + x_1t = 0 \qquad x_0f(t,u) + x_1u = 0$$

have only the trivial solution $x_0 = x_1 = 0$, and hence that $u^2 - tf(t,u) \neq 0$. But this follows directly from the definition of a likeable function, and so $\mathcal{S}(L)$ is a linespread of PG$(3,q)$. In fact, $\mathcal{S}(L)$ contains the q reguli $\mathcal{R}_x = \{\langle(x_0,x_1,0,0)M(x,y)\rangle : y \in F\} \cup \{\langle(0,0,x_2,x_3)\rangle\}$, that is, contains q reguli sharing a common line. The **likeable translation plane** arising from $\mathcal{S}(L)$ via the André/Bruck-Bose constructions is non-Desarguesian.

Now set $a = x$ and $z = y/a^2$ in the definition of likeability. Then we have the following lemma determining whether a given additive function is likeable.

Lemma 4.1 (Kantor (1982) [68]). *An additive function $L : F \to F$ is likeable if and only if the equation*

$$z^2 - z + \frac{1}{3} - \frac{L(a)}{a^3} = 0$$

has no solution for $z \in F$ and $a \in F\backslash\{0\}$. In particular, if q is odd then L is likeable if and only if $L(a)/a^3 - 1/12$ is a nonsquare for all $a \in F\backslash\{0\}$.

Example (The Kantor likeable translation planes) [Kantor (1982) [68]] Let $q = 5^h$, $h > 1$ and fix a nonsquare n of $GF(q)$. Define the following additive map from $GF(q)$ to $GF(q)$:

$$L(t) = nt^5 + n^{-1}t.$$

Then

$$\begin{aligned} & \tfrac{L(a)}{a^3} - \tfrac{1}{12} \\ = \;& na^2 + \tfrac{1}{na^2} - \tfrac{1}{2} \\ = \;& \tfrac{2n^2a^4+2-na^2}{2na^2} \\ = \;& \tfrac{n^2a^4+2na^2+1}{na^2} \\ = \;& \tfrac{(na^2+1)^2}{na^2} \end{aligned}$$

and since -1 is a square, $a^2 \neq -n^{-1}$. Hence L is a likeable function and will define a linespread of PG$(3,q)$ as above. The non-Desarguesian translation planes arising from L are called the Kantor likeable translation planes.

We may represent linespreads of PG$(3,q)$ algebraically as follows. Let M be an arbitrary 4×2 matrix over $GF(q)$ of column rank 2. Then the column space $\langle M \rangle$ of

M defines a line l_M of PG$(3,q)$. Let l_M, l_N be two such lines of PG$(3,q)$. Then l_M and l_N are skew if and only if together they span all of PG$(3,q)$, that is, if and only if the 4×4 matrix (M,N) has column rank 4. Let I be the 2×2 identity matrix over $GF(q)$, and let A, B be arbitrary 2×2 matrices over $GF(q)$. Then the lines $l_A = \langle \begin{pmatrix} I \\ A \end{pmatrix} \rangle$, $l_B = \langle \begin{pmatrix} I \\ B \end{pmatrix} \rangle$ are skew if and only if $\det \begin{pmatrix} I & I \\ A & B \end{pmatrix} \neq 0$, if and only if $\det(A-B) \neq 0$.

A **spread set** is a family $\mathbf{S}$ of q^2 2×2 matrices over $GF(q)$ such that $A-B$ is nonsingular, that is, $\det(A-B)\neq 0$, $\forall A \neq B \in \mathbf{S}$. Clearly, given a spread set $\mathbf{S}$, if we let

$$\mathcal{S}(\mathbf{S}) = \big\{\langle \begin{pmatrix} I \\ A \end{pmatrix} \rangle | A \in \mathbf{S}\big\} \cup \big\{ l_\infty = \langle \begin{pmatrix} 0 \\ I \end{pmatrix} \rangle \big\},$$

then $\mathcal{S}(\mathbf{S})$ is a linespread of PG$(3,q)$. Any linespread of PG$(3,q)$ is equivalent to a linespread of the form $\mathcal{S}(\mathbf{S})$, for some spread set $\mathbf{S}$. Furthermore, every spread set $\mathbf{S}$ can be normalised so that

$$\mathbf{S} = \left\{ \begin{pmatrix} g(x,y) & h(x,y) \\ x & y \end{pmatrix} | x, y \in GF(q) \right\}$$

for some functions $g, h : GF(q)^2 \to GF(q)$.

Theorem 4.3 (Hiramine, Matsumoto and Oyama (1987), Johnson (1988)). *Let*

$$\mathbf{S} = \left\{ \begin{pmatrix} g(x,y) & h(x,y) \\ x & y \end{pmatrix} | x, y \in GF(q) \right\}$$

be a spread set of 2×2 *matrices over* $GF(q)$. *For* $\omega \in GF(q)^2 \backslash GF(q)$, *and* $\overline{x} = x^q$ $\forall x \in GF(q^2)$,

$$\left\{ A_{x,y,x',y'} = \begin{pmatrix} x+\omega y & g(x',y') + \overline{\omega} h(x',y') \\ x' + \omega y' & \overline{x} + \overline{\omega y} \end{pmatrix} | x, y, x', y' \in GF(q) \right\}$$

is a spread set over $GF(q^2)$.

This remarkable construction was first given by Hiramine, Matsumoto and Oyama (1987) for characteristic not 2, and then generalised by Johnson (1988). Hence we have the following corollary.

Corollary 4.1. *Every linespread of* $PG(3,q)$ *gives rise to a linespread of* $PG(3,q^2)$.

In fact, different linespreads of $\mathrm{PG}(3,q^2)$ can arise from the same equivalence class of linespreads of $\mathrm{PG}(3,q)$, depending upon both the choice of the spread set $\mathbf{S}$ and the choice of ω. Clearly the process can be iterated, leading to linespreads in $\mathrm{PG}(3,q^4)$, $\mathrm{PG}(3,q^8)$, ..., and so there are no sporadic linespreads of $\mathrm{PG}(3,q)$: each linespread of $\mathrm{PG}(3,q)$ lies in many infinite families of linespreads. (See page 65 for a brief discussion of sporadicity.)

4.1.1 Flocks and translation planes Denote by $\mathcal{Q}^+$ the Klein quadric of $\mathrm{PG}(5,q)$. An **ovoid** of $\mathcal{Q}^+$ is a set of q^2+1 points such that no two of the points are collinear in a line of the quadric. Under the Klein correspondence, such a set of points will correspond to a set of q^2+1 lines of $\mathrm{PG}(3,q)$, no two of which are concurrent; that is, an ovoid of the Klein quadric corresponds to a linespread of $\mathrm{PG}(3,q)$.

Let $\mathcal{F} = \{\pi_1, \dots, \pi_q\}$ be a flock of the quadratic cone $\mathcal{K}$ of $\mathrm{PG}(3,q)$, and embed $\mathcal{K}$ as a section of $\mathcal{Q}^+$ by the solid Σ. Let $\perp$ denote the polarity arising from $\mathcal{Q}^+$. Then $\pi_i^\perp$ is a plane of the same type as π_i, and so intersects $\mathcal{Q}^+$ in a conic $C_i^\perp$. Define Ω to be the union of these conics, so $\Omega = \cup\{C_i^\perp : 1 \le i \le q\}$. The polar line l to Σ is tangent to $\mathcal{Q}^+$ at the vertex V of $\mathcal{K}$, and so each $\pi_i^\perp$ will contain l and hence contain V. Since the planes π_i of $\mathcal{F}$ are distinct, the planes $\pi_i^\perp$ will pairwise intersect exactly in l, and so $|\Omega| = q^2+1$.

Now consider two distinct planes $\pi_i^\perp$ and $\pi_j^\perp$. Then $\pi_i \cap \pi_j$ is a line l_{ij} exterior to $\mathcal{Q}^+$, as π_i, π_j are planes of the flock $\mathcal{F}$, and so l_{ij} is an elliptic subspace $O^-(2,q)$ of the hyperbolic space $O^+(6,q)$ underlying $\mathcal{Q}^+$. Recall that the orthogonal direct sum of two elliptic spaces is hyperbolic ("minus times minus is plus"). Thus we have that $l_{ij}^\perp = \langle \pi_i^\perp, \pi_j^\perp \rangle$ is an elliptic subspace $O^-(4,q)$, and so $\langle \pi_i^\perp, \pi_j^\perp \rangle$ intersects $\mathcal{Q}^+$ in an elliptic quadric. Hence no two points of $\langle \pi_i^\perp, \pi_j^\perp \rangle \cap \mathcal{Q}^+$ are collinear in a line of $\mathcal{Q}^+$, and so no two points of Ω are collinear in a line of $\mathcal{Q}^+$. Thus we have proven the following result due independently to Walker (1976) and Thas (unpublished, c. 1976).

Theorem 4.4 (Walker (1976), Thas). *Ω is an ovoid of the Klein quadric of $PG(5,q)$.*

We will see later exactly which types of linespreads may be constructed in this way from flocks of the quadratic cone. In a similar manner, an ovoid of the Klein quadric may also be constructed from any flock of an elliptic quadric or hyperbolic quadric of $\mathrm{PG}(3,q)$. With respect to the André/Bruck-Bose constructions and the

Thas/Walker construction, two flocks of the quadratic cone are isomorphic if and only if the corresponding translation planes are isomorphic. However, due to the constructions of Hiramine, Matsumoto and Oyama and Johnson, a flock gives rise to many infinite families of translation planes.

If $\mathcal{F}$ is a linear flock, so that all planes of $\mathcal{F}$ intersect in the common line m, it is clear from the above construction that the corresponding ovoid of the Klein quadric will be the elliptic quadric $m^\perp \cap \mathcal{Q}^+$. Under the Klein correspondence, this elliptic quadric corresponds to a regular linespread of $\mathrm{PG}(3,q)$, which we have seen gives rise to a Desarguesian translation plane via the André/Bruck-Bose constructions.

Example (The Kantor/Knuth semifield ovoids) [Kantor (1982) [67], Knuth (1965)] Let $F = GF(q)$, where q is odd and not prime. Fix a nonsquare n of F, and let σ and τ be automorphisms of F, at least one of which is nontrivial. Suppose the Klein quadric $\mathcal{Q}^+$ of $\mathrm{PG}(5,q)$ is defined by the quadratic form $Q : x_0x_5+x_1x_4+x_2x_3$. Define Ω to be the following set of points of $\mathcal{Q}^+$:

$$\Omega = \{\langle(1, a, b, b^\tau, -na^\sigma, -b^{\tau+1} + na^{\sigma+1})\rangle : a, b \in F\} \cup \{\langle(0,0,0,0,0,1)\rangle\}.$$

Clearly, the point $\langle(0,0,0,0,0,1)\rangle$ is not orthogonal to any other points in Ω. Let

$$\langle u\rangle = \langle(1, a, b, b^\tau, -na^\sigma, -b^{\tau+1}+na^{\sigma+1})\rangle \quad \text{and} \quad \langle v\rangle = \langle(1, c, d, d^\tau, -nc^\sigma, -d^{\tau+1}+nc^{\sigma+1})\rangle$$

be two distinct points of $\Omega\backslash\{\langle(0,0,0,0,0,1)\rangle\}$. Then with respect to the polar form f of Q we have :

$$\begin{aligned} f(u,v) &= u_0v_5 + u_5v_0 + u_1v_4 + u_4v_1 + u_2v_3 + u_3v_2 \\ &= -d^{\tau+1} + nc^{\sigma+1} - b^{\tau+1} + na^{\sigma+1} - nac^\sigma - nca^\sigma + bd^\tau + db^\tau \\ &= -(b^\tau - d^\tau)(b-d) + n(a^\sigma - c^\sigma)(a-c) \\ &= -(b-d)^{\tau+1} + n(a-c)^{\sigma+1} \end{aligned}$$

Suppose $\langle u\rangle$ and $\langle v\rangle$ are collinear in a line of $\mathcal{Q}^+$, that is, they are orthogonal. Then $f(u,v) = 0$ and so

$$n = \frac{(b-d)^{\tau+1}}{(a-c)^{\sigma+1}} = \left(\frac{(b-d)^{\frac{\tau+1}{2}}}{(a-c)^{\frac{\sigma+1}{2}}}\right)^2$$

since σ and τ are odd. But n is a nonsquare of F, and hence Ω is a set of q^2+1 pairwise noncollinear points of $\mathcal{Q}^+$, that is, an ovoid of $\mathcal{Q}^+$, given by Kantor (1982) [67]. The translation plane arising from Ω via the Klein correspondence and the André/Bruck-Bose constructions has as its coordinatising ternary field a semifield given by Knuth (1965). If one of σ and τ is the identity automorphism, then Ω

lies within some hyperplane H of PG$(5, q)$, and Ω is then an ovoid of the parabolic quadric $Q(4, q)$ defined by $H \cap \mathcal{Q}^+$. In this case, the associated semifield reduces to a commutative semifield first given by Dickson (1905) (see Dickson (1935)). For $q = 9$, it is equivalent to the commutative semifield of Ganley given in Section 2.1.1.

Now although a flock gives rise to an ovoid of the Klein quadric via the Thas/Walker construction, not every ovoid of the Klein quadric must arise from a flock. In the case that an ovoid of the Klein quadric lies in a hyperplane section of this quadric, so that it is an ovoid of $Q(4, q)$, we call it a **translation ovoid** if the translation plane arising via the Klein correspondence and André/Bruck-Bose constructions is a semifield plane. A flock giving rise to a semifield translation plane via the Thas/Walker construction is called a **semifield flock**, and every translation ovoid of $Q(4, q)$ defines a semifield flock. (See Lunardon (1997) and Thas (1997) [116].) Hence the Kantor/Knuth translation ovoid above gives rise to a semifield flock. Furthermore, the translation plane coordinatised by the Ganley commutative semifield (page 31) also arises from a flock, with the associated translation ovoid first being studied by Thas and Payne (1994).

4.2 Elation generalised quadrangles arising from q-clans

We saw earlier that elation generalised quadrangles of order (s, t), $s > 1, t > 1$, can be constructed from any finite group of order s^2t which admits a Kantor (4-gonal) family of subgroups. Motivated by this construction technique, Payne (1980) described an appropriate group in terms of a set of q 2×2 matrices, later called a *q-clan*, which could be used to construct an EGQ of order (q^2, q). Refining the calculations required in the odd characteristic case, Kantor (1986) used this group to describe two new infinite families of generalised quadrangles. Payne (1985) gave the corresponding simplifications in the even characteristic case and was able to describe a further infinite family, analogous to one of the examples found by Kantor. The work of Thas (1987) then connected this theory to the study of flocks of the quadratic cone.

Let A be a 2×2-matrix over $GF(q)$. Then A is **anisotropic** provided $xAx^T = 0$ if and only if $x = (0, 0) \in GF(q)^2$. So an anisotropic matrix represents a nondegenerate binary quadratic form.

Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ and $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$. We call A and B **equivalent**, written $A \equiv B$, if $a_1 = b_1$, $a_4 = b_4$ and $a_2 + a_3 = b_2 + b_3$. Then $xAx^T = xBx^T$ for all

$x \in GF(q)^2$ if and only if $A \equiv B$, that is, A and B represent the same quadratic form.

For q odd, $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \equiv \begin{pmatrix} a_1 & \frac{a_2+a_3}{2} \\ \frac{a_2+a_3}{2} & a_4 \end{pmatrix}$, and for q even, $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \equiv \begin{pmatrix} a_1 & a_2+a_3 \\ 0 & a_4 \end{pmatrix}$, so in general we often deal with upper triangular matrices, but may use symmetric matrices if q is odd.

Let $\mathcal{C} = \{A_t \equiv \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q)\}$ be a set of q 2×2-matrices over $GF(q)$, indexed by the elements of $GF(q)$. Then $\mathcal{C}$ is called a **q-clan** if and only if the pairwise difference of any two distinct matrices in $\mathcal{C}$ is anisotropic. Clearly the difference of two equivalent matrices cannot be anisotropic, and so a q-clan is a set of q pairwise inequivalent matrices, i.e., a set of q equivalence class representatives. If, for three functions $a : t \mapsto a_t$, $b : t \mapsto b_t$, $c : t \mapsto c_t$ from $GF(q)$ to $GF(q)$, $\mathcal{C} = \{A_t \equiv \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q)\}$ is a q-clan, then it is clear that the functions a and c must be one-to-one, and if q is even, then b must also be one-to-one.

Let $A_s = \begin{pmatrix} a_s & b_s \\ 0 & c_s \end{pmatrix}$ and $A_t = \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix}$. Solving $x(A_s - A_t)x^T = 0$ for $x \in GF(q)^2$ leads to the following useful condition on a set of matrices being a q-clan, where the determinant notation for q odd is used for ease of reference :

Theorem 4.5. *Let $a : t \mapsto a_t$, $b : t \mapsto b_t$, $c : t \mapsto c_t$ be three functions from $GF(q)$ to $GF(q)$. Then $\mathcal{C} = \{A_t \equiv \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q)\}$ is a q-clan if and only if the following holds :*

(i) $-\det((A_s + A_s^T) - (A_t + A_t^T)) = (b_s - b_t)^2 - 4(a_s - a_t)(c_s - c_t)$ *is a nonsquare in $GF(q)$ for distinct $s, t \in GF(q)$, if q is odd;*

(ii) $b_s \neq b_t$ and $\operatorname{trace}\left(\frac{(a_s+a_t)(c_s+c_t)}{(b_s+b_t)^2}\right) = 1$ *for distinct $s, t \in GF(q)$, if q is even.*

The functions $a(t) = t$, $b(t) = bt$ and $c(t) = ct$ for $x^2 + bx + c$ irreducible over $GF(q)$ define a q-clan, called a **classical** q-clan.

Example (The Kantor/Payne monomial q-clans) [Kantor (1986), Payne (1985)] Let $\mathcal{C} = \left\{A_t \equiv \begin{pmatrix} t & 5t^3 \\ 0 & 5t^5 \end{pmatrix} : t \in GF(q)\right\}$ be a set of q 2×2 matrices over $GF(q)$. Then $\mathcal{C}$ is a q-clan if and only if $q \equiv \pm 2 \pmod 5$. We prove this using the above theorem.

For q odd,

$$\begin{aligned} & (b_s-b_t)^2-4(a_s-a_t)(c_s-c_t) \\ = \; & (5s^3-5t^3)^2-4(s-t)(5s^5-5t^5) \\ = \; & 25(s-t)^2(s^2+st+t^2)^2-20(s-t)^2(s^4+s^3t+s^2t^2+st^3+t^4) \\ = \; & (s-t)^2(5s^4+30s^3t+55s^2t^2+30st^3+5t^4) \\ = \; & 5(s-t)^2(s^2+3st+t^2)^2 \end{aligned}$$

Now, for q odd, 5 is a non-square in $GF(q)$ if and only if $q \equiv \pm 2 \pmod 5$. So $s^2+3st+t^2 \neq 0$ for $s \neq t$, and hence $(b_s-b_t)^2-4(a_s-a_t)(c_s-c_t)$ is a nonsquare for $s \neq t$ if and only if $q \equiv \pm 2 \pmod 5$.

For q even,

$$\begin{aligned} & \operatorname{trace}\left(\tfrac{(a_s+a_t)(c_s+c_t)}{(b_s+b_t)^2}\right) \\ = \; & \operatorname{trace}\left(\tfrac{(s+t)(s^5+t^5)}{(s^3+t^3)^2}\right) \\ = \; & \operatorname{trace}\left(1+\tfrac{s^5t+st^5}{s^6+t^6}\right) \\ = \; & \operatorname{trace}\left(1+\tfrac{s^2t+st^2}{s^3+t^3}+\left(\tfrac{s^2t+st^2}{s^3+t^3}\right)^2\right) \\ = \; & \operatorname{trace}(1) \end{aligned}$$

Now, for q even, trace(1)=1 if and only if $q=2^h$, h odd if and only if $q \equiv \pm 2 \pmod 5$. Note that $s^3+t^3 \neq 0$ for $s \neq t$ as $x \mapsto x^3$ is one-to-one, since h is odd implies 3 is coprime to 2^h-1. Hence $\operatorname{trace}\left(\frac{(a_s+a_t)(c_s+c_t)}{(b_s+b_t)^2}\right)=1$ for $s \neq t$ if and only if $q \equiv \pm 2 \pmod 5$.

This q-clan is classical if and only if $q=2$ or $q=3$. It was first given by Kantor (1986) for q odd, and then by Payne (1985) for q even.

An appropriate group

Let $F=GF(q)$ and let $K=\{(\alpha,c,\beta) \in F^2 \times F \times F^2 : \alpha,\beta \in F^2, c \in F\}$. Define a binary operation on K by

$$(\alpha,c,\beta)\circ(\alpha',c',\beta')=(\alpha+\alpha',c+c'+\beta(\alpha')^T,\beta+\beta').$$

Then K is a group of order q^5 with $(\alpha,c,\beta)^{-1}=(-\alpha,\alpha\cdot\beta-c,-\beta)$. The centre of K is $Z=Z(K)=\{(0,c,0): c \in F\}$.

Let $\mathcal{C}$ be a set of q 2×2 matrices over F, indexed by the elements of F. Suppose $A_0=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ and put $K_t=A_t+A_t^T$ for all $A_t \in \mathcal{C}$. Define the following subgroups of K :

$$A(\infty) = \{((0,0),0,\beta) \in K : \beta \in F^2\};$$

$$A(t) = \{(\alpha, \alpha A_t \alpha^T, \alpha K_t) \in K : \alpha \in F^2\} \ \forall t \in F;$$

$$A^*(\infty) = A(\infty)Z = \{((0,0),c,\beta) \in K : c \in F, \beta \in F^2\};$$

$$A^*(t) = A(t)Z = \{(\alpha, c, \alpha K_t) \in K : \alpha \in F^2, c \in F\} \ \forall t \in F.$$

Put $\widetilde{F} = F \cup \{\infty\}$, $\mathcal{J}(\mathcal{C}) = \{A(t) : t \in \widetilde{F}\}$, $\mathcal{J}^*(\mathcal{C}) = \{A^*(t) : t \in \widetilde{F}\}$. Then Payne (1980) proved the following.

Theorem 4.6 (Payne (1980)). *The triple $(K, \mathcal{J}(\mathcal{C}), \mathcal{J}^*(\mathcal{C}))$ satisfies the conditions K1 and K2, and so forms a Kantor (4-gonal) family for K if and only if $\mathcal{C}$ is a q-clan. The resulting GQ, written $GQ(\mathcal{C})$, is an EGQ of order (q^2, q).*

These are precisely the EGQs we will consider in this thesis, namely EGQs of order (q^2, q) arising from a q-clan. From Higman's inequality (2.3) we see that GQs of order (s^2, s) are extremal. In fact, all known GQs of order (s^2, s) are EGQs, and except for the dual of $T_3(\Omega)$, they all arise from the elation group $PSU(4, q^2)$ of the classical GQ $H(3, q^2)$. This elation group $G = PSU(4, q^2)$ is a **special** group of order q^5, that is, its centre $Z(G)$, which has order q, is equal to both its derived subgroup G' and to its Frattini subgroup $\Phi(G)$: $Z(G) = G' = \Phi(G)$.

4.2.1 Flocks, translation planes and elation generalised quadrangles

We have seen a similar condition to that for q-clans before. Indeed, Thas (1987) gave the connection between q-clans and flocks of the quadratic cone.

Let $\mathcal{K}$ be the quadratic cone of PG$(3, q)$ defined earlier, that is, with equation $Q : x_1^2 = x_0 x_2$. Then we have the following :

Theorem 4.7 (Thas (1987)). *For three functions $a : t \mapsto a_t$, $b : t \mapsto b_t$, $c : t \mapsto c_t$ from $GF(q)$ to $GF(q)$,*

$$\mathcal{C} = \left\{ A_t \equiv \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q) \right\} \text{ is a } q\text{-clan}$$

$$\iff \mathcal{F}(\mathcal{C}) = \{[a_t, b_t, c_t, 1]^T : t \in GF(q)\} \text{ is a flock of } \mathcal{K}$$

Consequently, we may construct the spread sets of the associated Thas/Walker linespreads directly from the q-clan. Let $\mathcal{C} = \{A_t = \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q)\}$ be a

q-clan, and define the following set of q^2 2×2 matrices over $GF(q)$:

$$\mathbf{S}(\mathcal{C}) = \left\{ B_{s,t} = A_t + \begin{pmatrix} 0 & s \\ -s & 0 \end{pmatrix} | s, t \in GF(q) \right\}.$$

Then

$$\det(B_{s,t} - B_{s',t'}) = (s-s')^2 + (b_t - b_{t'})(s-s') + (a_t - a_{t'})(c_t - c_{t'}) = 0$$

$$\Leftrightarrow \begin{cases} (b_t - b_{t'})^2 - 4(a_t - a_{t'})(c_t - c_{t'}) = \square & (q \text{ odd}) \\ b_t + b_{t'} = 0 \text{ or trace}\left(\frac{(a_t + a_{t'})(c_t + c_{t'})}{(b_t + b_{t'})^2}\right) = 0 & (q \text{ even}). \end{cases}$$

Since $\mathcal{C}$ is a q-clan, if $B_{s,t} - B_{s',t'}$ is singular, this implies $t = t'$, and so $(s-s')^2 = 0$, giving $s = s'$. Hence $\mathbf{S}(\mathcal{C})$ is a spread set, and gives rise to a linespread $\mathcal{S}(\mathcal{C})$ of $\mathrm{PG}(3, q)$.

That the spread set arising directly from a q-clan is equivalent to the spread set arising from the corresponding flock by the Thas/Walker construction was shown using Plücker coordinates by Gevaert and Johnson (1988).

Note that for two 2×2 matrices A, B, $A \equiv B$ if and only if $B = A + s\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ for some $s \in GF(q)$. So a spread set arising from a q-clan consists of q equivalence classes each consisting of q equivalent matrices. Just as the associated ovoid of the Klein quadric is the union of q conics pairwise intersecting in a common point, this natural partition of a spread set arising from a q-clan hints at the following characterisation of the linespreads arising from flocks.

Theorem 4.8 (Gevaert, Johnson and Thas (1988)). *A flock of a quadratic cone in $PG(3, q)$ is equivalent to a linespread $\mathcal{S}$ of $PG(3, q)$, where $\mathcal{S}$ is the union of q reguli which pairwise intersect in the same line.*

Such a linespread is said to admit a **regular conical cover**. For example, we have seen earlier that the linespreads arising from the Kantor likeable functions have exactly this property, and so there arise flocks of the quadratic cone, called *Kantor likeable flocks.*

4.3 Fundamental Theorem of q-clan geometry

We have seen in the previous sections that the studies of flocks of a quadratic cone of $\mathrm{PG}(3, q)$, of elation generalised quadrangles of order (q^2, q) arising from q-clans, and of translation planes of order q^2 and dimension two over their kernel are intimately connected. These connections give rise to the question of isomorphism of and between these "q-clan geometries". To assist in answering these questions, the so-called Fundamental Theorem of q-clan geometry was developed by a number of authors, the main contributor being Payne (see Payne and Rogers (1990), Bader, Lunardon and Payne (1994), Payne (1996), Johnson and Payne (1997)). Here we present a complete statement of the theorem in context with the many associated structures we have seen. In the following chapter we will apply this theorem to the calculation of the automorphism groups of some known examples.

Let $\mathcal{C} = \{A_t \equiv \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q)\}$ be a q-clan. If $0 \neq \mu \in GF(q)$, $\sigma \in \mathrm{Aut}GF(q)$, $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,q)$, and if x, y, z are any fixed elements of $GF(q)$, then replacing $A_t \in \mathcal{C}$ with $A'_t \equiv \mu B A_t^\sigma B^T + \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ gives a new q-clan $\mathcal{C}' = \{A'_t : t \in GF(q)\}$. Hence if $\mathcal{C} = \{A_t : t \in GF(q)\}$ and $\mathcal{C}' = \{A'_t : t \in GF(q)\}$ are q-clans, we say $\mathcal{C}$ and $\mathcal{C}'$ are **equivalent**, written $\mathcal{C} \sim \mathcal{C}'$, provided there exist the following : $0 \neq \mu \in GF(q)$, $B \in GL(2,q)$, $\sigma \in \mathrm{Aut}GF(q)$, M a 2×2-matrix over $GF(q)$, and a permutation $\pi : t \mapsto \bar{t}$ on $GF(q)$ for which the following holds :

$$A'_{\bar{t}} \equiv \mu B A_t^\sigma B^T + M, \ \forall t \in GF(q).$$

Now let $\mathcal{C} = \{A_t \equiv \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q)\}$ be a q-clan normalised so that $A_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Furthermore, assume without loss of generality that when q is odd the members of $\mathcal{C}$ are indexed so that $a_t = t$ for all $t \in GF(q)$, and when q is even that $b_t = t$ for all $t \in GF(q)$. Let $\mathcal{C}'$ be a second q-clan normalised in the same manner.

The Fundamental Theorem of q-clan geometry shows how to interpret each equivalence between $\mathcal{C}$ and $\mathcal{C}'$ as an explicit isomorphism between the corresponding geometries : flocks of the quadratic cone, elation generalised quadrangles of order (q^2, q), or linespreads of $\mathrm{PG}(3,q)$.

Theorem 4.9 (Fundamental theorem of q-clan geometry). *For any prime power q, let $\mathcal{C} = \{A_t \equiv \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q)\}$ and $\mathcal{C}' = \{A'_t \equiv \begin{pmatrix} a'_t & b'_t \\ 0 & c'_t \end{pmatrix} : t \in GF(q)\}$ be two (not necessarily distinct) normalised q-clans. Then the following are equivalent :*

(i) $\mathcal{C} \sim \mathcal{C}'$;

(ii) The generalised quadrangles $GQ(\mathcal{C})$ and $GQ(\mathcal{C}')$ are isomorphic by an isomorphism mapping (∞) to (∞), $[A(\infty)]$ to $[A'(\infty)]$, and $(\overline{0}, 0, \overline{0})$ to $(\overline{0}, 0, \overline{0})$;

(iii) The flocks $\mathcal{F}(\mathcal{C})$ and $\mathcal{F}(\mathcal{C}')$ are isomorphic;

(iv) The linespreads $\mathcal{S}(\mathcal{C})$ and $\mathcal{S}(\mathcal{C}')$ are isomorphic.

Moreover, these four conditions hold if and only if there exist $0 \neq \lambda \in GF(q)$, $\sigma \in AutGF(q)$, $B \in GL(2,q)$ and a permutation $\pi : t \mapsto \overline{t}$ of $GF(q)$ for which

$$A'_{\overline{t}} \equiv \lambda B^{-1} A_t^{\sigma} B^{-T} + A'_{\overline{0}} \ \forall t \in GF(q).$$

The corresponding isomorphism $\theta : GQ(\mathcal{C}) \mapsto GQ(\mathcal{C}')$ is given by

$$\theta = \theta(\lambda, B, \sigma, \pi) : (\alpha, c, \beta) \mapsto (\alpha^{\sigma} B, \lambda c^{\sigma} + \alpha^{\sigma} B A'_{\overline{0}} B^T (\alpha^{\sigma})^T, \lambda \beta^{\sigma} B^{-T} + \alpha^{\sigma} B K'_{\overline{0}}).$$

If $B^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the corresponding isomorphism $T_\theta : \mathcal{F}(\mathcal{C}) \mapsto \mathcal{F}(\mathcal{C}')$ is defined for planes of the flocks by

$$T_\theta : \begin{bmatrix} a_t \\ b_t \\ c_t \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} a'_{\overline{t}} \\ b'_{\overline{t}} \\ c'_{\overline{t}} \\ 1 \end{bmatrix} = \begin{pmatrix} \lambda a^2 & \lambda ab & \lambda b^2 & a'_{\overline{0}} \\ 2\lambda ac & \lambda(ad+bc) & 2\lambda bd & b'_{\overline{0}} \\ \lambda c^2 & \lambda cd & \lambda d^2 & c'_{\overline{0}} \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} a_t^{\sigma} \\ b_t^{\sigma} \\ c_t^{\sigma} \\ 1 \end{bmatrix}.$$

The corresponding isomorphism between the associated translation planes is induced by the following isomorphism $T : \mathcal{S}(\mathcal{C}) \mapsto \mathcal{S}(\mathcal{C}')$ of the associated linespreads

$$T : (x_0, x_1, x_2, x_3) \mapsto (x_0, x_1, x_2, x_3) \begin{pmatrix} \lambda^{-1} B & \lambda^{-1} B A'_{\overline{0}} \\ 0 & B^{-T} \end{pmatrix}.$$

4.4 Hyperbolic fibrations

In this section we discuss a topic which has very recently been connected with the study of flocks of the quadratic cone.

A **hyperbolic fibration** of $\mathrm{PG}(3,q)$ is a set of $q-1$ hyperbolic quadrics and two lines which together partition the points of $\mathrm{PG}(3,q)$. The classical example of a hyperbolic fibration comes from a pencil of quadrics, but several other families are known to exist.

An important motivation for the study of hyperbolic fibrations is that they give rise to many linespreads of $\mathrm{PG}(3,q)$, and hence to many translation planes. Each choice of one regulus for each quadric in a hyperbolic fibration, together with the lines of the fibration, will define a linespread of $\mathrm{PG}(3,q)$, and so 2^{q-1} linespreads arise. Each of these linespreads contains $q-1$ disjoint reguli, and is said to admit a **regular elliptic cover**.

A hyperbolic fibration is called **regular** if the two lines in the fibration are polar to each other with respect to each of the $q-1$ hyperbolic quadrics in the fibration. All known hyperbolic fibrations are regular, and these are the type we are interested in here.

For a regular hyperbolic fibration $\mathcal{H}$ of $\mathrm{PG}(3,q)$, if we choose bases $\{v_0,v_1\}$ and $\{v_2,v_3\}$ for the two lines l_0 and l_∞ of $\mathcal{H}$, then with respect to the basis $\{v_0,v_1,v_2,v_3\}$ of the vector space underlying $\mathrm{PG}(3,q)$ any quadric in $\mathcal{H}$ will have an equation of the form $ax_0^2+bx_0x_1+cx_1^2+dx_2^2+ex_2x_3+fx_3^2$, for some $a,b,c,d,e,f\in GF(q)$. We abbreviate such a quadric by $V[a,b,c,d,e,f]$, and call (a,b,c) the **front half** and (d,e,f) the **back half**. Since $l_0=V[0,0,0,d,e,f]$ for any $d,e,f\in GF(q)$ with $dx_2^2+ex_2x_3+fx_3^2$ an anisotropic quadratic form, and similarly $l_\infty=V[a,b,c,0,0,0]$ for any $a,b,c\in GF(q)$ with $ax_0^2+bx_0x_1+cx_1^2$ an anisotropic quadratic form, a regular hyperbolic fibration may be written as

$$\mathcal{H}=\{V[d,e,f,0,0,0],V[0,0,0,d,e,f]\}\cup\{V[a_i,b_i,c_i,d,e,f]:i=1,\ldots,q-1\}$$

for some fixed $d,e,f\in GF(q)$ with $dx^2+exy+fy^2$ an anisotropic quadratic form. Such a hyperbolic fibration is said to have **constant back half**, and in a similar manner we may describe a hyperbolic fibration with **constant front half**.

It can be shown that $\mathcal{H}$ is a hyperbolic fibration if and only if $a_ix_0^2+b_ix_0x_1+c_ix_1^2$ is an anisotropic form over $GF(q)$ for all $i=1,\ldots,q-1$ and $(a_i-a_j)x_0^2+(b_i-b_j)x_0x_1+(c_i-c_j)x_1^2$ is an anisotropic form over $GF(q)$ whenever $i\neq j$ (see Baker, Dover, Ebert and Wantz (1998) for the q odd case). Hence we have the following result.

Theorem 4.10 (Baker, Ebert and Penttila (submitted)). *With notation as above, $\mathcal{H}$ is a hyperbolic fibration if and only if*

$$\mathcal{C} = \left\{ A_i \equiv \begin{pmatrix} a_i & b_i \\ 0 & c_i \end{pmatrix} : i = 1, \ldots, q-1 \right\} \cup \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \text{ is a } q\text{-clan.}$$

Thus we have a bijection between regular hyperbolic fibrations with constant back half and flocks of a quadratic cone with one plane specified, namely the plane π_0 corresponding to $A_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Furthermore, Baker, Ebert and Penttila (submitted) prove the following, where equivalence of hyperbolic fibrations is naturally defined under $P\Gamma L(4,q)$.

Theorem 4.11 (Baker, Ebert and Penttila (submitted)). *The number of mutually inequivalent regular hyperbolic fibrations with constant back half arising from a given flock $\mathcal{F}$ of the quadratic cone is the number of orbits of the stabiliser of $\mathcal{F}$ in $P\Gamma L(4,q)$ on the planes of $\mathcal{F}$.*

Thus each flock of the quadratic cone may give rise to a number of inequivalent examples of regular hyperbolic fibrations. Unfortunately, none of the five infinite families of regular hyperbolic fibrations (for q odd) known before these connections were made gave rise to new examples of flocks.

We have noted that a hyperbolic fibration also gives rise to 2^{q-1} linespreads of $\mathrm{PG}(3,q)$ admitting regular elliptic covers. Other than the case of the regular linespread, none of the linespreads arising from a hyperbolic fibration can be isomorphic to the linespread arising from the associated flock via the Thas/Walker construction, as this linespread admits a regular conical cover. Thus with the construction of hyperbolic fibrations from flocks of the quadratic cone, we see that a nonlinear flock gives rise to at least two inequivalent linespreads of $\mathrm{PG}(3,q)$, and hence at least two translation planes (before employing the construction of Hiramine, Matsumoto and Oyama, and Johnson). For a discussion concerning the equivalence of the linespreads arising from a hyperbolic fibration, see Baker, Ebert and Penttila (submitted).

Application of the Fundamental Theorem of q-clan geometry

The automorphism group of a geometric structure describes the symmetries inherent in that structure, and so provides a great deal of information about the nature of the structure. In particular, we can use the automorphism groups of certain structures of the same type to distinguish them from one another, which is extremely important in the context of describing 'new' examples of a certain structure. The Fundamental Theorem of q-clan geometry, presented in Section 4.3, shows how to interpret equivalence of q-clans as explicit isomorphisms between any of the associated geometries, and so can be used to describe the automorphism group of a particular object. Indeed, the explicit description of the isomorphisms between the associated flocks provides a concrete way of describing the isomorphisms between the associated q-clans and GQs in terms of semilinear mappings of three dimensional projective space. This enables the description of certain collineations of the GQ arising from a q-clan, from which we can calculate the order of the automorphism group of the GQ (and more). Often the order of the automorphism group, together with the necessary conditions on the values of q, are sufficient to distinguish examples from one another.

In this section we discuss the ideas behind applying the Fundamental Theorem of q-clan geometry to the calculation of the automorphism group of a GQ arising from a q-clan. A complete treatment of the Fundamental Theorem is given by Payne (1996); here we expound these ideas, and demonstrate their use by calculating the automorphism group of a recently discovered *semifield* example.

We will work in the group coset geometry model of an elation generalised quadrangle arising from a q-clan. So let $GQ(\mathcal{C})$ be the EGQ of order (q^2, q) arising from a q-clan $\mathcal{C}$ and the special group K of Section 4.2. Suppose $\mathcal{C}$ is normalised in the manner of Section 4.3, that is, each matrix A_t in $\mathcal{C}$ is symmetric or upper triangular according as q is odd or even, A_0 is the zero matrix, and $a_t = t$ if q is odd and $b_t = t$ if q is even.

We may assume that $GQ(\mathcal{C})$ is not the classical GQ $\mathrm{H}(3, q^2)$, since in this case the automorphism group is the classical group $P\Gamma U(4, q^2)$, which is well known from the theory of polar spaces. We now have the following useful result.

Theorem 5.1 (Payne and Thas (1991) [99]). *If $GQ(\mathcal{C})$ is not classical, then the point (∞) is fixed by all collineations of $GQ(\mathcal{C})$.*

As an aside, we note that this result is based upon the notion of a GQ having *Property (G)* at some point. This combinatorial property was introduced by Payne (1989), where it was proved that each GQ arising from a q-clan has Property (G) at its point (∞). Payne and Thas (1991) [99] then showed that if a GQ arising from a q-clan has Property (G) at some other point collinear with (∞), then the GQ is classical. We will not discuss Property (G) in any detail here, but mention that Thas (1999) has characterised the GQs arising from q-clans (*flock GQs*) in terms of this Property (G).

Now since all collineations of $GQ(\mathcal{C})$ fix the point (∞), any collineation will map elements of $GQ(\mathcal{C})$ to elements of the same type, with respect to distance from (∞) in the incidence graph of $GQ(\mathcal{C})$. Hence to determine the full automorphism group $\mathrm{Aut}GQ(\mathcal{C})$ of $GQ(\mathcal{C})$, we need only determine the action of $\mathrm{Aut}GQ(\mathcal{C})$ on one type of element of $GQ(\mathcal{C})$, and the kernel of that action if any exists. We choose to describe the action of $\mathrm{Aut}GQ(\mathcal{C})$ on the set X of points not collinear with (∞). The reason for this choice is as follows.

A standard result from permutation group theory says that a finite group acting on a set can be written as a semidirect product of some regular normal subgroup by the stabiliser of some point of the set. Now consider the group K acting by right multiplication on the set X of points not collinear with (∞). This induces a subgroup of $\mathrm{Aut}GQ(\mathcal{C})$ acting regularly on X and fixing every line through (∞), that is, right multiplication by K induces a subgroup of elations of $GQ(\mathcal{C})$. This subgroup has the maximum possible order $(s^2t = q^5)$ of a subgroup of elations, due to the regular action on the set X of size q^5, and so K induces the full elation group of the EGQ $GQ(\mathcal{C})$. Moreover, since $GQ(\mathcal{C})$ is nonclassical, the conjugate of an elation is again an elation, and so the induced elation group is also normal in $\mathrm{Aut}GQ(\mathcal{C})$. Hence we naturally have a normal subgroup K of $\mathrm{Aut}GQ(\mathcal{C})$ acting regularly on the set X of points not collinear with (∞), and so using the standard result mentioned above we need only determine the stabiliser in $\mathrm{Aut}GQ(\mathcal{C})$ of some point of X. The kernel of the action of $\mathrm{Aut}GQ(\mathcal{C})$ on the set X is clearly trivial.

Let $O = ((0,0), 0, (0,0))$. Then O is a point not collinear with (∞), and so we may determine the stabiliser G of O in $\mathrm{Aut}GQ(\mathcal{C})$. Note that G is analogous to the translation complement in the theory of translation planes, and so we might call G the *elation complement* of $GQ(\mathcal{C})$. Similar to above, we now consider the action of G on the set Y of lines through (∞). If $G_{[A(\infty)]}$ is the stabiliser of the line $[A(\infty)]$

through (∞), then we may write G as the following union of cosets

$$G = \bigcup_{[A(s)]\in\mathcal{O}} (G_{[A(\infty)]})g_{[A(s)]}$$

where $g_{[A(s)]}$ is some element of G taking $[A(\infty)]$ to the line $[A(s)]$ in the orbit $\mathcal{O}$ of $[A(\infty)]$ under G. In other words, to determine the action of G on Y we may first determine the stabiliser of the line $[A(\infty)]$ in G and then determine for each line $[A(s)]$ through (∞) a collineation in G taking $[A(\infty)]$ to $[A(s)]$. Furthermore, the kernel of the action of G on Y may not be trivial, and so this kernel must also be determined.

Let us first consider the stabiliser H of $[A(\infty)]$ in G. We are now asking for all collineations of $GQ(\mathcal{C})$ which fix O and $[A(\infty)]$ (and, of course, (∞)). If we take $\mathcal{C} = \mathcal{C}'$ in the statement of the Fundamental Theorem of q-clan geometry (Section 4.3), then such collineations exist if and only if there exist certain parameters defining the collineations which satisfy a particular condition. The concrete way to calculate the freedom of these parameters, and hence determine the number and form of these collineations, is to work with the equivalent condition on the planes of the flock $\mathcal{F}(\mathcal{C})$ associated with the q-clan $\mathcal{C}$.

Now suppose there exists a collineation $\theta \in G$ taking the line $[A(\infty)]$ to some other line $[A(t)]$ through (∞). As an automorphism of $GQ(\mathcal{C})$, θ will map the 4-gonal family corresponding to C to some other 4-gonal family of K corresponding to the line $[A(t)]$. In general, we cannot assume that a q-clan for this second 4-gonal family will be clearly present. However, Payne (1996) describes an automorphism i_s, called the *shift-flip*, which replaces the (normalised) q-clan $\mathcal{C}$ with a (normalised) q-clan $\mathcal{C}^{i_s}$ corresponding to the line $[A(s)]$ through (∞) (i_∞ is the identity automorphism), and uses this to prove the following useful theorem.

Theorem 5.2 (Payne (1996)). *Let $\mathcal{C}$ be a normalised q-clan. Then for arbitrary $s, t \in GF(q) \cup \{\infty\}$, there is a collineation of $GQ(\mathcal{C})$ mapping $[A(s)]$ to $[A(t)]$ if and only if $\mathcal{C}^{i_s}$ is equivalent to $\mathcal{C}^{i_t}$.*

Before continuing, note that each q-clan $\mathcal{C}^{i_s}$ gives rise to a flock of the quadratic cone, and so to each line through (∞) there corresponds a flock. Since there may or may not be a collineation of $GQ(\mathcal{C})$ mapping $[A(s)]$ to $[A(t)]$, the corresponding flocks may or may not be isomorphic by the Fundamental Theorem 4.9. Hence there arise $q + 1$ flocks from $GQ(\mathcal{C})$, which may or may not be pairwise equivalent. This will be clarified further in the following chapter, but will also be important in the following section.

Thus to determine a collineation taking $[A(\infty)]$ to the line $[A(t)]$ through (∞), we first compute the q-clan $\mathcal{C}' = \mathcal{C}^{i_t}$ corresponding to $[A(t)]$. Then by the above Theorem, there exists a collineation taking $[A(\infty)]$ to $[A(t)]$ if and only if $\mathcal{C}$ is equivalent to $\mathcal{C}'$, which by the Fundamental Theorem (Section 4.3) is true if and only if there exist certain parameters defining this collineation which satisfy a particular condition. Again, we attempt to calculate the freedom within these parameters by considering the equivalent condition on the planes of the flocks $\mathcal{F}(\mathcal{C})$ and $\mathcal{F}(\mathcal{C}')$.

Finally, Payne (1996) Proposition 3 shows that the kernel of the action of G on the set of lines through (∞) has order $q-1$, except in the case of the Kantor/Knuth semifield example, where the kernel has order $2(q-1)$ if $\sigma^2 \neq 1$ and order $4(q-1)$ if $\sigma^2 = 1 \neq \sigma$.

5.1 A semifield example

As mentioned earlier, the Fundamental Theorem of q-clan geometry was developed over a number of years by various authors. The ideas grew out of attempts to calculate the automorphism groups of some of the known examples of GQs, with much of the earlier work developing the Fundamental Theorem occurring for characteristic 2. The paper by Payne (1992) collects together many of these calculations and presents a rather complete treatment of the automorphism groups for each of the infinite families known at that time. Here we will demonstrate the use of the Fundamental Theorem by applying it to the calculation of the automorphism group of a recently discovered *semifield* example.

A flock which gives rise to a translation plane coordinatised by a semifield is called a *semifield flock*. Johnson (1987) showed that any semifield flock for q even must be linear, and so for this section we consider q to be odd, and consider a nonlinear semifield flock $\mathcal{F}(\mathcal{C})$ arising from a q-clan

$$\mathcal{C} = \left\{ A_t \equiv \begin{pmatrix} t & b_t \\ 0 & c_t \end{pmatrix} : t \in GF(q) \right\}.$$

Let f be the function $t \mapsto b_t$ and g be the function $t \mapsto c_t$. Then $\mathcal{F}(\mathcal{C})$ is a semifield flock if and only if f and g are additive (see Gevaert and Johnson (1988)). The generalised quadrangles arising from semifield flocks have associated with them a number of interesting structures, which have been deeply studied in recent times.

The point-line dual of the GQ arising from a semifield flock is an EGQ for which the elation group is abelian (see Johnson (1987)). Such EGQs are called *translation generalised quadrangles* (TGQs), and can be constructed from certain partial spreads of a higher dimensional projective space called *eggs*, which generalise the notion of an ovoid (see Payne and Thas (1984)). Such an egg gives rise to an egg in the dual space, from which a TGQ, called the *translation dual*, can be constructed as before, however now the translation dual need not be the point-line dual of a GQ arising from a flock (see Payne (1989)). For recent work on these topics see Blokhuis, Lavrauw and Ball (submitted), Lavrauw and Penttila (2001), Thas (1994), Thas (1997) [115], Thas (1999), Thas (2001) [118], K. Thas (2001), K. Thas [124], [125].

As the functions defining semifield flocks are additive, Bader and Lunardon (1994) have proved the following.

Theorem 5.3 (Bader and Lunardon (1994)). *If $\mathcal{F}(\mathcal{C})$ is a nonlinear semifield flock for which there exists a polynomial $h(t)$ over $GF(q)$ such that for a fixed nonsquare n of $GF(q)$ the equation $f^2(t) + 4tg(t) = nh^2(t)$ is a polynomial identity, then $\mathcal{F}(\mathcal{C})$ arises either from the Kantor/Knuth translation ovoid (page 50) or from the Ganley semifield (page 31).*

Hence any further example of a semifield flock cannot belong to an infinite family of semifield flocks. The term *sporadic* is often used to describe an example of a particular structure which does not belong to an infinite family of that type of structure, and so any further semifield flock must be sporadic (as a semifield flock).

Indeed, there exists such a further example. As a result of a computer search, Penttila and Williams (2000) described a translation ovoid of $Q(4,q)$ for $q = 3^5$, not equivalent with any previously known example. Bader, Lunardon and Pinneri (1999) then described the associated semifield flock, and studied the generalised quadrangles arising, showing them all to be new. In a recent paper, Bader, Ghinelli and Penttila (2001) gave a computerfree construction of this sporadic flock, linking it with the Mathieu group M_{11}. This group is considered to be sporadic as a finite simple group, and so provides further evidence for the sporadicity of this example.

The q-clan associated to the Penttila-Williams/Bader-Lunardon-Pinneri flock has the following form :

$$\mathcal{C} = \left\{ A_t \equiv \begin{pmatrix} t & -t^{27} \\ -t^{27} & -t^9 \end{pmatrix} : t \in GF(3^5) \right\}$$

We will now use the Fundamental Theorem of q-clan geometry to calculate the automorphism group of the GQ, $GQ(\mathcal{C})$, arising from this q-clan $\mathcal{C}$. Firstly, we wish to determine those collineations of $GQ(\mathcal{C})$ fixing the line $[A(\infty)]$ and the point $O = ((0,0),0,(0,0))$. By the Fundamental Theorem 4.9, this is equivalent to determining all permutations $\pi : t \mapsto \bar{t}$ of $GF(q)$, $0 \neq \lambda \in GF(q)$, $\sigma \in \mathrm{Aut}GF(q)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,q)$ for which

$$\begin{bmatrix} \bar{t} \\ \bar{t}^{27} \\ -\bar{t}^{9} \\ 1 \end{bmatrix} = \begin{pmatrix} \lambda a^2 & \lambda ab & \lambda b^2 & \bar{0} \\ 2\lambda ac & \lambda(ad+bc) & 2\lambda bd & \bar{0}^{27} \\ \lambda c^2 & \lambda cd & \lambda d^2 & -\bar{0}^{9} \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} t^{\sigma} \\ t^{27\sigma} \\ -t^{9\sigma} \\ 1 \end{bmatrix}$$

for all $t \in GF(q)$. Thus we obtain three equations :
(i) $\bar{t} = \lambda a^2 t^{\sigma} + \lambda ab t^{27\sigma} - \lambda b^2 t^{9\sigma} + \bar{0}$;
(ii) $\bar{t}^{27} = 2\lambda ac t^{\sigma} + \lambda(ad+bc)t^{27\sigma} - 2\lambda bd t^{9\sigma} + \bar{0}^{27}$;
(iii) $-\bar{t}^{9} = \lambda c^2 t^{\sigma} + \lambda cd t^{27\sigma} - \lambda d^2 t^{9\sigma} - \bar{0}^{9}$.
From (i) and (iii) we have :

$$\begin{aligned} -\bar{t}^{9} &= -\lambda^9 a^{18} t^{9\sigma} - \lambda^9 a^9 b^9 t^{\sigma} + \lambda^9 b^{18} t^{81\sigma} - \bar{0}^{9} \\ &= \lambda c^2 t^{\sigma} + \lambda cd t^{27\sigma} - \lambda d^2 t^{9\sigma} - \bar{0}^{9}. \end{aligned} \qquad (*)$$

The coefficient of $t^{81\sigma}$ must be 0, implying $b = 0$. The coefficient of $t^{27\sigma}$ must also be 0, and since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,q)$ and $b = 0$, we have $c = 0$. Thus from (i) and (ii) we now have :

$$\begin{aligned} \bar{t}^{27} &= \lambda^{27} a^{54} t^{27\sigma} + \bar{0}^{27} \\ &= \lambda ad t^{27\sigma} + \bar{0}^{27}, \end{aligned}$$

which implies $\lambda^{27} a^{54} = \lambda ad$, and so

$$d = \lambda^{26} a^{53}.$$

From the coefficients of $t^{9\sigma}$ in $(*)$ we have $\lambda^9 a^{18} = \lambda d^2 = \lambda^{53} a^{106}$, and so

$$(\lambda a^2)^{44} = 1.$$

Hence $\lambda = \frac{w}{a^2}$ where $w^{44} = 1$. Since $3^5 - 1 = 242$, the 44th roots of unity in $GF(3^5)$ are just the 22nd roots of unity, and so w is a 22nd root of unity. Now for $q = 3^5$, choose a in $q-1$ ways and let $\sigma \in \mathrm{Aut}GF(q)$. Put $\lambda = \frac{w}{a^2}$ where w is a 22nd root of unity, and put $d = w^4 a$, with $b = c = 0$. Then the three equations (i), (ii), (iii) above all hold. Hence the subgroup of Aut$GQ(\mathcal{C})$ fixing $[A(\infty)]$ and $O = ((0,0),0,(0,0))$ has order

$$5.22.(q-1).q = 6468660.$$

Now following the discussion above, we must determine, for each $t \in GF(q)$, a collineation taking $[A(\infty)]$ to the line $[A(t)]$ through (∞). However, if we allow ourselves to make a forward reference to the material in the following chapter, we can combine a result there with the following useful theorem to show that for the Penttila-Williams/Bader-Lunardon-Pinneri semifield flock $\mathcal{F}(\mathcal{C})$, no such collineations of $GQ(\mathcal{C})$ exist. As briefly indicated earlier (page 64), to each line through (∞) of a GQ arising from a q-clan there corresponds a flock of the quadratic cone. Denote these $q+1$ flocks by $\mathcal{F}_t$, where $[A(t)]$ is a line through (∞), for $t \in GF(q) \cup \{\infty\}$.

Theorem 5.4 (Lunardon (1991)). *Let $\mathcal{F}_\infty$ be a nonlinear semifield flock, and let $\mathcal{F}_1, \ldots, \mathcal{F}_q$ be the q flocks corresponding to the q lines through (∞) of the GQ arising from $\mathcal{F}_\infty$, other than the line $[A(\infty)]$ corresponding to $\mathcal{F}_\infty$. If $\mathcal{F}_\infty, \mathcal{F}_1, \ldots, \mathcal{F}_q$ are pairwise isomorphic, then $\mathcal{F}_\infty$ is a Kantor/Knuth semifield flock.*

This theorem as stated here is part of a more general result of Lunardon (1991). That theorem was originally given by Johnson, Lunardon and Wilke (1991), but relied upon the Classification of Finite Simple Groups. Lunardon's proof removed this requirement. The theorem we need from the following chapter is Theorem 6.2, which in the present context says that for a semifield flock $\mathcal{F}_\infty$, the q flocks $\mathcal{F}_1, \ldots, \mathcal{F}_q$ above are pairwise isomorphic. Hence, since the Penttila-Williams/Bader-Lunardon-Pinneri flock $\mathcal{F}(\mathcal{C}) = \mathcal{F}_\infty$ is not a Kantor/Knuth semifield flock, the q flocks $\mathcal{F}_1, \ldots, \mathcal{F}_q$ are not isomorphic to the original semifield flock $\mathcal{F}_\infty$, and so there is no collineation of $GQ(\mathcal{C})$ which maps $[A(\infty)]$ to another line through (∞), by the Fundamental Theorem 4.9. Thus the subgroup calculated above is in fact the full subgroup of Aut$GQ(\mathcal{C})$ fixing the point $O = ((0,0),0,(0,0))$. Hence, for the Penttila-Williams/Bader-Lunardon-Pinneri q-clan $\mathcal{C}$,

$$|\mathrm{Aut}GQ(\mathcal{C})| = 5.22.(q-1).q.q^5.$$

We note that Penttila and Williams (2000) gave the calculation of the stabiliser of the translation ovoid of $Q(4,3^5)$, showing it to be $E_{3^{10}} \rtimes (C_{22} \rtimes C_5)$, where E_n is an elementary abelian group of order n and C_m is a cyclic group of order m. The process of moving from the translation ovoid to the flock implies that the subgroup of $\mathrm{Aut}GQ(\mathcal{C})$ fixing $O = ((0,0),0,(0,0))$ has order $5.22.q.(q-1)$, confirming our calculation above.

BLT-sets

We come now to the main topic of this thesis, namely, BLT-sets. The many connections developed between flocks of the quadratic cone, elation generalised quadrangles and translation planes motivated anew the concentrated study of flocks. In attempting to construct new examples of flocks from known ones, Bader, Lunardon and Thas (1990) developed the method of derivation of flocks when q is odd, which constructs q flocks from a given one, not all of which need be isomorphic with the original flock. This process involves a certain set of $q+1$ points of the nondegenerate quadric in $\mathrm{PG}(4,q)$, called a BLT-set, from which the $q+1$ flocks of the derivation may be reconstructed. Consequently, we have a more general model in which to study flocks of the quadratic cone for q odd, and furthermore, this model is still embedded within a projective space.

The assumption that q be odd is very important, since the process of derivation requires the use of the polarity arising from the nondegenerate quadric $Q(4,q)$, and we have seen that even dimensional quadrics when q is even do not admit polarities. This assumption is somewhat clarified by considering $Q(4,q)$ as a generalised quadrangle. Hence the rest of this thesis is devoted to the study of flocks and their associated structures over fields of odd characteristic only. The case for q even, although we have seen shares much of the same foundational material with q odd, is very different in nature when studied closer. Here there are associated *herds* of $q+1$ ovals, and the techniques involved vary greatly from those for odd characteristic. As well as the linear flocks and the infinite families of examples connected with the Fisher-Thas/Walker flocks (Section 3.1) and the Payne monomial q-clans (Section 4.2), there exist two further infinite families called Subiaco (Cherowitzo, Penttila, Pinneri and Royle (1996)) and Adelaide (Cherowitzo, O'Keefe and Penttila (to appear)). Indeed, Cherowitzo, O'Keefe and Penttila (to appear) have given a unified construction of all of these families except that of Payne, and there currently exist no further examples in characteristic 2. As we shall see later, this is a very different situation to that of characteristic not 2. As well as the recent surveys mentioned at the beginning of Chapter 4, the case for q even is treated in detail in The Subiaco notebook of Payne [86].

6.1 Derivation of flocks and BLT-sets

Let $\mathcal{F}_0 = \{\pi_1, \ldots, \pi_q\}$ be a flock of the quadratic cone $\mathcal{K}_0$ with vertex P_0 of $\mathrm{PG}(3, q)$, with q odd. We may embed $\mathcal{K}_0$ in a nondegenerate quadric $\mathcal{Q}$ of $\mathrm{PG}(4, q)$ so that $\mathcal{K}_0$ is the intersection with $\mathcal{Q}$ of the polar hyperplane H_0 of P_0 with respect to $\mathcal{Q}$. For each plane π_i of $\mathcal{F}_0$, denote by l_i the polar line of π_i with respect to $\mathcal{Q}$. Then l_i is a secant line and meets $\mathcal{Q}$ in the points P_0 and P_i, say. The polar hyperplane H_i of P_i with respect to $\mathcal{Q}$ meets $\mathcal{Q}$ in a quadratic cone $\mathcal{K}_i$ with vertex P_i. For any pair (i, j), $i, j \in \{1, \ldots, q\}$ with $i \neq j$, denote by π_{ij} the plane $H_i \cap H_j$, and let $\pi_{jj} = \pi_j$. By imposing coordinates upon $\mathrm{PG}(4, q)$ and considering the condition on planes of a flock (see Theorem 3.4), Bader, Lunardon and Thas (1990) proved the following.

Theorem 6.1 (Bader, Lunardon and Thas (1990)). *For any $j \in \{1, \ldots, q\}$, the set $\mathcal{F}_j = \{\pi_{ij} \cap \mathcal{K}_j | i = 1, \ldots, q\}$ is a flock of the quadratic cone $\mathcal{K}_j$.*

The flocks $\mathcal{F}_1, \ldots, \mathcal{F}_q$ are said to be **derived** from the flock $\mathcal{F}_0$.

Now consider a set $\{P_0, P_1, \ldots, P_q\}$ of $q + 1$ points of the nondegenerate quadric $\mathcal{Q}$ of $\mathrm{PG}(4, q)$, q odd, and let H_i be the polar hyperplane of P_i with respect to $\mathcal{Q}$. Then the q planes $H_0 \cap H_i$, $i \in \{1, \ldots, q\}$, will define by intersection a flock of the quadratic cone $\mathcal{K}_0 = H_0 \cap \mathcal{Q}$ if and only if the line $H_0 \cap H_i \cap H_j$ is exterior to $\mathcal{Q}$ for all $i, j \in \{1, \ldots, q\}$ with $i \neq j$.

Conversely, for any point P_0 of $\mathcal{Q}$, let H_0 denote the polar hyperplane of P_0 with respect to $\mathcal{Q}$, and let $\mathcal{F}_0$ be any flock of the quadratic cone $\mathcal{K}_0 = H_0 \cap \mathcal{Q}$, so that $\mathcal{F}_0 = \{\pi_1, \ldots, \pi_q\}$ for some planes $\pi_1, \ldots, \pi_q$ of H_0. There exist q uniquely determined points $P_1, \ldots, P_q$ such that $\pi_i = H_0 \cap H_i$ for all $i \in \{1, \ldots, q\}$, where H_i is the polar hyperplane of P_i with respect to $\mathcal{Q}$. Since $\mathcal{F}_0$ is a flock, the line $H_0 \cap H_i \cap H_j$ is exterior to $\mathcal{Q}$ for all $i, j \in \{1, \ldots, q\}$ with $i \neq j$.

So starting with any flock $\mathcal{F}_0$ of the quadratic cone $\mathcal{K}_0 = H_0 \cap \mathcal{Q}$, let $P_0, P_1, \ldots, P_q$ be the points associated with $\mathcal{F}_0$ as before. For any $j \in \{1, \ldots, q\}$, the plane $H_0 \cap H_j$ and the planes $H_i \cap H_j$ with $i \in \{1, \ldots, q\}$ such that $i \neq j$, define a flock of the quadratic cone $\mathcal{K}_j = H_j \cap \mathcal{Q}$ by the above theorem. Hence any three distinct elements of $\{H_0, H_1, \ldots, H_q\}$ intersect in a line which is exterior to $\mathcal{Q}$. As H_i is the polar hyperplane of P_i, any three distinct elements of $\{P_0, P_1, \ldots, P_q\}$ define a plane whose polar line is exterior to $\mathcal{Q}$. Such a set of $q + 1$ points of $\mathcal{Q} = Q(4, q)$, q odd, is called a **BLT-set**, the name being due to Kantor (1991).

Example (**The classical BLT-sets**) Let l be an external line to $\mathcal{Q}$ and $\pi = l^{\perp}$ be the polar plane to l with respect to $\mathcal{Q}$. Then $\pi \cap \mathcal{Q}$ is a conic of π, so $|\pi \cap \mathcal{Q}| = q+1$. Moreover, for distinct $P, Q, R \in \pi \cap \mathcal{Q}$, $\pi = \langle P, Q, R \rangle$, so $\langle P, Q, R \rangle^{\perp}$ is an external line, namely l. Hence $\pi \cap \mathcal{Q}$ is a BLT-set, called the **classical BLT-set**. Note that classical BLT-sets therefore constitute one isometry class of conics within $Q(4,q)$, alluded to on page 14, the other class being those conics whose polar line is secant to $Q(4,q)$. The classical BLT-set gives a linear flock at each point $P \in \pi \cap \mathcal{Q}$, because all the planes $P^{\perp} \cap Q^{\perp}$ lie on the line $l = \pi^{\perp}$.

If the flock $\mathcal{F}$ gives rise to a semifield or likeable translation plane via the André/Bruck-Bose constructions, then $\mathcal{F}$ is called a **semifield** or **likeable** flock, respectively.

Theorem 6.2 (Bader, Lunardon and Thas (1990)). *If $\mathcal{F}_0$ is a semifield or likeable flock, then the flocks $\mathcal{F}_1, \ldots, \mathcal{F}_q$ derived from $\mathcal{F}_0$ are pairwise isomorphic.*

Hence for semifield and likeable flocks, there can be at most one new class of flocks arising from the process of derivation. In general, Bader, Lunardon and Thas (1990) gave the following result regarding the set of flocks derived from a given BLT-set.

Theorem 6.3 (Bader, Lunardon and Thas (1990)). *Let P_1 and P_2 be two points of the BLT-set $\mathcal{P}$. Then the flock $\mathcal{F}_1$ arising from P_1 is isomorphic to the flock $\mathcal{F}_2$ arising from P_2 if and only if P_1 and P_2 are in the same orbit of $P\Gamma O(5,q)_{\mathcal{P}}$.*

Thus we have

Corollary 6.1. *The number of distinct, non-isomorphic flocks arising from a BLT-set $\mathcal{P}$ is equal to the number of orbits of $P\Gamma O(5,q)_{\mathcal{P}}$ on $\mathcal{P}$.*

Now note that the property defining a BLT-set is a condition on triples of points from the set. Thus we may define a **partial BLT-set** as a set of $b \geq 3$ points of the nondegenerate quadric $Q(4,q)$, q odd, such that any three distinct points in the set span a plane whose polar line with respect to $Q(4,q)$ is an external line. Clearly, a partial BLT-set of size b will give rise to b **partial flocks**, that is, to b sets of pairwise disjoint conics on the relevant quadratic cones, each of size $b-1$. We will investigate this notion a little further here, but the real power of this observation will become clear when we later use the computer to search for new examples of BLT-sets. Note that the condition for a set of points of $Q(4,q)$ to be a BLT-set is equivalent to requiring that for any three points of the set, there is no point of $Q(4,q)$ collinear (in a line of $Q(4,q)$) with all three of the points.

Since the nondegenerate quadric $Q(4,q)$ of PG$(4,q)$ is also a generalised quadrangle of order q, we consider the concept of a BLT-set in the GQ model of $Q(4,q)$.

Motivated by the definition of a BLT-set in the quadric model above, we define a **partial BLT-set** of the generalised quadrangle $\mathrm{Q}(4,q)$ as a set $\mathcal{P}$ of $b \geq 3$ points of $\mathrm{Q}(4,q)$ such that no point of $\mathrm{Q}(4,q)$ is collinear with more than 2 points of $\mathcal{P}$. Note that we make no requirement upon the parity of q at this point, merely for purposes of investigating this definition in the abstract model of $Q(4,q)$ as a generalised quadrangle.

Clearly, no two points of a partial BLT-set are collinear, since by the GQ axiom, a point of a BLT-set not on a line through two other points of the BLT-set will be collinear with some point on that line. Furthermore, consider a line l meeting the partial BLT-set $\mathcal{P}$ in a point P. By the GQ axiom, every point of $\mathcal{P}\setminus\{P\}$ is collinear with a unique point of l. But no two points Q, R of $\mathcal{P}\setminus\{P\}$ can be collinear with the same point of l, since this common point would then be collinear with three points P, Q, R of $\mathcal{P}$. Hence a partial BLT-set can have at most $q+1$ points, the number of points on a line of $\mathrm{Q}(4,q)$. Thus we define a **BLT-set** of $\mathrm{Q}(4,q)$ to be a partial BLT-set of maximal size $q+1$ (in accordance with our earlier definition in the quadric model).

Now consider a line l not meeting a BLT-set $\mathcal{P}$. (Such a line l must exist : take a line m meeting $\mathcal{P}$ in a point P; then m contains a further point R not in $\mathcal{P}$; as $\mathrm{Q}(4,q)$ is a GQ of order $q \geq 2$, there are at least two further lines on R other than m; at most one of these further lines can meet $\mathcal{P}$; and so we have a third line l on R not meeting $\mathcal{P}$.) Consider a point R of l, and suppose R is collinear in the line m with a point P of $\mathcal{P}$. Then we have seen earlier that each point of $\mathcal{P}$ is collinear with a distinct point of m, and so there is a second point Q of $\mathcal{P}$ collinear with the point R. Thus each point of a line not meeting a BLT-set is collinear with exactly 0 or 2 points of the BLT-set. Hence, with respect to the points of a line not meeting a BLT-set we may pair up the points of the BLT-set, and so the size of a BLT-set is divisible by 2, i.e., $q+1$ is even. Thus BLT-sets can exist only when q is odd, as was required earlier in the quadric model of $Q(4,q)$.

A set of points of a GQ such that every point not in the set is collinear with exactly 0 or 2 points of the set has been called a $(0,2)$-set by De Soete and Thas (1984). Hence a BLT-set is a $(0,2)$-set, and some of the above ideas and results, for example, the size of a BLT-set and the parity of q for the existence of a BLT-set, can also be found in their paper. Furthermore, the concept of BLT-set has been generalised to higher polar rank polar spaces, in a number of different ways. See, for example, O'Keefe and Thas (1997), Bader, O'Keefe and Penttila (submitted) and Shult (1996) (surveying joint work with Thas). In this thesis we will only be concerned with BLT-sets and partial BLT-sets of $Q(4,q)$.

In Section 1.2 we defined the discriminant for nondegenerate orthogonal spaces with q odd, and saw that it provides a complete invariant of such spaces. Here we use the discriminant to study BLT-sets. The following results are due to Bader, O'Keefe and Penttila (submitted), the treatment of which we follow closely here, with the final corollary originally being due to Johnson (1992).

Let $F = GF(q)$, q odd, let $V = F^5$ be a vector space of rank 5 over F, and let Q be a nondegenerate quadratic form with polar form f defined on V. Then $(V,Q) = O(5,q)$ is a nondegenerate orthogonal space, which defines a nondegenerate parabolic quadric $Q(4,q)$ in the projective space $\mathrm{PG}(4,q)$ arising from V. Let $\perp$ be the polarity arising from f.

Lemma 6.1 (Bader, O'Keefe and Penttila (submitted)). *If $x,y,z \in O(5,q)$ are pairwise linearly independent singular vectors, then $\langle x,y,z\rangle^{\perp}$ defines an external line with respect to the $Q(4,q)$ if and only if*

$$\frac{-2f(x,y)f(x,z)f(y,z)\square}{\mathrm{disc}(Q)} = \boxtimes \in F^*/\square.$$

Proof : Since x,y,z are pairwise linearly independent singular vectors, $W = \langle x,y,z\rangle$ is a nondegenerate subspace of $O(5,q)$. Let $W^{\perp} = \langle u,v\rangle$. Then $S = \{x,y,z,u,v\}$ is a basis for V. Let B be the matrix of f with respect to S, and let B_W be the matrix of f restricted to W. Then

$$\det(B) = \det(B_W)\det(B_{W^{\perp}}).$$

So

$$\frac{\square}{\mathrm{disc}(Q\mid_{W^{\perp}})} = \frac{\mathrm{disc}(Q\mid_W)}{\mathrm{disc}(Q)}.$$

Now $\det(B_W) = 2f(x,y)f(x,z)f(y,z)$ since f is symmetric. So

$$\frac{\square}{\mathrm{disc}(Q\mid_{W^{\perp}})} = \frac{2f(x,y)f(x,z)f(y,z)\square}{\mathrm{disc}(Q)}.$$

Now consider the subspace $W^{\perp}$. This has rank 2, so is a line in $\mathrm{PG}(4,q)$. Hence $W^{\perp}$ is an external line (an $O^-(2,q)$ space) if and only if $-\mathrm{disc}(Q\mid_{W^{\perp}}) = \boxtimes$. The result follows.

Corollary 6.2. *If $\mathcal{P}$ is a set of at least 3 points of $Q(4,q)$, then $\mathcal{P}$ is a partial BLT-set if and only if for all $\langle x\rangle, \langle y\rangle, \langle z\rangle \in \mathcal{P}$ we have:*

$$\frac{-2f(x,y)f(x,z)f(y,z)\square}{\mathrm{disc}(Q)} = \boxtimes \in F^*/\square.$$

Lemma 6.2 (Bader, O'Keefe and Penttila (submitted)). *If $\mathcal{P} = \{\langle x\rangle, \langle y\rangle, \langle z\rangle, \langle w\rangle\}$ is a set of four points of $Q(4,q)$ such that $\{\langle x\rangle, \langle y\rangle, \langle z\rangle\}$, $\{\langle x\rangle, \langle y\rangle, \langle w\rangle\}$ and $\{\langle x\rangle, \langle z\rangle, \langle w\rangle\}$ are partial BLT-sets, then $\mathcal{P}$ is a partial BLT-set.*

Proof : It suffices to check that $\{\langle y\rangle, \langle z\rangle, \langle w\rangle\}$ is a partial BLT-set. Now we know that

$$-2f(x,y)f(x,z)f(y,z)\square/\mathrm{disc}(Q),$$

$$-2f(x,y)f(x,w)f(y,w)\square/\mathrm{disc}(Q),$$

$$-2f(x,z)f(x,w)f(z,w)\square/\mathrm{disc}(Q)$$

are all equal to $\boxtimes \in F^*/\square$, hence their product

$$\left(\frac{-2f(x,y)f(x,z)f(x,w)\square}{\mathrm{disc}(Q)}\right)^2 \frac{-2f(y,z)f(y,w)f(z,w)\square}{\mathrm{disc}(Q)}$$

also equals $\boxtimes \in F^*/\square$, and the result follows.

Corollary 6.3 (Johnson (1992)). *Let $\mathcal{P}$ be a set of at least 3 points of $Q(4,q)$. If there exists $\langle x\rangle \in \mathcal{P}$ such that $\{\langle x\rangle, \langle y\rangle, \langle z\rangle\}$ is a partial BLT-set for all $\langle y\rangle, \langle z\rangle \in \mathcal{P} \setminus \{\langle x\rangle\}$, then $\mathcal{P}$ is a partial BLT-set.*

Hence to determine if a set of points of $Q(4,q)$ is in fact a (partial) BLT-set, we need only consider the triples on one point of the set, and not all triples in the set. This observation, coupled with the previous corollary, provides a very cheap and easily implemented way for checking if a set of points of $Q(4,q)$ is a (partial) BLT-set, when later we use the computer to search for new examples of BLT-sets.

6.2 BLT-sets, generalised quadrangles and translation planes

We have seen earlier that a flock gives rise to an EGQ of order (q^2,q) via a group coset geometry construction involving the associated q-clan. Alternatively, Knarr (1992) gave a beautiful geometric construction of this GQ directly from the associated BLT-set.

The construction of Knarr takes place in the polar space $\mathrm{W}(5,q)$, q odd, arising from a symplectic polarity of $\mathrm{PG}(5,q)$. This polar space has polar rank 3, and so contains points, lines and planes. The construction involves fixing a 3-dimensional subspace of $\mathrm{PG}(5,q)$ and considering the generalised quadrangle $\mathrm{W}(q)$ induced in this subspace. Observe that the duality between the generalised quadrangles $\mathrm{W}(q)$

and Q$(4,q)$ (Theorem 1.12) means that the concept of a BLT-set of Q$(4,q)$, q odd, can be transferred to W(q). Hence, a **BLT-set** of *lines* of W(q) is a set $\mathcal{L}$ of $q+1$ lines of W(q) such that no line of W(q) is concurrent with more than 2 lines of $\mathcal{L}$. A classical BLT-set of W(q) will then be a regulus of PG$(3,q)$.

Let ρ be a symplectic polarity of PG$(5,q)$, q odd, defining W$(5,q)$, and fix a point P of W$(5,q)$. Let Σ be a 3-dimensional subspace of PG$(5,q)$ such that $P \notin \Sigma \subset P^\rho$. In Σ, ρ induces a symplectic polarity, and hence a generalised quadrangle W(q). Let $\mathcal{L} = \{l_0, l_1, \ldots, l_t\}$ be a BLT-set of W(q), and define the incidence structure $\mathbf{K}(\mathcal{L})$ as follows :

P	lines on P	points collinear with P	lines not on P	points not collinear with P
$\bullet$	$\odot$	$\odot$	$\odot$	$\odot$
P	planes $\pi_t = Pl_t$	lines m of PG$(5,q)$, not on P, in one plane $\pi_t = Pl_t$	totally isotropic planes of ρ, not in P^ρ, meeting some π_t in a line m	points of PG$(5,q)$, not in P^ρ

Incidence in $\mathbf{K}(\mathcal{L})$ is inherited from PG$(5,q)$. Then we have that

Theorem 6.4 (Knarr (1992)). $\mathbf{K}(\mathcal{L})$ *is a GQ of order* (q^2,q).

Proof : We present as an example the proof of the GQ axiom for a nonincident point not collinear with P and line not on P. The order of the GQ follows from the combinatorics of W$(5,q)$. We first note that a totally isotropic plane π (representing a line not on P) cannot meet two planes $\pi_s = Pl_s$, $\pi_t = Pl_t$ (representing lines on P) in W$(5,q)$, since the lines l_s, l_t are disjoint, being elements of a BLT-set. So suppose that Q is a point of PG$(5,q)$ not in P^ρ (representing a point not collinear with P), and that π is a totally isotropic plane of ρ not in P^ρ meeting some plane $\pi_t = Pl_t$, $l_t \in \mathcal{L}$ in a line n not on P (representing a line not on P), such that $Q \notin \pi$. We must show that there is a unique totally isotropic plane π' (of ρ not in P^ρ meeting some plane $\pi_s = Pl_s$, $l_s \in \mathcal{L}$ in a line not on P) containing Q which meets π in a unique point Q' of PG$(5,q)$ (not in P^ρ). So, as Q is a point not on the maximal subspace π of W$(5,q)$, by Tits' polar space axiom, $a = \{x \in \pi | Q \sim x\}$ is a line of π. Project a from Q onto P^ρ to obtain the line b. Projecting b from P onto Σ gives a line c, which meets a line $l \in \mathcal{L}$, and hence meets another line $l' \in \mathcal{L}$ in the point X, as $\mathcal{L}$ is a $(0,2)$-set with respect to lines. The point X corresponds to a point Y on the line b, and hence to a point Z on the line a in π. The line QZ is a line of $\mathrm{W}(5,q)$ which meets P^ρ in the point Y on the plane $\sigma = Pl'$. The points on σ collinear with Q form the line $m = \{x \in \sigma | Q \sim x\}$. Then the plane $\pi' = Qm$ and the point Z are the unique elements we require.

Furthermore, Knarr (1992) proved that $\mathbf{K}(\mathcal{L})$ is isomorphic to the generalised quadrangle arising from a flock associated to $\mathcal{L}$ via the group coset geometry construction. To see this, consider the following example.

Example ($\mathbf{K}(\mathcal{L})$ is an EGQ with base point P)
Here let $f((x_0,x_1,x_2,x_3,x_4,x_5),(y_0,y_1,y_2,y_3,y_4,y_5)) = x_0y_5 - x_5y_0 + x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2$ be a nondegenerate alternating form on $GF(q)^6$ defining the symplectic polarity ρ and so $\mathrm{W}(5,q)$. Let

$$G = \left\{ M_{a,b,c,d,e} = \begin{pmatrix} 1 & a & b & c & d & e \\ 0 & 1 & 0 & 0 & 0 & d \\ 0 & 0 & 1 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & -b \\ 0 & 0 & 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} | a,b,c,d,e \in GF(q) \right\}$$

Then G is a group of isometries of the vector space $GF(q)^6$ with form f, so $G \leq Sp(6,q)$. Thus G commutes with ρ and gives a group of automorphisms of the polar space $\Pi(\rho)$ $=\mathrm{W}(5,q)$. G fixes the point $P(1,0,0,0,0,0)$ and fixes every subspace of P^ρ on P. Hence, if we perform the Knarr construction using P, G will fix each plane that represents a line on P. Hence G fixes the set of lines that represent points collinear with P and the set of totally isotropic planes that represent lines not on P. G acts regularly on the set of points of $\mathrm{PG}(5,q)$ not in P^ρ, and so $\mathbf{K}(\mathcal{L})$ is an EGQ with base point P.

By multiplying two elements of G we see that

$$\begin{aligned} M_{a,b,c,d,e}M_{a',b',c',d',e'} &= M_{a+a',b+b',c+c',d+d',e+e'+ad'+bc'-b'c-a'd} \\ &\neq M_{a',b',c',d',e'}M_{a,b,c,d,e}, \end{aligned}$$

and so G is a non-abelian group of order q^5, with centre

$$Z = Z(G) = \{M_{0,0,0,0,e} | e \in GF(q)\}$$

of order q, and G/Z is an elementary abelian group of order q^4. Furthermore, the centre Z is both the derived subgroup G' and the Frattini subgroup $\Phi(G)$: $Z(G) = G' = \Phi(G)$. Indeed, this group G is isomorphic to the group of Payne in Section 4.2.

Note that $\mathbf{K}(\mathcal{L})$ is isomorphic to the classical GQ $\mathrm{H}(3, q^2)$ if and only if $\mathcal{L}$ is a classical BLT-set. As the Knarr construction relies on the existence of a BLT-set, we cannot use this construction for the case of q even. However, Thas (1999) has recently given a stunning geometric construction of these flock GQs which holds for all q. See Thas (1999) and also Thas (2001) [119] for this construction and the connections with the Knarr construction.

Working in the group coset geometry model of a GQ arising from a q-clan, Payne and Rogers (1990) were able to show that for any flock $\mathcal{F}$, the GQ arising from any derived flock is a recoordinatised version of the GQ arising from $\mathcal{F}$, and hence is isomorphic with the GQ arising from $\mathcal{F}$. In fact, each flock derived from $\mathcal{F}$ corresponds to a line through the base point (∞) of the GQ arising from $\mathcal{F}$, with $\mathcal{F}$ corresponding to the line $[A(\infty)]$, as was alluded to in the previous chapter. Hence derivation of $\mathcal{F}$ corresponds to interchanging the line $[A(\infty)]$ with each other line through (∞). In terms of the associated BLT-set, we then have the following.

Theorem 6.5 (Payne and Rogers (1990)). *A BLT-set gives rise to exactly one generalised quadrangle.*

Thus we see that BLT-sets are as general as GQs with respect to modelling flocks of the quadratic cone. As BLT-sets are substructures of polar spaces, two BLT-sets $\mathcal{P}_1$ and $\mathcal{P}_2$ of $Q(4, q)$ (respectively, $W(q)$) are said to be **isomorphic** if and only if there exists an element of $P\Gamma O(5, q)$ (respectively, $P\Gamma Sp(4, q)$) which maps $\mathcal{P}_1$ onto $\mathcal{P}_2$. The following result was first given by Kantor (1991) in the context of the group coset geometry construction, but was also proved by Payne and Thas (1991) [100] in a more geometric fashion.

Theorem 6.6. *The BLT-sets $\mathcal{P}_1$ and $\mathcal{P}_2$ are isomorphic if and only if the generalised quadrangle arising from $\mathcal{P}_1$ is isomorphic to the generalised quadrangle arising from $\mathcal{P}_2$.*

Hence the automorphism group of the generalised quadrangle arising from a BLT-set can be calculated from the group of the BLT-set, by which we mean the stabiliser of the BLT-set in the automorphism group of the relevant polar space in which the BLT-set is defined, namely in $P\Gamma O(5,q)$ or $P\Gamma Sp(4,q)$. In particular, every collineation of the GQ arising from a BLT-set induces an automorphism of the space of the BLT-set which fixes the BLT-set. Since the points of the BLT-set correspond to the lines through (∞) of the associated GQ, the group of the BLT-set corresponds to the subgroup of the automorphism group of the associated GQ acting on the lines through (∞), modulo the kernel of this action (except in the case of the Kantor/Knuth semifield example, where some elements of the kernel do indeed induce nontrivial automorphisms of the space of the BLT-set (fixing the BLT-set)).

We have seen that a flock gives rise to many linespreads of $\mathrm{PG}(3,q)$, both via the Thas/Walker construction of an ovoid of the Klein quadric and via the construction of regular hyperbolic fibrations with constant back half. Thus we may interpret these constructions instead directly from the associated BLT-set.

The ovoid of the Klein quadric constructed from a flock by the Thas/Walker construction (Section 4.1.1) consists of a union of q conics pairwise intersecting in a common point. The conics are the intersection with the Klein quadric of the planes which are polar to each of the planes of the given flock, and the common point is the vertex of the underlying quadratic cone. Now embed the quadratic cone $\mathcal{K}$ of $\mathrm{PG}(3,q)$ as a hyperplane section of the nondegenerate parabolic quadric $Q(4,q)$, which in turn is embedded as a section of the Klein quadric by the hyperplane H of $\mathrm{PG}(5,q)$. Let $\mathcal{F}$ be a flock of $\mathcal{K}$ and let $\mathcal{P}$ be the BLT-set of $Q(4,q)$ associated to $\mathcal{F}$. Then one point of $\mathcal{P}$ is the vertex V of $\mathcal{K}$, whilst the other q points of $\mathcal{P}$ correspond to the planes of $\mathcal{F}$. If Q is the polar point to H, then the ovoid arising from the Thas/Walker construction is the set of points of the quadric on the planes $\langle V,Q,P\rangle$, where P is a point of $\mathcal{P}$ other than V. Hence for each choice of a point of a BLT-set of $Q(4,q)$, we can construct an ovoid of the Klein quadric and hence a linespread of $\mathrm{PG}(3,q)$. Clearly points in the same orbit of the BLT-set will give rise to equivalent ovoids.

By the process of derivation, each point of a BLT-set determines a flock, each plane of which determines a regular hyperbolic fibration with constant back half (Section 4.4). Since each plane of a flock arising from a point P of a BLT-set $\mathcal{P}$ corresponds to a distinct point of $\mathcal{P}$ other than P, we see that each hyperbolic fibration arising from a flock corresponds to an ordered pair of points of the associated BLT-set. Hence equivalence of the regular hyperbolic fibrations with constant back half arising from a BLT-set $\mathcal{P}$ corresponds to orbits on ordered pairs of points of $\mathcal{P}$ under the stabiliser of $\mathcal{P}$ in $P\Gamma O(5,q)$. (See Baker, Ebert and Penttila (submitted).)

6.3 The known infinite families of BLT-sets

Consider the process of derivation in an analytic setting, that is, with coordinates.

Let the nondegenerate quadric $Q(4,q)$ of $\mathrm{PG}(4,q)$, q odd, be defined by the quadratic form $Q: x_0x_4 + x_1x_3 - x_2^2 = 0$, and let H_0 be the polar hyperplane of the point $P_0 = (0,0,0,0,1)$ with respect to $Q(4,q)$. Then H_0 meets $Q(4,q)$ in the quadratic cone $\mathcal{K}_0$ with equations $x_0 = x_1x_3 - x_2^2 = 0$, and P_0 is the vertex of $\mathcal{K}_0$. Let $\mathcal{F}_0$ be any flock of $\mathcal{K}_0$, where the planes $\pi_i = [a_i, b_i, c_i, 1]^T$ of $\mathcal{F}_0$ have equations $x_0 = a_ix_1 + b_ix_2 + c_ix_3 + x_4 = 0$, $i \in \{1, \ldots, q\}$, with $(b_i - b_j)^2 - 4(a_i - a_j)(c_i - c_j) = \boxtimes$, $i \neq j$. Then we saw above that the polar line l_i of π_i with respect to $Q(4,q)$ meets $Q(4,q)$ in two points P_0 and P_i. A short calculation shows that $P_i = (1, c_i, -\frac{b_i}{2}, a_i, \frac{b_i^2}{4} - a_ic_i)$, and so given coordinates for planes of a flock we can write down the coordinates of the associated BLT-set. In other words, if $\mathcal{C} = \left\{ \begin{pmatrix} a_t & \frac{1}{2}b_t \\ \frac{1}{2}b_t & c_t \end{pmatrix} : t \in GF(q) \right\}$ is a q-clan, then the associated BLT-set, with distinguished point $(0,0,0,0,1)$, can be written in the following form, where $Q(4,q)$ is defined by the quadratic form $Q: x_0x_4 + x_1x_3 - x_2^2$.

$$\mathcal{P}(\mathcal{C}) = \left\{ (1, c_t, -\frac{b_t}{2}, a_t, \frac{b_t^2}{4} - a_tc_t) | t \in GF(q) \right\} \cup \left\{ (0,0,0,0,1) \right\}.$$

An important consequence of the development of derivation of flocks is the possibility of obtaining new examples of flocks from known ones. Bader, Lunardon and Thas (1990) investigated this for each of the examples known at that time. We have seen many of the known examples in earlier sections as examples of one or another of the various related structures. Here we collect together these examples, and present them as q-clans corresponding to flocks of the quadratic cone given above, so that the corresponding BLT-set with distinguished point $(0,0,0,0,1)$ is defined with respect to the quadratic form $Q: x_0x_4 + x_1x_3 - x_2^2$. The calculation of the q-clan condition (see Theorem 4.5) for each example is given here for consistency. For each family of BLT-sets we will discuss the various related structures and attempt to give complete references for where these appeared in the literature before the connections were known. Note that the paper of Gevaert and Johnson (1988) provided at that time a unified description of both the connections and the known examples. The associated ovoids, linespreads and translation planes discussed here will be those arising via the Thas/Walker and André/Bruck-Bose constructions.

The general group orders presented are taken from the survey of Payne (1992) of the collineation groups of the GQs known at that time. The calculations appeared in various papers predating Payne (1992), and we refer to this paper for full references. Here we have factored out the q^5 elations and the $q-1$ collineations in the kernel of the action on the lines through (∞) to obtain the order in general of the stabiliser $P\Gamma O(5,q)_{\mathcal{P}}$ of the BLT-set $\mathcal{P}$ in $P\Gamma O(5,q)$, where $q = p^h$. Note that for the Kantor/Knuth semifield example, we do not factor out the entire kernel, since some of these collineations do induce automorphisms of the space of the BLT-set fixing the BLT-set, in particular, hyperbolic reflections with axis the hyperbolic quadric spanned by the BLT-set (see Corollary 6.5). For small q, some examples belong to more than one infinite family, which may or may not yet be known, and consequently the group order may grow somewhat in various cases. Using a computer, as we discuss in later chapters, we have calculated the group orders for all the known examples over small fields, and to clarify the general statements in Payne (1992), we here state explicitly the group order for each example of the infinite family, since this is a significant piece of information when studying small examples.

There exist two further families which we have not yet seen in detail, namely the family of Fisher (Fisher and Thas 1979) and the family of Penttila (1998). Since their description as q-clans is somewhat involved, these two examples will be discussed later in the alternative model of $Q(4,q)$ given by Penttila (1998), in which the second example was originally described.

For clarity, we note here that there exists a further infinite family of BLT-sets, published by Penttila and the present author (2001) and appearing in this thesis in Chapter 9.

The classical BLT-sets

These have been described in the example on page 70, and exist for all odd q. If n is a fixed nonsquare of $GF(q)$, then the classical q-clan is

$$\mathbf{C} = \left\{ \begin{pmatrix} t & 0 \\ 0 & -nt \end{pmatrix} : t \in GF(q) \right\}.$$

We saw that all flocks arising from the classical BLT-set are linear, and so all line-spreads are regular. Hence the translation planes arising are Desarguesian. The generalised quadrangle arising is isomorphic to the classical GQ $\mathrm{H}(3,q^2)$ (see Payne and Thas (1984)), which has automorphism group $P\Gamma U(4,q^2)$. In this case, the kernel of the GQ is larger than that of nonclassical GQs, and has size $2(q-1)(q+1)$.

$$|P\Gamma O(5,q)_{\mathcal{P}}| = 2h(q-1)q(q+1)^2.$$

The Fisher-Thas/Walker/Kantor BLT-sets

For q odd and $q \equiv -1 \pmod 3$:

$$\mathbf{C} = \left\{ \begin{pmatrix} t & \frac{3}{2}t^2 \\ \frac{3}{2}t^2 & 3t^3 \end{pmatrix} : t \in GF(q) \right\}$$

$$\begin{aligned} & (b_s - b_t)^2 - 4(a_s - a_t)(c_s - c_t) \\ = \; & (3s^2 - 3t^2)^2 - 4(s-t)(3s^3 - 3t^3) \\ = \; & 9(s-t)^2(s+t)^2 - 12(s-t)^2(s^2 + st + t^2) \\ = \; & (s-t)^2(-3s^2 + 6st - 3t^2) \\ = \; & -3(s-t)^4 \end{aligned}$$

Since $q \equiv -1 \pmod 3$, -3 is a non-square in $GF(q)$.

The Fisher-Thas/Walker flock described on page 43 is the flock arising from the point $(0,0,0,0,1)$ of this BLT-set. In fact, this flock gives rise to a likeable translation plane, where the likeable function is just the zero function $L(t) = 0$ for all $t \in GF(q)$. Hence by Theorem 6.2, all the derived flocks are isomorphic. Bader, Lunardon and Thas (1990) showed that the flock arising from the point $(1,0,0,0,0)$ is isomorphic to the original flock, and hence all flocks arising from this BLT-set are Fisher-Thas/Walker flocks. Hence the translation planes arising are those of Walker (1976). Note that these examples can be defined similarly for q even and $q \equiv -1 \pmod 3$, $q > 2$, as we have seen. In this case, the associated translation planes were first described by Betten (1973). The generalised quadrangle arising in general was first given by Kantor (1980), from a construction involving the $G_2(q)$ generalised hexagon. We note that it was this paper which began the detailed study of generalised quadrangles as group coset geometries.

$$|P\Gamma O(5,q)_{\mathcal{P}}| = \begin{cases} h(q-1)q(q+1), & q > 5; \\ 720, & q = 5. \end{cases}$$

Theorem 6.7 (Thas (1993)). *Let $\mathcal{F}$ be a flock of the quadratic cone of $PG(3,q)$. Assume $q \geq 4$ and, if q is odd, assume that*

$$q \notin \{17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 79, 83\}.$$

Then $\mathcal{F}$ is the flock of Fisher-Thas/Walker if and only if no four planes of $\mathcal{F}$ have a point in common.

A $(q+1)$-**arc** of $\mathrm{PG}(4,q)$ is a set of $q+1$ points such that any 5 points of the set span the whole space.

Corollary 6.4. *With the same conditions on q as in the previous theorem, a set of $q+1$ points of $Q(4,q)$ is a Fisher-Thas/Walker/Kantor BLT-set if and only if it is a $(q+1)$-arc.*

The Kantor/Knuth semifield BLT-sets

For q odd and not prime, n a fixed nonsquare of $GF(q)$ and $\sigma \neq 1$ a nonidentity automorphism of $GF(q)$:

$$\mathbf{C} = \left\{ \begin{pmatrix} t & 0 \\ 0 & -nt^{\sigma} \end{pmatrix} : t \in GF(q) \right\}$$

$$\begin{aligned} & (b_s - b_t)^2 - 4(a_s - a_t)(c_s - c_t) \\ = \; & (0-0)^2 - 4(s-t)(-ns^{\sigma} + nt^{\sigma}) \\ = \; & 4n(s-t)(s^{\sigma} - t^{\sigma}) \\ = \; & 4n(s-t)(s-t)^{\sigma} \\ = \; & 4n(s-t)^{\sigma+1} \end{aligned}$$

Since q is odd, if $x \mapsto x^{\sigma}$ is an automorphism of $GF(q)$ then σ is odd, and so $\sigma+1$ is even.

The Kantor/Knuth semifield ovoid described on page 50 with $\tau = 1$ is the ovoid arising from the point $(0,0,0,0,1)$ of this BLT-set. Hence the associated flock is a semifield flock, and so by Theorem 6.2, all the derived flocks are isomorphic. Bader, Lunardon and Thas (1990) showed that the flock arising from the point $(1,0,0,0,0)$ is isomorphic to the original flock, and so all flocks arising from this BLT-set are isomorphic semifield flocks. The generalised quadrangle arising was first given by Kantor (1986) in the group coset geometry model, before the connections with ovoids and translation planes were known. Note that equivalent BLT-sets arise from different field automorphisms σ, γ exactly when $\gamma = \sigma^{\pm 1}$.

$$|P\Gamma O(5,q)_{\mathcal{P}}| = \begin{cases} 2h(q-1)q(q+1), & \sigma^2 \neq 1; \\ 4h(q-1)q(q+1), & \sigma^2 = 1 \neq \sigma. \end{cases}$$

Theorem 6.8 (Thas (1987)). *If all planes of a nonlinear flock $\mathcal{F}$ intersect in a common point, then $\mathcal{F}$ arises from a Kantor/Knuth semifield BLT-set.*

Let $\mathcal{P}$ be the Kantor/Knuth semifield BLT-set arising from the q-clan above. Then the point common to all planes of the flock $\mathcal{F}$ arising from the point $(0,0,0,0,1)$ of $\mathcal{P}$ is the point $P=(0,0,1,0,0)$, which is not on $Q(4,q)$. Since P lies on every plane of $\mathcal{F}$, every point of $\mathcal{P}$ will lie in the polar hyperplane H of P. Hence we have the following corollary.

Corollary 6.5. *The points of a Kantor/Knuth semifield BLT-set span a hyperplane of $PG(4,q)$ meeting $Q(4,q)$ in a hyperbolic quadric $Q^+(3,q)$.*

The Kantor monomial BLT-sets

For q odd and $q \equiv \pm 2 \pmod 5$:

$$\mathbf{C} = \left\{ \begin{pmatrix} t & \frac{5}{2}t^3 \\ \frac{5}{2}t^3 & 5t^5 \end{pmatrix} : t \in GF(q) \right\}$$

$$\begin{aligned}
& (b_s-b_t)^2 - 4(a_s-a_t)(c_s-c_t) \\
= \;& (5s^3-5t^3)^2 - 4(s-t)(5s^5-5t^5) \\
= \;& 25(s-t)^2(s^2+st+t^2)^2 - 20(s-t)^2(s^4+s^3t+s^2t^2+st^3+t^4) \\
= \;& (s-t)^2(5s^4+30s^3t+55s^2t^2+30st^3+5t^4) \\
= \;& 5(s-t)^2(s^2+3st+t^2)^2
\end{aligned}$$

Since $q \equiv \pm 2 \pmod 5$, 5 is a nonsquare in $GF(q)$.

The Kantor monomial q-clan on page 52 with q odd is the q-clan given here. Bader, Lunardon and Thas (1990) showed that the flocks arising from the points $(0,0,0,0,1)$ and $(1,0,0,0,0)$ of this BLT-set are isomorphic, and that the remaining $q-1$ flocks are also pairwise isomorphic. This was done by considering the associated translation planes, which Bader (1988) [6] shows are equivalent to the planes of Narayana Rao, Satyanarayana and Vithal Rao (1987) in the case $q \not\equiv 0 \pmod 3$. The translation planes are also related to some planes of Cohen and Ganley (1984) and of Barriga (1987). Both Johnson (1992) and Payne (1992) then showed that indeed the remaining $q-1$ derived flocks were not isomorphic with the first two flocks, and so exactly two classes of nonisomorphic flocks arise from this BLT-set.

$$|P\Gamma O(5,q)_{\mathcal{P}}| = \begin{cases} 2h(q-1), & q>13; \\ 48, & q=13; \\ 384, & q=7; \\ 192, & q=3. \end{cases}$$

The Kantor likeable BLT-sets

For $q = 5^h$ and n a fixed non-square of $GF(q)$:

$$\mathbf{C} = \left\{ \begin{pmatrix} t & 3t^2 \\ 3t^2 & n^{-1}t + 2t^3 + nt^5 \end{pmatrix} : t \in GF(q) \right\}$$

$$\begin{aligned} & (b_s - b_t)^2 - 4(a_s - a_t)(c_s - c_t) \\ = \quad & (s^2 - t^2)^2 - 4(s - t)(n^{-1}s + 2s^3 + ns^5 - n^{-1}t - 2t^3 - nt^5) \\ = \quad & (s - t)^2(s + t)^2 - 4n^{-1}(s - t)^2(1 + 2n(s^2 + st + t^2) \\ & +n^2(s^4 + s^3t + s^2t^2 + st^3 + t^4)) \\ = \quad & n^{-1}(s - t)^2(-4 + n(-7s^2 - 6st - 7t^2) - 4n^2(s^4 + s^3t + s^2t^2 + st^3 + t^4)) \\ = \quad & n^{-1}(s - t)^2(1 - 2n(s^2 - 2st + t^2) + n^2(s^4 + s^3t + s^2t^2 + st^3 + t^4)) \\ = \quad & n^{-1}(s - t)^2(1 - 2n(s - t)^2 + n^2(s - t)^4) \\ = \quad & n^{-1}(s - t)^2(1 - n(s - t)^2)^2 \end{aligned}$$

The Kantor likeable translation plane on page 47 is the translation plane corresponding to the flock arising from the point $(0, 0, 0, 0, 1)$ of this BLT-set. Hence this flock is likeable, and so by Theorem 6.2, all the derived flocks are isomorphic. Bader, Lunardon and Thas (1990) showed that in fact the derived flocks were not isomorphic to the original flock, and so exactly two classes of nonisomorphic flocks arise from this BLT-set.

$$|P\Gamma O(5, q)_{\mathcal{P}}| = \begin{cases} 2hq, & q > 5; \\ 720, & q = 5. \end{cases}$$

The Ganley semifield BLT-sets

For $q = 3^h$ and n a fixed nonsquare of $GF(q)$:

$$\mathbf{C} = \left\{ \begin{pmatrix} t & -t^3 \\ -t^3 & -nt - n^{-1}t^9 \end{pmatrix} : t \in GF(q) \right\}$$

$$\begin{aligned}
& (b_s - b_t)^2 - 4(a_s - a_t)(c_s - c_t) \\
= \; & (s^3 - t^3)^2 - 4(s-t)(-ns - n^{-1}s^9 + nt + n^{-1}t^9) \\
= \; & (s-t)^2(s^2+st+t^2)^2 \\
& +4n^{-1}(s-t)^2(n^2 + s^8 + s^7t + s^6t^2 + s^5t^3 + s^4t^4 + s^3t^5 + s^2t^6 + st^7 + t^8) \\
= \; & n^{-1}(s-t)^2(4n^2 + n(s^2+st+t^2)^2 \\
& +4(s^8 + s^7t + s^6t^2 + s^5t^3 + s^4t^4 + s^3t^5 + s^2t^6 + st^7 + t^8)) \\
= \; & n^{-1}(s-t)^2(n^2 - 2n(s^2+st+t^2)^2 \\
& +(s^8 + s^7t + s^6t^2 + s^5t^3 + s^4t^4 + s^3t^5 + s^2t^6 + st^7 + t^8)) \\
= \; & n^{-1}(s-t)^2(n - (s^2+st+t^2)^2)^2
\end{aligned}$$

The plane coordinatised by the Ganley semifield on page 31 is the translation plane corresponding to the flock arising from the point $(0,0,0,0,1)$ of this BLT-set. Hence this flock is semifield, and so by Theorem 6.2, all the derived flocks are isomorphic. Both Payne and Thas (1991) [99] and Johnson, Lunardon and Wilke (1991) showed that in fact the derived flocks were not isomorphic to the original flock, and so exactly two classes of nonisomorphic flocks arise from this BLT-set. In particular, the derived flocks are not semifield.

$$|P\varGamma O(5,q)_{\mathcal{P}}| = \begin{cases} 2hq, & q > 27; \\ 648, & q = 27; \\ 5760, & q = 9; \\ 192, & q = 3. \end{cases}$$

6.3.1 An alternative model of $Q(4,q)$ As mentioned above, there exist two further infinite families of BLT-sets. The family of flocks due to Fisher (Fisher and Thas (1979)) can be described in a number of different ways, though these are all somewhat involved. In particular, the explicit description in terms of q-clans, due to Payne (1988), can be given as follows.

For all odd q, let ζ be a primitive element of $GF(q^2)$, so $\omega = \zeta^{q+1}$ is a primitive element of $GF(q)$ and hence a nonsquare of $GF(q)$. Put $i = \zeta^{(q+1)/2}$, so $i^2 = \omega$, $i^q = -i$. Put $z = \zeta^{q-1} = a + bi$, so z has order $q+1$ in the multiplicative group of $GF(q^2)$. Then the matrices A_t of the q-clan $\mathcal{C}$ are given by:

$$A_t = \begin{bmatrix} t & 0 \\ 0 & -\omega t \end{bmatrix}$$

for those $t \in GF(q)$ with $t^2 - 2(1+a)^{-1}$ a square in $GF(q)$, and the other matrices are those of the form

$$A_t = \begin{bmatrix} -a_{2j} & b_{2j} \\ b_{2j} & -\omega a_{2j} \end{bmatrix}$$

for $0 \le j \le (q-1)/2$ and with

$$a_k = (z^{k+1} + z^{-k})/(z+1)$$

$$b_k = i(z^{k+1} - z^{-k})/(z+1).$$

Recall from Section 3.1 that the Fisher flocks have been characterised as follows.

Theorem 6.9 (Payne and Thas (1991) [99]). *If $\mathcal{F}$ is a nonlinear flock of the quadratic cone for which $\frac{q-1}{2}$ of the planes of $\mathcal{F}$ intersect in a common line, then $\mathcal{F}$ is a Fisher flock.*

Let $\mathcal{F}$ be a flock of Fisher type of the quadratic cone $\mathcal{K}$ embedded in $Q(4,q)$, and let $\mathcal{P}$ be the associated BLT-set. Then $\frac{q-1}{2}$ of the planes of $\mathcal{F}$ meet in a common line l, which is exterior to $Q(4,q)$. Hence the $\frac{q-1}{2}$ points of $\mathcal{P}$ corresponding to these planes lie on the plane $\pi = l^\perp$, which also contains the vertex of $\mathcal{K}$. Now π intersects $Q(4,q)$ in a conic, which is a classical BLT-set since the polar line of π is an external line, and so $\frac{q+1}{2}$ of the points of a Fisher BLT-set meet some classical BLT-set. By the characterisation of Payne and Thas (1991) above, the Fisher BLT-set is the only BLT-set meeting a classical BLT-set in $\frac{q+1}{2}$ points.

Bader (1990) and Payne and Thas (1991) [99] showed that all flocks derived from a Fisher flock are equivalent to a Fisher flock, and so the associated BLT-set is transitive, that is, the stabiliser of the Fisher BLT-set in $P\Gamma O(5,q)$ acts transitively on the set of points of the BLT-set. From Payne (1992) and our computer calculations discussed above, the order of the stabiliser of a Fisher BLT-set is

$$|P\Gamma O(5,q)_{\mathcal{P}}| = \begin{cases} 2h(q+1)^2, & q > 7; \\ 384, & q = 7; \\ 720, & q = 5; \\ 192, & q = 3. \end{cases}$$

Payne (1988) also showed that the translation planes of Baker and Ebert (1988) correspond to some of the translation planes arising from the Fisher flocks.

We now present an alternative model of $Q(4,q)$ which was introduced by Penttila (1998). Within this model Penttila describes the classical BLT-sets, the Fisher-Thas/Walker/Kantor BLT-sets and the Fisher BLT-sets, and also gives a new family of BLT-sets. We will give a proof that the Fisher BLT-sets presented are indeed those arising from the flocks of Fisher (Fisher and Thas (1979)), and present the new family of examples due to Penttila (1998).

Let $V = \{(x,y,a) : x,y \in GF(q^2), a \in GF(q)\}$, considered as a vector space of rank 5 over $GF(q)$, q odd. Define the following maps

$$\begin{gathered}
\text{-} : GF(q^2) \to GF(q^2) \text{ by } \bar{x} = x^q \ \forall x \in GF(q^2) \\
\mathrm{N} : GF(q^2) \to GF(q) \text{ by } \mathrm{N}(x) = x\bar{x} \ \forall x \in GF(q^2) \\
\mathrm{T} : GF(q^2) \to GF(q) \text{ by } \mathrm{T}(x) = x + \bar{x} \ \forall x \in GF(q^2) \\
Q : V \to GF(q) \text{ by } Q(x,y,a) = \mathrm{N}(x) + \mathrm{N}(y) + a^2 \ \forall (x,y,a) \in V \\
f : V \times V \to GF(q) \text{ by } f((x_1,y_1,a_1),(x_2,y_2,a_2)) = \mathrm{T}(x_1\bar{x_2}) + \mathrm{T}(y_1\bar{y_2}) + 2a_1a_2 \\
\forall (x_1,y_1,a_1),(x_2,y_2,a_2) \in V
\end{gathered}$$

so that $-$ is conjugation, N is the relative norm, T is the relative trace, and Q is a non-degenerate quadratic form on V which polarises to the bilinear form f. Thus

$$\mathcal{Q}_1 = \{\langle (x,y,a) \rangle | Q(x,y,a) = 0\}$$

is a parabolic quadric of the projective space $\mathrm{PG}(4,q)$ arising from V.

The classical BLT-sets are of the form $\{\langle (x,0,1)\rangle : x \in GF(q^2),\ \mathrm{N}(x) = -1\}$.

Before presenting the Fisher BLT-sets, we make some useful observations.

(1) $\mathrm{T}(\alpha^2) = \mathrm{T}(\alpha)^2 - 2\mathrm{N}(\alpha)$ $\forall \alpha \in GF(q^2)$, since $\mathrm{T}(\alpha)^2 = (\alpha+\bar{\alpha})^2 = \alpha^2 + \bar{\alpha}^2 + 2\alpha\bar{\alpha} = \mathrm{T}(\alpha^2) + 2\mathrm{N}(\alpha)$

(2) $\mathrm{T}(\alpha^2) - 2 = \boxtimes$ $\forall \alpha \in GF(q^2)$ with $\mathrm{N}(\alpha) = 1$ and $\alpha \neq \pm 1$, since, by (1), $\mathrm{T}(\alpha^2) - 2 = \mathrm{T}(\alpha)^2 - 4$, which is the discriminant of the minimal polynomial $x^2 - \mathrm{T}(\alpha)x + 1$ of α, which is a non-square, as the only elements of $GF(q)$ of norm 1 are ± 1.

(3) Since V is the orthogonal direct sum of $\{(x,0,0)|x \in GF(q^2)\}$, $\{(0,y,0)|y \in GF(q^2)\}$ and $\{(0,0,a)|a \in GF(q)\}$, the discriminant of Q is the product of the discriminants of Q restricted to these subspaces. The first two subspaces are isometric, and so have the same discriminant, whereas the discriminant of Q restricted to the third subspace is clearly 2. Hence $\mathrm{disc}(Q) = 2\square$.

Example (The Fisher BLT-sets) For any odd q, fix $\beta \in GF(q^2)$ with $\beta \neq 1$, $\mathrm{N}(\beta) = -1$. Let

$$\mathcal{P} = \{\langle(\beta x^2, 0, 1)\rangle | \mathrm{N}(x) = 1\} \cup \{\langle(0, \beta y^2, 1)\rangle | \mathrm{N}(y) = 1\}.$$

Then $\mathcal{P}$ is a BLT-set of $\mathcal{Q}_1$, due to Fisher (Fisher-Thas (1979)). We prove this as follows.

Define $\mathcal{P}_1 = \{\langle(\beta x^2, 0, 1)\rangle | \mathrm{N}(x) = 1\}$ and $\mathcal{P}_2 = \{\langle(0, \beta y^2, 1)\rangle | \mathrm{N}(y) = 1\}$. Then $Q(\beta x^2, 0, 1) = \mathrm{N}(\beta)\mathrm{N}(x^2) + 1 = 0$ and $Q(0, \beta y^2, 1) = \mathrm{N}(\beta)\mathrm{N}(y^2) + 1 = 0$, so $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2 \subseteq \mathcal{Q}_1$ of size $q + 1$.

Let $\langle v\rangle = \langle(\beta x_1^2, 0, 1)\rangle$, $\mathrm{N}(x_1) = 1$ and $\langle w\rangle = \langle(\beta x_2^2, 0, 1)\rangle$, $\mathrm{N}(x_2) = 1$ be distinct points of $\mathcal{P}_1$. Then $f(v, w) = f((\beta x_1^2, 0, 1), (\beta x_2^2, 0, 1)) = \mathrm{T}(-x_1^2 \bar{x_2}^2) + 2 = -\mathrm{T}(x_1^2 \bar{x_2}^2) + 2$. Let $\alpha = x_1 \bar{x_2}$. Then $\mathrm{N}(\alpha) = 1$. Since $\langle v\rangle \neq \langle w\rangle$, $\alpha^2 \neq 1$. By (2), $\mathrm{T}(\alpha^2) - 2 = \boxtimes$, and so we have $f(v, w) = -\boxtimes$ for any two distinct points of $\mathcal{P}_1$. Similarly for $\mathcal{P}_2$. Clearly, if $\langle v\rangle$ is a point of $\mathcal{P}_1$ and $\langle w\rangle$ is a point of $\mathcal{P}_2$, then $f(v, w) = 2$. Hence for any three distinct points $\langle u\rangle, \langle v\rangle, \langle w\rangle$ in $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$, we have

$$f(u, v) f(u, w) f(v, w) = -\boxtimes\,.$$

By (3), the discriminant of Q equals $2\square$, and so by Corollary 6.2, $\mathcal{P}$ is a BLT-set of $\mathcal{Q}_1$. Since $\mathcal{P}$ meets the classical BLT-set given above in exactly $\frac{q+1}{2}$ points, by Theorem 6.9 we have that $\mathcal{P}$ is equivalent to a BLT-set of Fisher.

The maps $(x, y, a) \mapsto (y, x, a)$, $(x, y, a) \mapsto (\lambda^2 x, y, a)$ $(\mathrm{N}(\lambda) = 1)$ and $(x, y, a) \mapsto (x, \lambda^2 y, a)$ $(\mathrm{N}(\lambda) = 1)$ are isometries of (V, Q) stabilising $\mathcal{P}$. Furthermore, they act transitively on $\mathcal{P}$, and so we see clearly that all flocks derived from a Fisher flock are again Fisher flocks, as shown by Bader (1990) and Payne and Thas (1991) [99].

We now present the family of BLT-sets given by Penttila (1998). A proof that they are indeed new BLT-sets appears in that paper. They had not been previously described in any of the associated models.

Example (The Penttila BLT-sets) For $q \equiv \pm 1 \pmod{10}$, fix $\beta, \gamma \in GF(q^2)$ with $\mathrm{N}(\beta) = -\frac{4}{5}$ and $\mathrm{N}(\gamma) = -\frac{1}{5}$. Let

$$\mathcal{P} = \{\langle(\beta x^2, \gamma x^3, 1)\rangle | \mathrm{N}(x) = 1\}.$$

Then $\mathcal{P}$ is a BLT-set of $\mathcal{Q}_1$ due to Penttila (1998).

If λ is an element of $GF(q^2)$ of order $q + 1$ with $\mathrm{N}(\lambda) = 1$, the cyclic group of order $q + 1$ defined by the isometry $(x, y, a) \mapsto (\lambda^2 x, \lambda^3 y, a)$ of (V, Q) stabilises $\mathcal{P}$. In fact, this group acts regularly on $\mathcal{P}$, and so there is only one equivalence class of flocks arising. The full group of this example has not yet been calculated.

Searching for BLT-sets

We have now seen that BLT-sets provide a general model for studying flocks of the quadratic cone and their associated geometries over fields of odd characteristic. Indeed, one BLT-set may give rise to a number of nonisomorphic flocks, each of which gives rise to a linespread of $\mathrm{PG}(3, q)$ via the Thas/Walker construction, as well as a number of linespreads via the associated regular hyperbolic fibrations. Each of these linespreads then admits a number of infinite families of linespreads via the construction of Hiramine, Matsumoto and Oyama. Hence a single BLT-set can give rise to many infinite families of translation planes of order q^2 and dimension two over their kernel. As we have seen, only the generalised quadrangle model can provide as general a setting as that of BLT-sets. An added feature of the BLT-set model is that it is embedded in projective space, unlike the GQ model. These observations are particularly relevant with respect to the central goal of this project, which is to search for new examples of these interconnected structures using a computer.

As well as the infinite families of BLT-sets described in the previous chapter, we saw earlier the q-clan of Bader, Lunardon and Pinneri for $q = 243$, arising from the translation ovoid of Penttila and Williams. There exist further individual examples of BLT-sets, not yet belonging to infinite families, which have also been found with the use of computers. De Clerck and Herssens (1992) used the computer algebra packages CAYLEY and GAP to construct flocks of the quadratic cone, finding one example for $q = 11$, one example for $q = 16$, two examples for $q = 17$, related by derivation, and two examples for $q = 23$, also related by derivation. Penttila and Royle (1998) then extended these searches by considering the more general setting of BLT-sets, and using back-track algorithms with the collinearity graph of $Q(4, q)$ as a GQ, found one example for $q = 17$, three examples for $q = 19$, four examples for $q = 23$ and two examples for $q = 25$. These new BLT-sets gave rise to 26 new flocks. An unpublished result of De Clerck and Penttila (1997) described a further example of a flock for $q = 47$.

One of the most important reasons for attempting to describe individual examples of BLT-sets (or flocks or GQs or translation planes) is the possibility of constructing infinite families by way of analysis of these examples. Indeed, the example of De Clerck and Herssens (1992) for $q = 11$, denoted by them as $DCHT(11)$, was generalised to an infinite family of partial flocks of size 11 for any $q \equiv -1 \bmod 12$ in a computerfree construction by Thas, Herssens and De Clerck (1993). Furthermore, the BLT-set arising from the flock $DCHT(11)$ and the example of Penttila and Royle (1998) for $q = 19$ with a group of order 40 are examples of the infinite family of BLT-sets of Penttila (1998) in Section 6.3.1. The wealth of existing data suggests the possibility of more infinite families, and yet any new family discovered may only contain one or two of these existing examples. Thus we feel that continuing these sorts of experimental searches, in particular, continuing past the field of order 25 where Penttila and Royle left off, is of worthwhile value. Hence the main aim of this thesis is to search for new examples of BLT-sets using a computer. Advances in both theoretical and computational aspects of this problem have made this a viable possibility, and in this chapter we discuss the ideas behind these searches.

Note that, although thorough, the searches are in no sense complete, and so we make no claim towards classification in any particular case. Currently, BLT-sets have been classified for $q \leq 17$, by various authors. Thas (1987) proved that for $q = 3$ there arises only the linear flock, and hence only the classical BLT-set. For $q = 5$ and $q = 7$, De Clerck, Gevaert and Thas (1988) proved there is exactly one nonlinear flock, and so there is exactly one nonclassical BLT-set, equivalent to the example of Fisher. For $q = 9$, Mylle (1991) showed with the use of a computer that there exist exactly two nonlinear flocks, and so there exist two nonclassical BLT-sets, equivalent to the Fisher example and to the Kantor/Knuth semifield example. De Clerck and Herssens (1992) used a computer to show that there exist exactly three nonlinear flocks for $q = 11$, giving rise to the BLT-sets of Fisher, Fisher-Thas-Walker/Kantor and Penttila($DCHT(11)$). Finally, Penttila and Royle (1998) classified BLT-sets using a computer for $q = 13$ and $q = 17$, showing that there exist exactly two and five nonclassical BLT-sets in each respective case. A future paper by Penttila and the present author classifies BLT-sets for $19 \leq q \leq 29$ using a computer.

7.1 Search techniques

The techniques for searching for BLT-sets which we shall discuss here are different to those of the earlier searches mentioned above, and have been implemented using the computer algebra system MAGMA [32]. Here we discuss only some of the generic concepts relevant to these searches, which also have the potential to be used in different situations, that is, for searching for different structures. Note that a great deal of time can be spent in any particular case experimenting (or "playing around") with the structures and the spaces they live in, determining the feasibility of various approaches.

The techniques used by Penttila and Royle (1998) involved computing the automorphism groups of the generalised quadrangles $Q(4,q)$ for $q \leq 25$, which we have seen are known to be $P\Gamma O(5,q)$. In terms of computer time, this was by far the most expensive part of their work. As a result of recent upgrades, MAGMA now has $PGO(5,q)$ for $q \leq 97$ implemented in it as a permutation group acting on the points of the associated parabolic quadric $Q(4,q)$. It is a trivial matter to extend these groups to the full groups $P\Gamma O(5,q)$ necessary for the searches.

The theme of our searches is the use of nontrivial symmetry hypotheses. This involves the choice of a subgroup H of $P\Gamma O(5,q)$ and the determination of all BLT-sets that are H-invariant. Since we are only interested in BLT-sets up to equivalence, we are only interested in conjugacy classes of subgroups. Such a search determines, up to equivalence, all BLT-sets with stabiliser containing a conjugate of H. The weakest nontrivial symmetry hypothesis is to use a minimal subgroup of $P\Gamma O(5,q)$. The minimal subgroups of a finite group - the atoms of the lattice of subgroups - are the subgroups of prime order. So our basic philosophy is to loop through the primes p dividing $|P\Gamma O(5,q)|$ in descending order of magnitude, take one representative H of each conjugacy class of subgroups of $P\Gamma O(5,q)$ of order p, and determine all BLT-sets that are H-invariant. This "prime-at-a-time" technique has previously been used for hyperovals by O'Keefe and Penttila (1992) and Penttila and Royle (1995).

The determination of all BLT-sets admitting a subgroup H is achieved by enlarging BLT-sets to the hereditary class of partial BLT-sets and then stitching together H-orbits. Namely a graph with vertices H-orbits that are partial BLT-sets and edges pairs of vertices with union a partial BLT-set is (perhaps only conceptually) formed. Every BLT-set is a clique of this graph with union of the vertices containing $q+1$ points of $Q(4,q)$, although not every such clique need be a BLT-set.

Finally, using the results on discriminants of Bader, O'Keefe and Penttila (submitted) in Section 6.1, we have available a computationally inexpensive and easily implemented check for determining if a set of points of $Q(4,q)$ is a partial BLT-set. The significance of these results is that we may test a set of points for being a partial BLT-set by performing a simple field calculation on all triples in the set containing a chosen element of the set, instead of having to test collinearity of all points of $Q(4,q)$ with each point of the set. This plays a major role in making these searches successful.

As mentioned above, our searches are not considered to be complete in any particular case. For, although in theory we know how to determine up to equivalence all BLT-sets with nontrivial stabiliser, in practice this is sometimes not feasible. Thus we do not always determine the BLT-sets up to equivalence, nor determine all conjugacy classes of subgroups to work with. Instead, we often only work up to certain invariants, such as the order of the stabiliser or number of fixed points of elements of the subgroup, which we find appealing or are inexpensive to compute. Furthermore, small primes, particularly 2 and 3, are often beyond our means, and so a selection of subgroups properly containing such subgroups is chosen as an alternative. Note however, that by Sylow's theorem, the conjugacy classes of subgroups of prime order p are all represented within a single Sylow p-subgroup.

In the following, the code fragments presented are by no means the most efficient, but merely for instructive purposes as examples of the MAGMA syntax.

When we call the projective general orthogonal group $PGO(5,q)$ of five dimensions over the Galois field of order $q = p^h$, MAGMA indexes the points of the parabolic quadric $Q(4,q)$ and computes $PGO(5,q)$ as a permutation group acting on this set of indices. We label the field, group and indexed set `I` as follows :

```
> q:=p^h;
> F:=GaloisField(q);
> G,I:=ProjectiveGeneralOrthogonalGroup(5,F);
```

We remark that `I` is a sequence of q^3+q^2+q+1 points of $\mathrm{PG}(4,q)$, each represented by a (homogeneous) 5-tuple from $GF(q)$, normalised so that the leftmost nonzero coordinate is a 1.

The quadratic form used by MAGMA to represent $Q(4,q)$ is

$$Q(x) = x_1x_5 + x_2x_4 + \frac{1}{4}x_3^2$$

(up to a scalar multiple). This can be verified by the following code :

```
> Q:=func<x|F!(x[1]*x[5]+x[2]*x[4]+x[3]^2/4)>;
> for i:=1 to #I do
>  if Q(I[i]) ne 0 then print i;end if;
> end for;
```

and observing no output occurring. (This does not seem to be documented in the manual for MAGMA.)

The full group of the quadric $Q(4,q)$ is the projective semilinear orthogonal group $P\Gamma O(5,q)$, which for prime order fields is equivalent to $PGO(5,q)$. In general, we can construct $P\Gamma O(5,q)$ by forming the subgroup of the symmetric group on the set of indices generated by $PGO(5,q)$ and a field automorphism, namely, the Frobenius automorphism $x \mapsto x^p$.

```
> V:=VectorSpace(F,5);
> a:=[];
> for i:=1 to #I do x:=I[i];
>  Append(~a,Index(I,V![x[1]^p,x[2]^p,x[3]^p,x[4]^p,x[5]^p]));
> end for;
> PGammaO:=sub<Sym(#I)|G,a>;
```

To determine if a set of points of $Q(4,q)$ is a partial BLT-set, we implement the results on discriminants of Bader, O'Keefe and Penttila (submitted) in Section 6.1. This can be done as follows :

```
> Q:=func<x|x[1]*x[5]+x[2]*x[4]+x[3]^2/4>;
> f:=func<x,y|Q(x+y)-Q(x)-Q(y)>;

> d:=((q-1) div 2);
> blt:=function(X);
>  if #X ge 3 then x:=Random(X);
>   for y in X diff {x} do flag:=true;
>    for z in X diff {x,y} do
>     flag:=(-4*f(I[x],I[y])*f(I[x],I[z])*f(I[y],I[z]))^d eq F!(-1);
>     if not flag then break;end if;
>    end for;
>    if not flag then break;end if;
>   end for;
>   return flag;
>  else return true;
>  end if;
> end function;
```

Our basic pattern of searching is for each prime p dividing $|P\Gamma O(5,q)|$ to compute a Sylow p-subgroup of $P\Gamma O(5,q)$

```
> P:=Sylow(PGammaO,p);
```

loop over the elements of P of order p

```
> list:={};
> for g in P do
>  if Order(g) eq p then
>   H:=sub<P|g>; FP:=Fix(H);
>   if not done(H,list) then
>     O:=Orbits(H);
>     cand:={i:i in {1..#O}|blt(O[i])};
>     c:={i:i in cand|#O[i] eq p};
>     edges:={{i,j}:i in c,j in c|i lt j and blt(O[i] join O[j])};
>     Gamma:=Graph<c|edges>;
>     d:=((q+1-#FP) div p)+1;e:=(q+1) div p;
>     for k:=d to e do
>      Cl:=AllCliques(Gamma,k);
>      for j:=1 to #Cl do Y:={};
>       for k in {x:x in c|VertexSet(Gamma)!x in Cl[j]} do
>        Y:=Y join O[k];
>       end for;
>       for X in Subsets(FP,(q+1)-k*p) do
>        if blt(Y join X) then
>         PrintFile(``bltsets'',Y join X);list:=list join {H};
>        end if;
>       end for;
>      end for;
>     end for;
>   end if;
>  end if;
> end for;
```

and provided that the subgroup H it generates has not already been dealt with up to conjugacy, calculate and write all H-invariant BLT-sets to a file. Here the function for testing whether a subgroup has already been dealt with can be implemented as follows :

```
> done:=function(H,list);
>  flag:=false;
>  for X in list do flag:=IsConjugate(PGammaO,H,X);
>   if flag then break;end if;
>  end for;
>  return flag;
> end function;
```

In the interest of efficiency, not all of these computations need be performed. For instance, conjugacy testing need only be performed if (cheap) invariants indicate the subgroups may be conjugate, and normalisers may be used to not have to calculate all H-invariant BLT-sets, reducing, in the process, the size of the cliques that need to be computed.

Finally, we must have some way of determining whether a BLT-set that is discovered is in fact new. For most of the searching done the order of the stabiliser of the BLT-set in $P\Gamma O(5,q)$ was used.

```
> GB:=Stabiliser(PGammaO,B);
```

This proved to be a reasonably effective test in most cases, though it should be noted that it was not always sufficient, and stricter testing was sometimes required; for example, comparing the order and number of fixed points of elements of the stabilisers. Indeed, this is how the new example for $q = 37$ with group order 72 was discovered to be different from the Kantor monomial example, which also has order 72 for $q = 37$. This highlights the fact that our searches have been far from exhaustive, and that possibly some new examples were overlooked during searching because they had the same group orders as known examples. Other more complex invariants could be used, including an adaptation of the conic invariant of Williams (1998). However, these simple invariants are enough to distinguish the examples presented in the following chapter.

The new BLT-sets

In this chapter we present the new examples arising from the searches discussed in the previous chapter, along with some new examples discovered by other ad hoc searches. The results of the searches are summarised in the following table, along with the known examples not yet belonging to an infinite family. The group order listed is that of the stabiliser of the BLT-set in $P\Gamma O(5,q)$, and the orbit structure is listed as a multiset, so, e.g., $\{4^2, 8^3\}$ indicates that there are two orbits of length 4 and three of length 8. As we saw earlier, the number of orbits of the stabiliser of a BLT-set in $P\Gamma O(5,q)$ on the BLT-set is equal to the number of nonisomorphic flocks arising from the BLT-set, and so we list this number explicitly in the final column of the table.

We abbreviate the attributions discussed in the previous chapter as follows :

DCH - De Clerck and Herssens (1992)
DCP - De Clerck and Penttila (1997)
PR - Penttila and Royle (1998)
PW/BLP - Penttila and Williams (2000) / Bader, Lunardon and Pinneri (1999)

For $q = 27$ we find one new example, for $q = 29$ five new examples, for $q = 31$ five new examples, for $q = 37$ three new examples, for $q = 41$ three new examples, for $q = 43$ one new example, for $q = 47$ two new examples, for $q = 49$ two new examples, for $q = 53$ two new examples, for $q = 59$ three new examples, for $q = 71$ one new example, for $q = 83$ one new example, for $q = 89$ one new example, and for $q = 125$ one new example, all of which will be presented in the following sections.

q	Attribution	Group Order	Orbit Structure	# flocks
17	DCH	144	{12,6}	2
	PR	24	{12,6}	2
19	PR	20	{20}	1
	PR	16	$\{8^2, 2^2\}$	4
23	DCH	72	{18,6}	2
	PR	1152	{24}	1
	PR	24	{24}	1
	PR	16	$\{8^2, 4^2\}$	4
	PR	6	$\{6^3, 3^2\}$	5
25	PR	16	{16,8,2}	3
	PR	8	$\{8^3, 2\}$	4
27	New	6	$\{1^2, 2, 6^4\}$	7
29	New	720	{30}	1
	New	48	{24,6}	2
	New	8	$\{8^3, 4, 2\}$	5
	New	6	$\{6^4, 3^2\}$	6
	New	3	$\{3^{10}\}$	10
31	New	96	{24,6,2}	3
	New	10	$\{10^2, 5^2, 2\}$	5
	New	8	$\{8^3, 4^2\}$	5
	New	4	$\{4^8\}$	8
	New	4	$\{4^7, 2^2\}$	9
37	New	72	{36,2}	2
	New	4	$\{4^9, 2\}$	10
	New	4	$\{4^9, 1^2\}$	11
41	New	60	{30,12}	2
	New	24	{24,12,6}	3
	New	8	$\{8^5, 2\}$	6
43	New	4	$\{4^{11}\}$	11
47	DCP	2304	{48}	1
	New	24	$\{24^2\}$	2
	New	3	$\{3^{16}\}$	16
49	New	40	{40,10}	2
	New	20	$\{20^2, 5^2\}$	4
53	New	24	$\{24^2, 6\}$	3
	New	12	$\{12^4, 6\}$	5
59	New	120	{60}	1
	New	24	$\{24^2, 12\}$	3
	New	5	$\{5^{12}\}$	12
71	New	24	$\{24^3\}$	3
83	New	24	$\{12, 24^3\}$	4
89	New	24	$\{6, 12, 24^3\}$	5
125	New	72	$\{72, 24^2, 6\}$	4
243	PW/BLP	26730	{243,1}	2

8.1 The new examples for $q \leq 89$

In this section we present the new BLT-sets discovered for $q \leq 89$, along with the known BLT-sets not yet belonging to an infinite family. Each example is presented as a set of $q+1$ points of the nondegenerate quadric $Q(4, q)$ defined by the quadratic equation

$$Q(x) = x_1 x_5 + x_2 x_4 + x_3^2$$

and containing $\langle(0, 0, 0, 0, 1)\rangle$ and $\langle(1, 0, 0, 0, 0)\rangle$. Note that this quadratic form is different to the form used by MAGMA (see Section 7.1) and to the form used in earlier theoretical discussions (see Section 6.3). We identify each BLT-set by the order of its stabiliser in $P\Gamma O(5, q)$, with the abbreviations of attributions as above. The orbits of the stabiliser on the BLT-set are distinguished by vertical bars, reading across the table from left to right. The example X_4^{cyc} for $q = 31$ has a cyclic stabiliser, whilst X_4^{noncyc} has stabiliser isomorphic to the non-cyclic group of order 4. The example X_4^2 for $q = 37$ has two fixed points on the BLT-set, whilst X_4^0 has two fixed points not on the BLT-set.

DCH_{144}	(1, 5, 15, 2, 3)	(1, 9, 3, 5, 14)	(1, 7, 12, 9, 14)	
$q = 17$	(1, 4, 2, 13, 12)	(1, 14, 0, 1, 3)	(1, 11, 13, 16, 12)	$\vert$
	(1, 2, 14, 7, 11)	(1, 0, 0, 0, 0)	(1, 12, 3, 4, 11)	
	(1, 10, 14, 10, 10)	(1, 6, 5, 14, 10)	(1, 16, 16, 6, 5)	
	(1, 3, 10, 3, 10)	(1, 13, 15, 8, 11)	(1, 8, 1, 12, 5)	
	(1, 15, 12, 15, 5)	(0, 0, 0, 0, 1)	(1, 1, 1, 11, 5)	

PR_{24}	(1, 0, 0, 0, 0)	(1, 7, 1, 4, 5)	(1, 12, 12, 3, 7)	
$q = 17$	(1, 2, 10, 8, 3)	(1, 11, 3, 6, 10)	(1, 5, 0, 1, 12)	$\vert$
	(1, 13, 16, 10, 5)	(1, 3, 15, 14, 5)	(1, 10, 9, 13, 10)	
	(1, 8, 8, 12, 10)	(1, 9, 3, 9, 12)	(1, 15, 5, 16, 7)	
	(1, 4, 14, 7, 14)	(1, 6, 13, 5, 5)	(0, 0, 0, 0, 1)	
	(1, 14, 2, 15, 7)	(1, 1, 0, 11, 6)	(1, 16, 8, 2, 6)	

PR_{20}	(1, 0, 0, 0, 0)	(1, 1, 12, 1, 7)	(1, 14, 11, 18, 7)
$q = 19$	(1, 11, 4, 4, 16)	(1, 6, 16, 7, 6)	(1, 4, 18, 5, 17)
	(1, 9, 17, 11, 11)	(1, 5, 3, 10, 17)	(1, 18, 2, 8, 4)
	(1, 12, 16, 15, 1)	(1, 17, 13, 13, 9)	(1, 2, 3, 6, 17)
	(1, 7, 8, 14, 9)	(1, 16, 8, 9, 1)	(1, 10, 5, 12, 7)
	(1, 8, 8, 17, 9)	(1, 15, 13, 16, 9)	(1, 3, 8, 2, 6)
	(0, 0, 0, 0, 1)	(1, 13, 6, 3, 1)	

PR_{16}	(1, 3, 5, 5, 17)	(1, 6, 10, 8, 4)	(1, 17, 10, 11, 17)
$q = 19$	(1, 18, 14, 3, 16)	(1, 14, 17, 14, 9)	(1, 13, 4, 10, 6)
	(1, 0, 0, 0, 0)	(1, 9, 10, 6, 17)	(1, 1, 9, 9, 5)
	(1, 10, 5, 18, 4)	(1, 11, 1, 1, 7)	(1, 12, 9, 2, 9)
	(1, 2, 12, 13, 1)	(1, 16, 1, 4, 11)	(1, 7, 15, 17, 17)
	(0, 0, 0, 0, 1)	(1, 4, 7, 15, 5)	(1, 15, 16, 12, 1)
	(1, 8, 12, 7, 9)	(1, 5, 14, 16, 9)	

DCH_{72}	(1, 9, 11, 17, 2)	(1, 7, 3, 6, 18)	(0, 0, 0, 0, 1)
$q = 23$	(1, 16, 7, 4, 2)	(1, 22, 14, 7, 18)	(1, 21, 5, 2, 2)
	(1, 0, 0, 0, 0)	(1, 11, 8, 15, 1)	(1, 3, 17, 18, 2)
	(1, 10, 20, 22, 1)	(1, 2, 10, 1, 13)	(1, 14, 22, 8, 2)
	(1, 20, 14, 16, 13)	(1, 4, 13, 19, 8)	(1, 1, 19, 3, 4)
	(1, 18, 9, 21, 1)	(1, 6, 4, 20, 2)	(1, 17, 9, 10, 2)
	(1, 13, 10, 9, 13)	(1, 5, 1, 12, 8)	(1, 15, 3, 13, 3)
	(1, 8, 18, 5, 4)	(1, 19, 20, 14, 1)	(1, 12, 16, 11, 3)

PR_{1152}	(1, 0, 0, 0, 0)	(1, 10, 12, 7, 16)	(1, 19, 0, 12, 2)
$q = 23$	(1, 17, 4, 13, 16)	(1, 22, 13, 1, 16)	(1, 6, 19, 10, 16)
	(1, 13, 11, 16, 16)	(1, 11, 19, 18, 16)	(1, 4, 18, 2, 13)
	(1, 1, 21, 11, 8)	(1, 5, 10, 5, 13)	(1, 14, 0, 4, 13)
	(1, 15, 7, 15, 2)	(1, 18, 5, 3, 13)	(1, 3, 6, 21, 16)
	(1, 20, 9, 17, 16)	(0, 0, 0, 0, 1)	(1, 16, 17, 14, 16)
	(1, 8, 15, 9, 2)	(1, 9, 2, 8, 16)	(1, 21, 1, 20, 16)
	(1, 7, 14, 19, 16)	(1, 12, 8, 6, 2)	(1, 2, 19, 22, 9)

PR_{24}	(1, 0, 0, 0, 0)	(1, 3, 21, 11, 9)	(1, 5, 7, 16, 9)
$q = 23$	(1, 10, 0, 3, 16)	(1, 7, 4, 17, 3)	(1, 16, 16, 12, 12)
	(1, 8, 10, 9, 12)	(1, 17, 9, 6, 1)	(1, 2, 5, 18, 8)
	(1, 22, 14, 7, 18)	(1, 1, 20, 8, 6)	(1, 21, 17, 1, 12)
	(1, 14, 19, 14, 18)	(1, 9, 19, 2, 12)	(1, 20, 6, 20, 1)
	(1, 19, 21, 10, 13)	(0, 0, 0, 0, 1)	(1, 15, 3, 5, 8)
	(1, 12, 12, 22, 6)	(1, 6, 17, 15, 12)	(1, 13, 16, 13, 12)
	(1, 11, 16, 19, 18)	(1, 4, 6, 21, 18)	(1, 18, 18, 4, 18)

PR_{16}	(1, 0, 0, 0, 0)	(0, 0, 0, 0, 1)	(1, 11, 1, 18, 8)
$q = 23$	(1, 7, 7, 6, 1)	(1, 16, 21, 16, 16)	(1, 21, 16, 19, 12)
	(1, 5, 0, 2, 13)	(1, 18, 0, 21, 13)	(1, 20, 2, 17, 1)
	(1, 13, 4, 7, 8)	(1, 10, 15, 15, 16)	(1, 17, 18, 3, 16)
	(1, 12, 20, 12, 8)	(1, 1, 18, 9, 12)	(1, 14, 17, 13, 12)
	(1, 4, 5, 5, 1)	(1, 22, 21, 8, 4)	(1, 19, 18, 1, 2)
	(1, 6, 19, 20, 2)	(1, 8, 6, 4, 1)	(1, 2, 15, 10, 8)
	(1, 3, 3, 11, 4)	(1, 9, 13, 22, 1)	(1, 15, 14, 14, 8)

PR_6	(1, 8, 0, 22, 8)	(1, 5, 15, 9, 6)	(1, 11, 18, 13, 16) $\mid$
$q = 23$	(1, 17, 19, 7, 3)	(1, 1, 4, 12, 18)	(1, 4, 10, 19, 8) $\mid$
	(1, 0, 0, 0, 0)	(1, 21, 8, 15, 12)	(1, 13, 12, 10, 2)
	(1, 15, 5, 8, 16)	(1, 2, 16, 20, 3)	(1, 6, 14, 18, 18) $\mid$
	(0, 0, 0, 0, 1)	(1, 9, 9, 21, 6)	(1, 22, 22, 2, 1)
	(1, 10, 7, 5, 16)	(1, 14, 15, 6, 13)	(1, 19, 14, 16, 6) $\mid$
	(1, 18, 0, 11, 9)	(1, 20, 8, 1, 8)	(1, 7, 4, 17, 3)
	(1, 12, 8, 4, 3)	(1, 3, 18, 3, 12)	(1, 16, 4, 14, 13)

PR_{16}	$(1,w^5,w^{21},w^{17},w^5)$	$(1,w^{13},w^{17},2,w^9)$ $\mid$	$(1,2,w^{14},w^{11},w^{21})$
$q = 25$	$(1,w^{23},w^{23},w^{22},w^7)$	$(1,4,w^{16},3,w^{11})$	$(1,w^{16},1,w^7,w^9)$
$w^2 = w-2$	$(1,w^3,w^{10},w^{16},w^5)$	$(1,w,w^{13},w^{23},w^5)$	$(0,0,0,0,1)$
	$(1,w^{15},w^8,w^{15},w^7)$ $\mid$	$(1,w^8,w^8,4,w^3)$	$(1,0,0,0,0)$
	$(1,w^{10},w^{13},w^5,w^{19})$	$(1,w^9,w^9,w^4,w^{15})$	$(1,w^4,2,w^{21},w^5)$
	$(1,1,w^{15},w^{20},w^{21})$	$(1,w^7,w^5,1,w^5)$	$(1,3,w^7,w^{19},w^{23})$
	$(1,w^2,w^{15},w^2,w^9)$	$(1,w^{11},w^{21},w^3,w)$	$(1,w^{20},3,w^{13},w^7)$
	$(1,w^{22},w^{14},w,w)$	$(1,w^{21},3,w^{10},w^9)$	$(1,w^{17},w^9,w^{14},w^{11})$
	$(1,w^{19},w^7,w^9,w^5)$	$(1,w^{14},1,w^8,w^3)$	

PR_8	$(1,1,w^8,w^9,w^5)$	$(1,w^{23},w^{21},w^{21},w^{23})$ $\mid$	$(1,0,0,0,0)$
$q = 25$	$(0,0,0,0,1)$	$(1,w^8,3,w^{13},w^{11})$	$(1,w^{20},w^4,w^{14},w^{13})$
$w^2 = w-2$	$(1,w^{10},3,w^{15},w^5)$	$(1,w^3,w^{10},w^{16},w^5)$	$(1,w^{11},w^4,2,w^7)$
	$(1,3,w^2,w^{19},w^3)$ $\mid$	$(1,w^9,0,w^{22},w^{19})$	$(1,w^4,1,3,w^3)$
	$(1,w^{22},w^{10},w^{20},w^{23})$	$(1,w^{16},w^{21},w^4,w^{23})$	$(1,w^{17},w^{13},w^5,w^9)$
	$(1,w^{15},w^4,4,w^5)$	$(1,w^{19},w^{23},w,w)$	$(1,w^7,w^5,1,w^5)$ $\mid$
	$(1,2,w^8,w^8,w^{19})$	$(1,w^{14},w^5,w^{10},w)$	$(1,4,w^4,w^{17},w^3)$
	$(1,w^{13},w^{21},w^3,w^{21})$	$(1,w^5,2,w^{11},w^{23})$	$(1,w^2,4,w^7,w^{23})$
	$(1,w,w^{13},w^{23},w^5)$	$(1,w^{21},4,w^2,w^9)$	

X_6	$(0,0,0,0,1)$ $\mid$	$(1,0,0,0,0)$	$(1,w,w^{19},2,w^{20})$ $\mid$
$q = 27$	$(1,w^{14},w^6,1,w^{20})$ $\mid$	$(1,w^{20},w^{18},w^{17},w^6)$	$(1,w^{25},w^{24},w^{25},w^4)$
$w^3 = w-1$	$(1,w^3,w^6,w^{24},w^{24})$	$(1,w^{16},w^5,w^{23},w^{24})$	$(1,w^{15},w^7,w^8,w^4)$
	$(1,w^5,w^{21},w^{20},w^6)$ $\mid$	$(1,w^{24},w^5,w^{14},w^{18})$	$(1,w^7,w^2,w^{16},w^{14})$
	$(1,2,w^{12},w^{11},w^{24})$	$(1,w^{23},w^6,w^7,w^6)$	$(1,w^{17},w^3,w^{21},w^4)$
	$(1,w^{11},w^{16},w^{22},w^2)$ $\mid$	$(1,w^8,w^{24},w^{15},w^{18})$	$(1,w^{21},0,w^{12},w^{20})$
	$(1,w^{18},w^{14},w^4,w^{20})$	$(1,1,w^{22},w^{19},w^{14})$	$(1,w^2,w^7,w^{10},w^{20})$
	$(1,w^6,w^9,w^5,w^2)$ $\mid$	$(1,w^4,w^8,w^6,w^8)$	$(1,w^{19},w^{23},w^2,w^{16})$
	$(1,w^{10},w^5,w^9,1)$	$(1,w^9,w^{22},w,w^{12})$	$(1,w^{12},w^{14},w^{18},w^{10})$
	$(1,w^{22},w^5,w^3,w^{22})$		

X_{720}	(1, 26, 16, 3, 14)	(1, 0, 0, 0, 0)	(1, 20, 11, 4, 2)
$q = 29$	(1, 6, 27, 27, 8)	(1, 16, 20, 2, 3)	(1, 19, 15, 9, 10)
	(1, 10, 19, 28, 26)	(0, 0, 0, 0, 1)	(1, 9, 28, 24, 15)
	(1, 13, 9, 7, 2)	(1, 14, 11, 15, 17)	(1, 27, 24, 23, 21)
	(1, 23, 22, 16, 18)	(1, 7, 17, 6, 17)	(1, 15, 10, 25, 18)
	(1, 5, 20, 26, 21)	(1, 24, 26, 11, 17)	(1, 22, 0, 17, 3)
	(1, 3, 8, 5, 8)	(1, 8, 25, 21, 19)	(1, 2, 24, 8, 17)
	(1, 1, 0, 12, 17)	(1, 25, 27, 22, 26)	(1, 18, 8, 18, 18)
	(1, 21, 0, 20, 15)	(1, 12, 24, 14, 10)	(1, 17, 23, 19, 18)
	(1, 11, 0, 13, 2)	(1, 28, 17, 1, 2)	(1, 4, 4, 10, 2)

X_{48}	(1, 26, 24, 25, 21)	(1, 15, 3, 24, 8)	(1, 5, 14, 3, 21)
$q = 29$	(1, 18, 23, 20, 10)	(1, 3, 28, 13, 18)	(1, 14, 26, 5, 8)
	(0, 0, 0, 0, 1)	(1, 0, 0, 0, 0)	(1, 2, 23, 17, 17)
	(1, 12, 17, 18, 17)	(1, 20, 19, 7, 21)	(1, 21, 12, 27, 14)
	(1, 7, 28, 1, 21)	(1, 24, 8, 28, 18)	(1, 19, 19, 15, 21)
	(1, 11, 25, 21, 14)	(1, 25, 11, 2, 3)	(1, 13, 7, 8, 21)
	(1, 17, 18, 26, 17)	(1, 28, 19, 23, 10)	(1, 6, 18, 6, 17)
	(1, 23, 11, 11, 3)	(1, 4, 12, 4, 14)	(1, 8, 21, 12, 14)
	(1, 9, 11, 10, 21)	(1, 27, 9, 22, 21)	(1, 10, 18, 9, 21)
	(1, 22, 2, 16, 21)	(1, 16, 19, 19, 2)	(1, 1, 19, 14, 2)

X_8	(1, 18, 7, 11, 14)	(1, 15, 20, 28, 21)	(1, 13, 20, 8, 18)
$q = 29$	(1, 24, 23, 24, 26)	(1, 22, 26, 1, 27)	(1, 7, 6, 13, 18)
	(1, 0, 0, 0, 0)	(1, 16, 11, 26, 14)	(1, 27, 18, 12, 19)
	(1, 14, 23, 20, 3)	(1, 6, 5, 22, 17)	(1, 11, 10, 6, 8)
	(1, 26, 3, 2, 26)	(1, 28, 22, 23, 3)	(1, 25, 24, 25, 17)
	(1, 1, 22, 27, 11)	(1, 2, 28, 5, 18)	(1, 21, 13, 4, 8)
	(1, 5, 24, 14, 21)	(1, 10, 24, 16, 18)	(0, 0, 0, 0, 1)
	(1, 8, 25, 3, 18)	(1, 23, 15, 15, 10)	(1, 4, 10, 21, 19)
	(1, 3, 3, 10, 19)	(1, 12, 16, 7, 8)	(1, 9, 20, 18, 18)
	(1, 17, 2, 17, 26)	(1, 20, 27, 9, 19)	(1, 19, 17, 19, 17)

X_6	(1, 0, 0, 0, 0)	(1, 9, 21, 11, 11)	(1, 8, 16, 17, 14)
$q = 29$	(1, 2, 20, 28, 8)	(1, 1, 24, 1, 3)	(1, 10, 7, 26, 10)
	(1, 3, 1, 25, 11)	(1, 20, 1, 21, 14)	(1, 15, 17, 3, 14)
	(1, 14, 0, 23, 26)	(1, 21, 3, 19, 27)	(0, 0, 0, 0, 1)
	(1, 11, 28, 5, 2)	(1, 24, 1, 24, 3)	(1, 17, 4, 15, 19)
	(1, 27, 11, 4, 3)	(1, 4, 6, 10, 11)	(1, 25, 26, 22, 21)
	(1, 19, 18, 8, 17)	(1, 26, 21, 7, 15)	(1, 16, 7, 9, 10)
	(1, 5, 3, 16, 27)	(1, 22, 17, 14, 12)	(1, 23, 27, 12, 10)
	(1, 6, 16, 13, 14)	(1, 12, 15, 27, 2)	(1, 18, 5, 6, 12)
	(1, 7, 26, 18, 10)	(1, 13, 3, 20, 21)	(1, 28, 4, 2, 15)

X_3	(1, 0, 0, 0, 0)	(1, 23, 28, 3, 17)	(1, 22, 20, 12, 3) $\vert$
$q = 29$	(1, 16, 25, 7, 17)	(1, 20, 27, 9, 19)	(0, 0, 0, 0, 1) $\vert$
	(1, 2, 16, 18, 27)	(1, 19, 4, 14, 8)	(1, 8, 0, 25, 3) $\vert$
	(1, 25, 9, 16, 12)	(1, 14, 20, 11, 26)	(1, 9, 28, 26, 26) $\vert$
	(1, 6, 9, 15, 3)	(1, 12, 6, 13, 11)	(1, 27, 5, 4, 12) $\vert$
	(1, 21, 22, 1, 17)	(1, 17, 16, 24, 3)	(1, 1, 25, 2, 11) $\vert$
	(1, 13, 26, 8, 3)	(1, 18, 13, 27, 12)	(1, 11, 1, 20, 11) $\vert$
	(1, 26, 6, 19, 21)	(1, 7, 9, 17, 3)	(1, 4, 16, 5, 14) $\vert$
	(1, 15, 5, 28, 19)	(1, 5, 5, 21, 15)	(1, 28, 7, 10, 19) $\vert$
	(1, 24, 11, 22, 18)	(1, 3, 9, 6, 17)	(1, 10, 9, 23, 8)

X_{96}	(1, 0, 0, 0, 0)	(0, 0, 0, 0, 1) $\vert$	(1, 30, 30, 3, 2)
$q = 31$	(1, 1, 1, 28, 2)	(1, 6, 6, 13, 10)	(1, 5, 5, 16, 19)
	(1, 25, 25, 18, 10)	(1, 26, 26, 15, 19) $\vert$	(1, 12, 3, 1, 10)
	(1, 21, 13, 25, 19)	(1, 22, 10, 27, 19)	(1, 4, 24, 14, 19)
	(1, 3, 15, 22, 19)	(1, 16, 24, 19, 19)	(1, 28, 11, 10, 2)
	(1, 23, 2, 24, 2)	(1, 2, 13, 30, 19)	(1, 11, 28, 20, 19)
	(1, 19, 15, 6, 2)	(1, 8, 16, 21, 10)	(1, 29, 15, 5, 2)
	(1, 27, 18, 4, 2)	(1, 15, 13, 17, 10)	(1, 18, 27, 2, 10)
	(1, 7, 11, 9, 2)	(1, 24, 16, 7, 10)	(1, 14, 28, 29, 19)
	(1, 17, 19, 11, 10)	(1, 9, 18, 12, 2)	(1, 10, 3, 26, 10)
	(1, 20, 27, 8, 10)	(1, 13, 3, 23, 2)	

X_{10}	(1, 0, 0, 0, 0)	(0, 0, 0, 0, 1) $\vert$	(1, 30, 3, 18, 9)
$q = 31$	(1, 14, 14, 20, 20)	(1, 28, 17, 17, 10)	(1, 12, 10, 16, 18)
	(1, 9, 18, 22, 5) $\vert$	(1, 15, 8, 14, 5)	(1, 2, 1, 6, 18)
	(1, 11, 5, 11, 9)	(1, 24, 18, 30, 10)	(1, 10, 30, 1, 20) $\vert$
	(1, 4, 18, 7, 20)	(1, 13, 4, 10, 9)	(1, 23, 16, 21, 5)
	(1, 8, 18, 19, 20)	(1, 18, 24, 29, 18)	(1, 3, 2, 3, 18)
	(1, 25, 2, 28, 9)	(1, 19, 2, 27, 10)	(1, 26, 6, 2, 5)
	(1, 16, 1, 9, 10) $\vert$	(1, 5, 20, 25, 2)	(1, 7, 28, 4, 25)
	(1, 21, 9, 24, 4)	(1, 6, 13, 13, 1)	(1, 20, 14, 5, 14)
	(1, 17, 25, 15, 19)	(1, 1, 10, 8, 16)	(1, 29, 10, 23, 8)
	(1, 22, 14, 26, 7)	(1, 27, 12, 12, 28)	

<table>
<tr><td>X_8</td><td>(1, 0, 0, 0, 0)</td><td>(1, 29, 27, 17, 18)</td><td>(1, 5, 22, 20, 5)</td></tr>
<tr><td>$q = 31$</td><td>(1, 26, 8, 6, 28) |</td><td>(1, 8, 20, 2, 18)</td><td>(1, 27, 15, 10, 1)</td></tr>
<tr><td></td><td>(1, 21, 0, 4, 9)</td><td>(1, 9, 22, 15, 1) |</td><td>(1, 22, 7, 30, 4)</td></tr>
<tr><td></td><td>(1, 28, 14, 5, 5)</td><td>(1, 4, 24, 7, 16)</td><td>(1, 10, 3, 19, 18)</td></tr>
<tr><td></td><td>(0, 0, 0, 0, 1)</td><td>(1, 17, 23, 14, 8)</td><td>(1, 30, 26, 8, 14)</td></tr>
<tr><td></td><td>(1, 11, 12, 11, 14) |</td><td>(1, 18, 6, 27, 5)</td><td>(1, 24, 14, 13, 19)</td></tr>
<tr><td></td><td>(1, 6, 24, 29, 25)</td><td>(1, 2, 23, 25, 10)</td><td>(1, 13, 3, 23, 2)</td></tr>
<tr><td></td><td>(1, 20, 28, 1, 2)</td><td>(1, 12, 1, 12, 10)</td><td>(1, 1, 26, 21, 16) |</td></tr>
<tr><td></td><td>(1, 3, 17, 26, 5)</td><td>(1, 25, 5, 16, 9)</td><td>(1, 23, 6, 9, 5)</td></tr>
<tr><td></td><td>(1, 14, 7, 18, 9)</td><td>(1, 19, 12, 3, 16)</td><td>(1, 16, 21, 28, 10)</td></tr>
<tr><td></td><td>(1, 15, 14, 22, 1)</td><td>(1, 7, 4, 24, 2)</td><td></td></tr>
</table>

<table>
<tr><td>X_4^{cyc}</td><td>(1, 16, 1, 13, 8)</td><td>(1, 29, 12, 19, 18)</td><td>(1, 0, 0, 0, 0)</td></tr>
<tr><td>$q = 31$</td><td>(1, 14, 4, 7, 10) |</td><td>(1, 28, 15, 11, 25)</td><td>(1, 27, 27, 1, 19)</td></tr>
<tr><td></td><td>(1, 19, 11, 18, 2)</td><td>(1, 20, 4, 27, 2) |</td><td>(1, 5, 1, 5, 5)</td></tr>
<tr><td></td><td>(1, 12, 10, 4, 7)</td><td>(1, 25, 12, 6, 16)</td><td>(1, 1, 26, 2, 4) |</td></tr>
<tr><td></td><td>(1, 6, 16, 3, 5)</td><td>(1, 24, 5, 9, 7)</td><td>(1, 8, 4, 20, 10)</td></tr>
<tr><td></td><td>(1, 4, 14, 24, 18) |</td><td>(0, 0, 0, 0, 1)</td><td>(1, 9, 15, 29, 10)</td></tr>
<tr><td></td><td>(1, 3, 25, 23, 19)</td><td>(1, 7, 11, 8, 9) |</td><td>(1, 18, 23, 14, 25)</td></tr>
<tr><td></td><td>(1, 17, 18, 15, 10)</td><td>(1, 22, 18, 21, 20)</td><td>(1, 11, 25, 16, 5) |</td></tr>
<tr><td></td><td>(1, 30, 10, 26, 19)</td><td>(1, 26, 1, 30, 25)</td><td>(1, 21, 26, 25, 8)</td></tr>
<tr><td></td><td>(1, 2, 13, 17, 14) |</td><td>(1, 13, 4, 12, 14)</td><td>(1, 15, 1, 22, 10)</td></tr>
<tr><td></td><td>(1, 23, 0, 10, 18)</td><td>(1, 10, 20, 28, 2)</td><td></td></tr>
</table>

<table>
<tr><td>X_4^{noncyc}</td><td>(1, 14, 29, 2, 2)</td><td>(1, 28, 26, 18, 9) |</td><td>(1, 7, 21, 19, 28)</td></tr>
<tr><td>$q = 31$</td><td>(1, 5, 13, 3, 28) |</td><td>(1, 15, 27, 12, 2)</td><td>(1, 30, 24, 29, 9)</td></tr>
<tr><td></td><td>(1, 23, 5, 30, 9)</td><td>(1, 0, 0, 0, 0) |</td><td>(0, 0, 0, 0, 1)</td></tr>
<tr><td></td><td>(1, 18, 26, 6, 2)</td><td>(1, 4, 1, 28, 4)</td><td>(1, 21, 12, 10, 2) |</td></tr>
<tr><td></td><td>(1, 9, 22, 7, 2)</td><td>(1, 10, 28, 11, 4)</td><td>(1, 27, 23, 1, 19)</td></tr>
<tr><td></td><td>(1, 20, 15, 9, 4) |</td><td>(1, 22, 25, 15, 2)</td><td>(1, 26, 1, 16, 10)</td></tr>
<tr><td></td><td>(1, 25, 21, 25, 1)</td><td>(1, 11, 13, 5, 19) |</td><td>(1, 2, 0, 21, 20)</td></tr>
<tr><td></td><td>(1, 1, 15, 27, 2)</td><td>(1, 3, 14, 26, 28)</td><td>(1, 16, 3, 22, 10) |</td></tr>
<tr><td></td><td>(1, 8, 8, 13, 4)</td><td>(1, 29, 1, 24, 9)</td><td>(1, 6, 15, 17, 20)</td></tr>
<tr><td></td><td>(1, 13, 8, 4, 25) |</td><td>(1, 24, 0, 8, 25)</td><td>(1, 12, 25, 23, 25)</td></tr>
<tr><td></td><td>(1, 19, 8, 14, 28)</td><td>(1, 17, 5, 20, 18)</td><td></td></tr>
</table>

X_{72}	(0, 0, 0, 0, 1)		(1, 0, 0, 0, 0)	$\mid$	(1, 20, 1, 33, 5)	
$q = 37$	(1, 6, 23, 19, 23)		(1, 32, 11, 35, 17)		(1, 33, 12, 14, 23)	
	(1, 25, 8, 12, 6)		(1, 16, 6, 1, 22)		(1, 23, 8, 5, 6)	
	(1, 8, 6, 13, 8)		(1, 22, 19, 20, 13)		(1, 21, 23, 16, 23)	
	(1, 28, 6, 9, 8)		(1, 2, 26, 7, 13)		(1, 5, 9, 36, 35)	
	(1, 12, 23, 10, 17)		(1, 14, 16, 25, 23)		(1, 9, 8, 26, 35)	
	(1, 1, 11, 8, 19)		(1, 19, 12, 11, 17)		(1, 18, 27, 22, 22)	
	(1, 24, 36, 17, 35)		(1, 26, 27, 23, 5)		(1, 27, 25, 24, 22)	
	(1, 36, 21, 32, 35)		(1, 7, 16, 31, 8)		(1, 35, 5, 15, 5)	
	(1, 10, 36, 6, 13)		(1, 30, 4, 3, 5)		(1, 4, 3, 30, 19)	
	(1, 17, 13, 2, 19)		(1, 11, 28, 18, 17)		(1, 13, 16, 27, 22)	
	(1, 29, 12, 28, 6)		(1, 15, 10, 34, 19)		(1, 3, 30, 4, 13)	
	(1, 31, 9, 21, 8)		(1, 34, 9, 29, 6)			

X_4^0	(1, 9, 16, 8, 5)		(1, 13, 20, 26, 2)	$\mid$	(1, 0, 0, 0, 0)	
$q = 37$	(1, 4, 12, 14, 22)		(1, 19, 23, 5, 5)		(1, 24, 17, 19, 32)	$\mid$
	(0, 0, 0, 0, 1)		(1, 18, 18, 10, 14)		(1, 2, 4, 36, 23)	
	(1, 7, 5, 24, 29)	$\mid$	(1, 36, 20, 22, 29)		(1, 14, 10, 13, 14)	
	(1, 28, 22, 7, 23)		(1, 32, 28, 20, 19)	$\mid$	(1, 30, 27, 23, 24)	
	(1, 3, 30, 28, 15)		(1, 1, 20, 31, 13)		(1, 11, 36, 33, 6)	$\mid$
	(1, 29, 22, 30, 15)		(1, 20, 10, 4, 5)		(1, 8, 14, 32, 29)	
	(1, 25, 15, 9, 31)	$\mid$	(1, 26, 13, 18, 29)		(1, 23, 19, 6, 19)	
	(1, 35, 11, 15, 20)		(1, 22, 11, 25, 32)	$\mid$	(1, 10, 16, 2, 20)	
	(1, 17, 18, 27, 31)		(1, 15, 29, 16, 29)		(1, 31, 18, 1, 15)	$\mid$
	(1, 12, 34, 35, 15)		(1, 33, 23, 17, 20)		(1, 27, 23, 21, 14)	
	(1, 34, 22, 3, 6)	$\mid$	(1, 21, 11, 11, 18)		(1, 5, 33, 12, 35)	
	(1, 6, 22, 34, 15)		(1, 16, 31, 29, 18)			

X_4^2	(1, 3, 7, 25, 24)	$\mid$	(1, 35, 30, 32, 15)	$\mid$	(1, 0, 0, 0, 0)	
$q = 37$	(1, 4, 10, 30, 2)		(1, 14, 8, 17, 31)		(1, 30, 18, 2, 23)	$\mid$
	(0, 0, 0, 0, 1)		(1, 19, 0, 10, 32)		(1, 8, 18, 12, 24)	
	(1, 34, 2, 20, 19)	$\mid$	(1, 28, 34, 15, 15)		(1, 2, 21, 23, 31)	
	(1, 13, 29, 36, 23)		(1, 23, 13, 8, 17)	$\mid$	(1, 25, 12, 35, 17)	
	(1, 1, 14, 4, 22)		(1, 17, 2, 19, 6)		(1, 12, 17, 1, 32)	$\mid$
	(1, 27, 23, 3, 19)		(1, 20, 2, 21, 20)		(1, 33, 30, 22, 2)	
	(1, 11, 16, 31, 32)	$\mid$	(1, 29, 6, 13, 31)		(1, 16, 17, 7, 6)	
	(1, 6, 25, 14, 31)		(1, 32, 27, 29, 8)	$\mid$	(1, 15, 8, 9, 23)	
	(1, 5, 17, 24, 35)		(1, 18, 13, 33, 14)		(1, 7, 36, 26, 2)	$\mid$
	(1, 21, 34, 28, 32)		(1, 10, 22, 16, 22)		(1, 26, 34, 27, 29)	
	(1, 31, 13, 34, 35)	$\mid$	(1, 9, 13, 18, 2)		(1, 22, 28, 5, 31)	
	(1, 24, 3, 11, 23)		(1, 36, 27, 6, 17)			

X_{60}	(1, 27, 36, 26, 11)	(1, 0, 0, 0, 0)	(0, 0, 0, 0, 1)
$q = 41$	(1, 22, 11, 6, 34)	(1, 11, 40, 30, 38)	(1, 24, 20, 33, 38)
	(1, 38, 11, 3, 11)	(1, 28, 1, 1, 12)	(1, 35, 25, 31, 12)
	(1, 12, 27, 36, 28)	(1, 15, 31, 27, 28)	(1, 34, 3, 12, 34)
	(1, 32, 24, 37, 3)	(1, 26, 1, 7, 22)	(1, 30, 23, 2, 26)
	(1, 4, 2, 34, 24)	(1, 29, 29, 10, 17)	(1, 8, 32, 25, 6)
	(1, 16, 16, 22, 7)	(1, 20, 1, 28, 13)	(1, 36, 19, 29, 30)
	(1, 18, 12, 20, 29)	(1, 37, 10, 18, 13)	(1, 14, 7, 35, 35)
	(1, 33, 40, 14, 29)	(1, 9, 21, 40, 19)	(1, 40, 28, 32, 27)
	(1, 23, 26, 16, 22)	(1, 10, 20, 13, 3)	(1, 17, 16, 39, 24)
	(1, 13, 26, 38, 19)	(1, 3, 13, 21, 14)	(1, 5, 4, 8, 26)
	(1, 21, 39, 5, 14)	(1, 2, 39, 15, 7)	(1, 1, 24, 9, 30)
	(1, 19, 9, 23, 15)	(1, 31, 14, 17, 15)	(1, 25, 12, 24, 35)
	(1, 7, 32, 11, 6)	(1, 6, 8, 19, 27)	(1, 39, 27, 4, 17)

X_{24}	(1, 25, 4, 20, 17)	(1, 16, 12, 25, 30)	(1, 22, 5, 30, 12)
$q = 41$	(1, 15, 0, 8, 3)	(1, 14, 3, 39, 19)	(1, 26, 23, 2, 34)
	(1, 3, 14, 40, 12)	(1, 10, 2, 5, 28)	(1, 5, 26, 23, 29)
	(1, 37, 9, 34, 14)	(1, 39, 40, 6, 11)	(1, 13, 30, 33, 24)
	(1, 11, 22, 18, 15)	(1, 38, 34, 7, 13)	(1, 28, 24, 29, 6)
	(1, 23, 35, 17, 24)	(1, 32, 29, 19, 27)	(1, 33, 36, 4, 7)
	(1, 21, 38, 36, 14)	(1, 0, 0, 0, 0)	(1, 7, 12, 13, 11)
	(1, 20, 26, 28, 35)	(1, 27, 36, 3, 17)	(1, 24, 14, 16, 35)
	(1, 40, 24, 9, 7)	(1, 30, 17, 31, 11)	(1, 36, 6, 37, 26)
	(1, 4, 28, 21, 34)	(1, 35, 23, 15, 12)	(1, 1, 7, 14, 19)
	(1, 18, 2, 35, 22)	(1, 17, 30, 26, 11)	(1, 31, 21, 27, 34)
	(1, 34, 39, 22, 27)	(1, 2, 13, 12, 12)	(1, 9, 19, 24, 38)
	(1, 12, 8, 1, 6)	(1, 6, 25, 11, 6)	(0, 0, 0, 0, 1)
	(1, 29, 37, 38, 30)	(1, 19, 40, 32, 6)	(1, 8, 7, 10, 35)

X_8	(1, 28, 16, 28, 26)	(1, 5, 1, 25, 38)	(1, 8, 12, 30, 26)
$q = 41$	(1, 0, 0, 0, 0)	(1, 2, 27, 10, 30)	(1, 10, 32, 18, 26)
	(1, 36, 10, 32, 19)	(1, 22, 8, 21, 7)	(1, 9, 2, 9, 38)
	(1, 35, 10, 26, 15)	(1, 6, 12, 33, 27)	(0, 0, 0, 0, 1)
	(1, 37, 29, 6, 3)	(1, 24, 10, 34, 27)	(1, 13, 24, 40, 11)
	(1, 34, 15, 39, 7)	(1, 17, 22, 17, 6)	(1, 18, 13, 5, 28)
	(1, 40, 31, 31, 13)	(1, 12, 14, 3, 14)	(1, 38, 40, 22, 24)
	(1, 29, 6, 13, 38)	(1, 31, 11, 27, 26)	(1, 23, 12, 35, 35)
	(1, 26, 15, 36, 28)	(1, 30, 17, 29, 30)	(1, 39, 11, 14, 30)
	(1, 33, 35, 12, 19)	(1, 11, 24, 2, 17)	(1, 21, 33, 24, 6)
	(1, 27, 12, 20, 13)	(1, 19, 16, 11, 27)	(1, 25, 9, 16, 11)
	(1, 1, 3, 15, 17)	(1, 16, 39, 4, 14)	(1, 7, 36, 19, 6)
	(1, 3, 11, 7, 22)	(1, 4, 19, 8, 17)	(1, 15, 14, 1, 35)
	(1, 32, 21, 38, 24)	(1, 20, 15, 37, 19)	(1, 14, 10, 23, 29)

X_4	(1, 13, 23, 21, 15)		(1, 0, 0, 0, 0)		(1, 27, 39, 11, 31)	
$q = 43$	(1, 1, 7, 40, 40)	$\mid$	(1, 39, 7, 4, 10)		(1, 2, 6, 29, 35)	
	(0, 0, 0, 0, 1)		(1, 16, 8, 25, 9)	$\mid$	(1, 32, 16, 41, 23)	
	(1, 10, 6, 1, 40)		(1, 18, 37, 14, 13)		(1, 12, 27, 18, 1)	$\mid$
	(1, 3, 6, 19, 36)		(1, 20, 13, 36, 14)		(1, 26, 31, 12, 17)	
	(1, 11, 19, 37, 6)	$\mid$	(1, 40, 0, 26, 35)		(1, 42, 36, 27, 21)	
	(1, 25, 18, 2, 13)		(1, 7, 39, 23, 38)	$\mid$	(1, 34, 28, 22, 16)	
	(1, 19, 9, 7, 1)		(1, 33, 2, 24, 21)		(1, 14, 19, 10, 15)	$\mid$
	(1, 6, 21, 39, 13)		(1, 31, 3, 8, 1)		(1, 17, 35, 13, 16)	
	(1, 41, 6, 38, 40)	$\mid$	(1, 21, 27, 30, 17)		(1, 29, 14, 31, 23)	
	(1, 5, 9, 42, 10)		(1, 24, 6, 9, 6)	$\mid$	(1, 37, 35, 17, 38)	
	(1, 36, 34, 15, 24)		(1, 35, 10, 33, 35)		(1, 38, 14, 34, 17)	$\mid$
	(1, 4, 23, 16, 9)		(1, 8, 33, 20, 41)		(1, 15, 24, 3, 24)	
	(1, 30, 29, 5, 41)	$\mid$	(1, 28, 40, 28, 24)		(1, 22, 2, 6, 36)	
	(1, 23, 25, 32, 15)		(1, 9, 31, 35, 14)			

DCP_{2304}	(1, 12, 6, 19, 18)	(1, 0, 0, 0, 0)	(1, 23, 22, 36, 4)
$q = 47$	(1, 25, 40, 13, 2)	(1, 13, 29, 5, 34)	(1, 44, 44, 30, 34)
	(1, 15, 43, 11, 7)	(1, 8, 41, 3, 34)	(1, 37, 7, 16, 17)
	(1, 16, 32, 22, 34)	(1, 41, 25, 34, 2)	(1, 27, 17, 17, 4)
	(1, 6, 11, 1, 14)	(1, 5, 35, 2, 34)	(1, 1, 23, 33, 2)
	(1, 31, 24, 31, 14)	(1, 10, 12, 27, 9)	(1, 38, 29, 45, 34)
	(1, 33, 12, 35, 17)	(1, 20, 33, 15, 21)	(1, 46, 38, 8, 21)
	(1, 42, 26, 6, 12)	(1, 21, 4, 12, 14)	(1, 36, 1, 9, 4)
	(1, 32, 6, 28, 8)	(1, 40, 43, 37, 8)	(1, 26, 11, 10, 42)
	(1, 11, 5, 38, 27)	(1, 34, 18, 42, 34)	(1, 7, 18, 4, 24)
	(0, 0, 0, 0, 1)	(1, 29, 5, 21, 24)	(1, 39, 25, 40, 24)
	(1, 3, 17, 25, 12)	(1, 17, 23, 29, 12)	(1, 2, 24, 14, 7)
	(1, 28, 23, 24, 21)	(1, 45, 33, 41, 27)	(1, 24, 28, 43, 17)
	(1, 18, 3, 46, 9)	(1, 19, 4, 18, 18)	(1, 22, 0, 7, 34)
	(1, 30, 38, 26, 32)	(1, 43, 6, 23, 9)	(1, 35, 36, 39, 18)
	(1, 9, 38, 32, 7)	(1, 14, 38, 44, 8)	(1, 4, 38, 20, 27)

X_{24}	(1, 42, 19, 42, 37)	(1, 0, 0, 0, 0)	(1, 11, 4, 24, 2)
$q = 47$	(1, 8, 30, 36, 34)	(1, 19, 42, 1, 3)	(1, 22, 36, 19, 25)
	(1, 28, 19, 7, 7)	(1, 16, 38, 12, 9)	(1, 34, 23, 11, 37)
	(1, 33, 25, 17, 36)	(1, 31, 23, 25, 12)	(1, 25, 3, 16, 14)
	(1, 23, 25, 30, 1)	(1, 13, 30, 3, 1)	(1, 35, 16, 40, 36)
	(1, 5, 4, 2, 21)	(1, 46, 35, 9, 6)	(1, 38, 3, 28, 8)
	(1, 43, 22, 5, 6)	(1, 29, 28, 35, 34)	(1, 9, 4, 33, 16)
	(1, 2, 24, 13, 9)	(1, 17, 14, 38, 4)	(1, 12, 23, 22, 6)
	(1, 44, 21, 15, 27)	(1, 39, 33, 18, 42)	(1, 18, 41, 44, 18)
	(1, 20, 38, 45, 6)	(1, 7, 24, 34, 32)	(1, 36, 23, 10, 4)
	(1, 24, 30, 27, 3)	(0, 0, 0, 0, 1)	(1, 45, 32, 32, 27)
	(1, 30, 43, 20, 42)	(1, 4, 18, 26, 42)	(1, 21, 32, 39, 37)
	(1, 37, 12, 43, 4)	(1, 26, 46, 23, 12)	(1, 14, 7, 31, 34)
	(1, 27, 11, 4, 6)	(1, 15, 17, 8, 14)	(1, 32, 17, 46, 25)
	(1, 41, 43, 41, 42)	(1, 6, 34, 21, 34)	(1, 1, 46, 29, 17)
	(1, 10, 11, 6, 7)	(1, 40, 25, 14, 37)	(1, 3, 34, 37, 2)

X_3	(1, 0, 0, 0, 0)	(1, 36, 44, 32, 14)	(1, 12, 12, 28, 37)
$q = 47$	(1, 30, 43, 2, 18)	(1, 32, 37, 10, 3)	(0, 0, 0, 0, 1)
	(1, 24, 16, 40, 6)	(1, 43, 43, 18, 9)	(1, 18, 32, 44, 17)
	(1, 3, 38, 42, 28)	(1, 9, 35, 22, 34)	(1, 4, 23, 20, 2)
	(1, 17, 13, 37, 1)	(1, 44, 3, 35, 2)	(1, 5, 45, 25, 12)
	(1, 40, 37, 1, 1)	(1, 7, 43, 43, 12)	(1, 21, 35, 4, 7)
	(1, 39, 28, 16, 2)	(1, 1, 22, 6, 27)	(1, 26, 28, 8, 42)
	(1, 42, 43, 21, 42)	(1, 16, 4, 38, 34)	(1, 46, 43, 17, 1)
	(1, 45, 21, 26, 34)	(1, 33, 7, 36, 32)	(1, 13, 21, 13, 1)
	(1, 14, 43, 29, 1)	(1, 35, 33, 19, 32)	(1, 37, 29, 5, 8)
	(1, 25, 13, 23, 8)	(1, 11, 39, 11, 3)	(1, 19, 26, 46, 1)
	(1, 31, 3, 33, 2)	(1, 10, 8, 39, 16)	(1, 38, 25, 15, 27)
	(1, 27, 44, 27, 14)	(1, 15, 10, 34, 1)	(1, 22, 32, 30, 8)
	(1, 2, 14, 41, 4)	(1, 34, 17, 9, 16)	(1, 29, 12, 24, 6)
	(1, 6, 31, 3, 8)	(1, 8, 14, 14, 21)	(1, 41, 28, 45, 3)
	(1, 20, 9, 31, 4)	(1, 28, 36, 7, 12)	(1, 23, 40, 12, 4)

X_{40}	$(1,0,0,0,0)$	$(1,w^{44},w^{27},5,w^{33})$	$(1,w^{6},w^{27},w^{3},w^{27})$
$q=49$	$(1,w^{21},w^{11},w^{7},w^{45})$	$(1,w^{35},w^{34},1,w^{33})$	$(1,w^{26},w^{33},w^{17},w)$
$w^2=w-3$	$(1,5,1,w^{10},w^{35})$	$(1,w^{17},4,w,w^{3})$	$(1,4,0,w^{33},w^{41})$
	$(1,w^{25},2,w^{25},w^{29})$	$(1,w^{27},w^{26},w^{45},w^{23})$	$(1,w^{20},w^{43},2,w^{23})$
	$(1,w^{14},w^{25},w^{43},w^{13})$	$(1,3,w^{37},w^{22},w^{19})$	$(1,w^{41},w^{7},6,w^{35})$
	$(1,w^{30},w^{34},w^{11},w^{23})$	$(1,w^{9},3,w^{14},w^{27})$	$(1,w^{15},w^{41},w^{5},w^{25})$
	$(1,w^{7},w^{21},w^{39},w^{35})$	$(0,0,0,0,1)$	$(1,w^{23},6,w^{21},w^{37})$
	$(1,w,6,w^{20},w^{3})$	$(1,w^{12},w^{41},w^{26},w^{27})$	$(1,w^{18},w^{22},4,w^{19})$
	$(1,w^{19},w^{27},w^{44},w)$	$(1,w^{13},6,w^{37},w^{35})$	$(1,w^{10},w^{19},w^{9},w^{39})$
	$(1,w^{36},5,w^{46},w^{19})$	$(1,w^{43},w^{14},w^{15},w^{7})$	$(1,w^{11},w^{17},w^{27},w^{27})$
	$(1,w^{33},w^{5},w^{34},w^{5})$	$(1,w^{2},w^{11},w^{38},w^{19})$	$(1,w^{29},w^{2},w^{18},w^{13})$
	$(1,w^{37},w^{29},w^{35},w^{15})$	$(1,2,w^{38},w^{41},w^{29})$	$(1,w^{47},w^{7},w^{13},w^{47})$
	$(1,w^{31},w^{10},w^{31},w^{37})$	$(1,w^{28},w^{17},w^{4},w^{19})$	$(1,w^{3},w^{29},w^{36},w^{11})$
	$(1,w^{34},w^{25},w^{2},w^{41})$	$(1,w^{22},w^{44},w^{47},w^{41})$	$(1,w^{4},w^{7},w^{12},w)$
	$(1,w^{39},w^{15},w^{19},w^{29})$	$(1,w^{45},w^{39},w^{6},w^{33})$	$(1,w^{46},w^{20},w^{28},w^{31})$
	$(1,w^{38},0,w^{29},w^{43})$	$(1,6,4,w^{42},w^{3})$	$(1,w^{5},w^{35},w^{23},w^{45})$
	$(1,w^{42},w^{19},w^{30},w^{29})$	$(1,1,w^{25},3,w^{25})$	

X_{20}	$(1,0,0,0,0)$	$(1,w^{21},w^{2},w^{27},w^{41})$	$(1,w^{41},1,w^{20},w^{15})$
$q=49$	$(1,w,w^{12},w^{37},w^{29})$	$(1,w^{4},2,w^{43},w^{45})$	$(1,w^{14},w^{5},w^{2},w^{33})$
$w^2=w-3$	$(1,w^{28},w^{46},w^{19},w^{17})$	$(1,w^{39},w^{25},5,w^{3})$	$(1,w^{38},w^{34},1,w^{17})$
	$(1,1,w^{39},w^{13},w^{7})$	$(1,w^{7},w^{22},w^{46},w^{39})$	$(1,w^{20},w^{35},w^{30},w^{21})$
	$(1,w^{9},w^{18},w^{9},w^{15})$	$(1,4,w^{31},6,w^{31})$	$(1,w^{10},w,w^{6},w^{7})$
	$(1,w^{11},w^{7},w^{21},w^{11})$	$(1,w^{29},w^{45},w^{28},w^{7})$	$(1,w^{17},w^{13},w^{38},w^{27})$
	$(1,w^{37},3,w^{45},w^{13})$	$(1,5,w^{17},w,w^{45})$	$(1,w^{6},w^{13},w^{35},w^{39})$
	$(1,w^{18},w^{6},w^{12},w^{9})$	$(1,w^{2},6,w^{23},w^{31})$	$(0,0,0,0,1)$
	$(1,w^{22},w^{37},w^{47},w^{35})$	$(1,w^{44},w^{33},w^{31},w^{13})$	$(1,w^{3},w^{41},3,w^{17})$
	$(1,3,w^{29},w^{5},w^{31})$	$(1,w^{23},w^{22},w^{34},w^{1}1)$	$(1,w^{19},w^{34},w^{10},w^{15})$
	$(1,w^{5},w^{35},4,w^{35})$	$(1,w^{43},w^{33},w^{29},w^{41})$	$(1,w^{46},w^{33},w^{26},w^{41})$
	$(1,w^{42},w^{20},w^{42},w^{29})$	$(1,w^{26},w^{25},w^{22},w^{35})$	$(1,w^{13},w^{35},w^{7},w^{7})$
	$(1,w^{47},w^{3},w^{36},w^{7})$	$(1,w^{45},w^{4},w^{15},w)$	$(1,w^{31},w^{45},w^{41},w^{21})$
	$(1,w^{25},w^{38},w^{18},w^{41})$	$(1,w^{30},w^{31},w^{4},w^{33})$	$(1,w^{27},w^{30},w^{14},w^{13})$
	$(1,w^{33},3,w^{33},w^{3})$	$(1,2,w^{25},w^{17},w^{27})$	$(1,w^{15},w^{17},w^{44},w^{17})$
	$(1,w^{36},w^{33},w^{39},w^{13})$	$(1,6,w^{19},w^{25},w^{45})$	$(1,w^{35},w^{17},w^{3},w^{27})$
	$(1,w^{12},w^{45},w^{11},w^{43})$	$(1,w^{34},w^{15},2,w)$	

X_{24}	(1, 4, 23, 6, 30)	(1, 20, 37, 26, 19)	(1, 47, 33, 37, 34)
$q = 53$	(1, 2, 40, 47, 2)	(1, 29, 10, 21, 33)	(1, 11, 32, 14, 41)
	(1, 0, 0, 0, 0)	(1, 24, 7, 35, 12)	(1, 26, 34, 16, 18)
	(1, 17, 51, 20, 27)	(1, 8, 11, 9, 19)	(1, 45, 6, 15, 31)
	(1, 41, 6, 12, 2)	(1, 25, 45, 52, 14)	(1, 14, 2, 19, 48)
	(1, 40, 25, 23, 45)	(1, 12, 10, 2, 35)	(1, 22, 14, 44, 2)
	(1, 51, 32, 28, 39)	(1, 23, 41, 43, 33)	(1, 10, 22, 27, 41)
	(1, 43, 23, 42, 50)	(1, 16, 21, 40, 32)	(1, 48, 24, 4, 27)
	(1, 38, 18, 31, 35)	(1, 28, 41, 33, 45)	(1, 30, 44, 49, 39)
	(1, 19, 31, 48, 35)	(1, 52, 17, 36, 12)	(1, 6, 1, 30, 31)
	(1, 18, 9, 32, 32)	(1, 37, 32, 3, 31)	(1, 36, 20, 39, 51)
	(1, 13, 43, 24, 12)	(1, 1, 1, 1, 51)	(1, 42, 25, 34, 14)
	(1, 31, 42, 22, 45)	(1, 3, 32, 13, 50)	(1, 44, 46, 51, 39)
	(1, 27, 14, 38, 50)	(1, 49, 3, 7, 19)	(1, 15, 19, 17, 20)
	(1, 50, 43, 45, 35)	(1, 46, 14, 25, 32)	(1, 39, 20, 50, 35)
	(1, 33, 19, 11, 18)	(1, 35, 31, 46, 26)	(1, 9, 49, 41, 39)
	(0, 0, 0, 0, 1)	(1, 34, 1, 10, 30)	(1, 5, 12, 18, 31)
	(1, 21, 30, 8, 45)	(1, 32, 31, 29, 19)	(1, 7, 35, 5, 12)

X_{12}	(1, 49, 15, 31, 5)	(0, 0, 0, 0, 1)	(1, 12, 24, 48, 14)
$q = 53$	(1, 21, 37, 15, 12)	(1, 20, 39, 37, 18)	(1, 52, 42, 46, 31)
	(1, 0, 0, 0, 0)	(1, 41, 26, 30, 2)	(1, 2, 26, 20, 26)
	(1, 38, 47, 33, 35)	(1, 45, 23, 39, 48)	(1, 16, 33, 49, 35)
	(1, 46, 21, 32, 48)	(1, 43, 14, 7, 33)	(1, 3, 0, 47, 18)
	(1, 28, 15, 35, 14)	(1, 8, 14, 1, 8)	(1, 44, 37, 26, 31)
	(1, 9, 30, 51, 19)	(1, 7, 3, 8, 41)	(1, 5, 27, 38, 35)
	(1, 51, 12, 43, 48)	(1, 27, 42, 34, 21)	(1, 26, 41, 27, 2)
	(1, 48, 15, 29, 26)	(1, 30, 51, 24, 18)	(1, 18, 31, 23, 3)
	(1, 47, 22, 13, 18)	(1, 32, 29, 36, 21)	(1, 42, 39, 52, 5)
	(1, 35, 46, 4, 23)	(1, 24, 42, 25, 21)	(1, 36, 37, 17, 33)
	(1, 14, 30, 2, 26)	(1, 15, 35, 3, 2)	(1, 22, 11, 6, 12)
	(1, 39, 41, 9, 35)	(1, 34, 5, 28, 30)	(1, 10, 33, 10, 30)
	(1, 29, 37, 5, 23)	(1, 25, 17, 18, 3)	(1, 1, 4, 19, 18)
	(1, 11, 38, 12, 14)	(1, 17, 15, 16, 33)	(1, 19, 11, 44, 50)
	(1, 23, 32, 45, 8)	(1, 40, 51, 42, 12)	(1, 33, 43, 22, 22)
	(1, 37, 35, 40, 51)	(1, 31, 3, 11, 21)	(1, 50, 45, 14, 31)
	(1, 13, 34, 21, 2)	(1, 6, 40, 50, 8)	(1, 4, 44, 41, 20)

X_{120}	(1, 0, 0, 0, 0)	(1, 20, 23, 24, 53)	(1, 31, 45, 58, 12)
$q = 59$	(1, 5, 41, 43, 51)	(1, 55, 28, 36, 9)	(1, 32, 47, 32, 12)
	(1, 34, 19, 51, 29)	(1, 46, 58, 22, 49)	(1, 41, 13, 3, 3)
	(1, 18, 54, 50, 19)	(1, 28, 46, 9, 51)	(1, 33, 10, 26, 45)
	(1, 54, 19, 47, 51)	(1, 26, 2, 56, 15)	(1, 4, 53, 2, 15)
	(1, 49, 20, 35, 9)	(1, 44, 7, 34, 48)	(1, 47, 41, 30, 36)
	(1, 17, 50, 29, 16)	(1, 56, 50, 54, 22)	(0, 0, 0, 0, 1)
	(1, 11, 55, 49, 35)	(1, 35, 18, 23, 51)	(1, 21, 1, 44, 19)
	(1, 23, 37, 6, 27)	(1, 2, 4, 4, 35)	(1, 30, 7, 48, 45)
	(1, 51, 5, 33, 3)	(1, 48, 49, 16, 17)	(1, 36, 32, 15, 29)
	(1, 14, 19, 18, 36)	(1, 57, 10, 38, 35)	(1, 13, 0, 53, 19)
	(1, 58, 53, 55, 19)	(1, 16, 32, 27, 19)	(1, 25, 36, 1, 36)
	(1, 27, 1, 20, 49)	(1, 10, 4, 31, 28)	(1, 42, 38, 45, 29)
	(1, 19, 38, 25, 28)	(1, 7, 12, 11, 15)	(1, 8, 35, 12, 36)
	(1, 50, 5, 19, 28)	(1, 43, 16, 14, 27)	(1, 1, 30, 46, 57)
	(1, 6, 31, 8, 53)	(1, 40, 34, 52, 9)	(1, 38, 38, 57, 48)
	(1, 29, 12, 17, 12)	(1, 9, 24, 39, 17)	(1, 39, 13, 40, 41)
	(1, 24, 18, 37, 27)	(1, 37, 7, 41, 27)	(1, 53, 21, 28, 22)
	(1, 52, 40, 42, 51)	(1, 22, 58, 21, 9)	(1, 12, 23, 7, 36)
	(1, 3, 58, 13, 19)	(1, 15, 58, 10, 26)	(1, 45, 54, 5, 45)

X_{24}	(1, 36, 40, 12, 53)	(1, 54, 38, 46, 46)	(1, 5, 25, 4, 45)
$q = 59$	(1, 58, 45, 9, 19)	(1, 41, 13, 21, 26)	(1, 18, 6, 34, 28)
	(1, 13, 7, 42, 17)	(1, 55, 7, 58, 28)	(1, 21, 44, 35, 20)
	(1, 12, 3, 51, 20)	(1, 8, 48, 38, 5)	(1, 3, 22, 30, 25)
	(1, 25, 38, 50, 41)	(1, 30, 21, 32, 36)	(1, 34, 46, 56, 45)
	(1, 19, 1, 31, 45)	(0, 0, 0, 0, 1)	(1, 1, 25, 53, 12)
	(1, 24, 28, 2, 51)	(1, 51, 16, 14, 48)	(1, 44, 4, 52, 9)
	(1, 11, 1, 5, 48)	(1, 40, 35, 36, 9)	(1, 0, 0, 0, 0)
	(1, 33, 54, 11, 29)	(1, 53, 43, 49, 53)	(1, 43, 52, 20, 57)
	(1, 28, 35, 18, 1)	(1, 27, 50, 57, 19)	(1, 26, 12, 41, 19)
	(1, 45, 17, 26, 41)	(1, 35, 35, 48, 5)	(1, 14, 23, 28, 51)
	(1, 39, 31, 43, 15)	(1, 10, 5, 7, 27)	(1, 49, 34, 3, 36)
	(1, 17, 39, 45, 20)	(1, 4, 42, 47, 20)	(1, 2, 36, 40, 9)
	(1, 32, 1, 23, 16)	(1, 38, 13, 22, 51)	(1, 7, 16, 44, 41)
	(1, 16, 58, 1, 28)	(1, 20, 11, 16, 48)	(1, 56, 45, 39, 9)
	(1, 23, 21, 19, 28)	(1, 9, 17, 33, 29)	(1, 42, 16, 17, 48)
	(1, 31, 38, 27, 41)	(1, 15, 48, 29, 51)	(1, 46, 18, 13, 29)
	(1, 37, 58, 24, 41)	(1, 47, 24, 10, 35)	(1, 48, 37, 25, 36)
	(1, 57, 23, 15, 1)	(1, 6, 30, 55, 35)	(1, 22, 1, 54, 36)
	(1, 29, 22, 8, 1)	(1, 52, 57, 6, 41)	(1, 50, 18, 37, 16)

X_5	(1, 0, 0, 0, 0)		(1, 24, 54, 52, 25)		(1, 55, 0, 21, 25)	
$q = 59$	(1, 23, 52, 12, 29)		(1, 3, 36, 35, 15)	|	(0, 0, 0, 0, 1)	
	(1, 53, 5, 54, 4)		(1, 19, 28, 27, 1)		(1, 41, 15, 13, 9)	
	(1, 11, 13, 18, 46)	|	(1, 10, 30, 10, 3)		(1, 56, 17, 20, 7)	
	(1, 6, 30, 31, 35)		(1, 15, 36, 41, 36)		(1, 43, 21, 44, 27)	|
	(1, 58, 11, 30, 27)		(1, 8, 35, 16, 4)		(1, 45, 16, 6, 5)	
	(1, 44, 35, 39, 9)		(1, 12, 46, 25, 3)	|	(1, 35, 53, 37, 26)	
	(1, 52, 40, 47, 27)		(1, 30, 31, 40, 22)		(1, 51, 15, 58, 3)	
	(1, 34, 15, 34, 35)	|	(1, 13, 15, 38, 48)		(1, 21, 4, 49, 17)	
	(1, 7, 14, 45, 20)		(1, 50, 42, 24, 45)		(1, 16, 22, 46, 19)	|
	(1, 40, 19, 11, 25)		(1, 22, 11, 42, 17)		(1, 29, 15, 2, 12)	
	(1, 5, 33, 29, 5)		(1, 57, 39, 7, 27)	|	(1, 14, 19, 5, 41)	
	(1, 49, 39, 15, 45)		(1, 38, 41, 23, 41)		(1, 54, 24, 26, 26)	
	(1, 25, 3, 57, 41)	|	(1, 31, 0, 53, 9)		(1, 27, 43, 50, 46)	
	(1, 17, 19, 48, 3)		(1, 26, 42, 55, 51)		(1, 28, 41, 19, 29)	|
	(1, 1, 30, 32, 12)		(1, 48, 19, 14, 29)		(1, 39, 24, 3, 15)	
	(1, 46, 55, 43, 12)		(1, 18, 50, 28, 5)	|	(1, 37, 49, 33, 36)	
	(1, 32, 31, 17, 29)		(1, 42, 1, 8, 17)		(1, 9, 14, 22, 19)	
	(1, 47, 45, 56, 4)	|	(1, 4, 12, 1, 29)		(1, 36, 57, 4, 29)	
	(1, 33, 50, 9, 35)		(1, 2, 17, 51, 22)		(1, 20, 20, 36, 1)	

X_{24}	(1, 40, 64, 64, 18)	(1, 0, 0, 0, 0)	(1, 29, 70, 61, 5)
$q = 71$	(1, 13, 43, 48, 12)	(1, 44, 22, 47, 4)	(1, 8, 56, 45, 54)
	(1, 24, 3, 4, 37)	(1, 12, 37, 63, 5)	(1, 48, 2, 62, 2)
	(1, 68, 13, 59, 8)	(1, 67, 69, 3, 8)	(1, 66, 23, 53, 20)
	(1, 38, 41, 58, 20)	(1, 46, 14, 11, 8)	(1, 57, 16, 31, 36)
	(1, 32, 68, 27, 50)	(1, 52, 2, 43, 32)	(1, 37, 37, 33, 37)
	(1, 39, 26, 42, 29)	(1, 64, 63, 55, 37)	(1, 2, 22, 37, 10)
	(1, 5, 43, 26, 9)	(1, 25, 70, 39, 18)	(1, 30, 18, 36, 16)
	(1, 20, 7, 20, 48)	(1, 61, 1, 23, 16)	(1, 54, 37, 41, 38)
	(1, 56, 12, 12, 36)	(1, 1, 35, 51, 2)	(1, 6, 5, 35, 49)
	(1, 17, 49, 19, 45)	(1, 62, 24, 57, 8)	(1, 23, 26, 29, 6)
	(1, 59, 9, 65, 60)	(1, 33, 5, 25, 2)	(1, 50, 67, 40, 43)
	(1, 69, 50, 21, 27)	(1, 49, 44, 30, 2)	(1, 53, 19, 60, 9)
	(1, 45, 21, 68, 49)	(1, 15, 30, 46, 43)	(1, 41, 48, 44, 10)
	(1, 19, 27, 52, 58)	(1, 28, 10, 9, 3)	(0, 0, 0, 0, 1)
	(1, 47, 61, 17, 24)	(1, 31, 7, 28, 6)	(1, 11, 57, 16, 54)
	(1, 7, 5, 6, 4)	(1, 70, 30, 15, 38)	(1, 34, 44, 8, 64)
	(1, 43, 48, 14, 5)	(1, 22, 70, 49, 57)	(1, 35, 5, 66, 8)
	(1, 55, 47, 54, 4)	(1, 58, 20, 50, 37)	(1, 51, 5, 56, 30)
	(1, 60, 2, 69, 45)	(1, 63, 3, 13, 24)	(1, 3, 18, 5, 16)
	(1, 16, 18, 24, 2)	(1, 4, 36, 7, 25)	(1, 65, 35, 32, 32)
	(1, 14, 6, 70, 49)	(1, 42, 13, 1, 2)	(1, 10, 51, 38, 1)
	(1, 26, 28, 67, 30)	(1, 36, 52, 22, 54)	(1, 9, 27, 18, 32)
	(1, 18, 28, 2, 32)	(1, 27, 20, 10, 40)	(1, 21, 46, 34, 10)

X_{24}	(1, 77, 47, 43, 41)	(1, 50, 57, 5, 70)	(1, 82, 59, 2, 7)
$q = 83$	(1, 6, 67, 54, 1)	(1, 80, 28, 69, 4)	(1, 67, 31, 64, 63)
	(1, 8, 56, 3, 77)	(1, 18, 14, 77, 78)	(1, 64, 56, 68, 65)
	(1, 51, 22, 16, 28)	(1, 2, 81, 21, 37)	(1, 39, 31, 19, 41)
	(1, 32, 48, 39, 17)	(1, 0, 0, 0, 0)	(1, 81, 36, 37, 23)
	(1, 54, 39, 57, 49)	(1, 13, 55, 53, 21)	(1, 70, 71, 6, 17)
	(1, 47, 26, 58, 1)	(1, 26, 54, 50, 17)	(1, 38, 70, 7, 63)
	(1, 31, 56, 79, 59)	(1, 49, 63, 74, 41)	(1, 4, 48, 20, 23)
	(1, 44, 33, 1, 29)	(1, 42, 26, 63, 81)	(1, 60, 72, 17, 21)
	(1, 24, 4, 22, 37)	(1, 73, 49, 80, 59)	(1, 40, 32, 33, 63)
	(1, 57, 28, 47, 23)	(1, 55, 76, 76, 4)	(1, 9, 27, 26, 33)
	(1, 3, 20, 4, 3)	(1, 19, 13, 78, 9)	(1, 14, 4, 31, 48)
	(1, 69, 16, 9, 36)	(1, 41, 33, 11, 37)	(1, 33, 56, 60, 30)
	(1, 76, 0, 81, 69)	(1, 56, 17, 32, 77)	(1, 68, 35, 25, 63)
	(1, 37, 5, 67, 69)	(1, 71, 50, 35, 78)	(1, 58, 38, 29, 28)
	(1, 78, 51, 62, 33)	(1, 17, 54, 66, 29)	(1, 35, 48, 59, 30)
	(1, 43, 39, 23, 63)	(1, 7, 37, 8, 69)	(1, 21, 7, 41, 3)
	(1, 72, 42, 27, 27)	(1, 79, 65, 75, 59)	(1, 15, 12, 10, 38)
	(1, 48, 13, 30, 51)	(0, 0, 0, 0, 1)	(1, 22, 2, 15, 81)
	(1, 30, 62, 73, 25)	(1, 53, 32, 61, 59)	(1, 20, 60, 45, 65)
	(1, 1, 47, 40, 75)	(1, 12, 61, 34, 21)	(1, 63, 54, 52, 33)
	(1, 29, 57, 46, 65)	(1, 11, 54, 65, 21)	(1, 25, 17, 12, 75)
	(1, 62, 40, 36, 69)	(1, 46, 65, 51, 69)	(1, 27, 39, 44, 30)
	(1, 5, 63, 28, 41)	(1, 16, 28, 56, 63)	(1, 45, 0, 38, 33)
	(1, 66, 25, 48, 25)	(1, 61, 71, 13, 59)	(1, 36, 49, 72, 70)
	(1, 28, 41, 82, 7)	(1, 75, 60, 55, 77)	(1, 34, 55, 42, 29)
	(1, 10, 63, 49, 23)	(1, 65, 1, 24, 16)	(1, 52, 23, 71, 12)
	(1, 23, 20, 14, 25)	(1, 74, 17, 70, 9)	(1, 59, 14, 18, 70)

X_{24}	(1, 0, 0, 0, 0)	(1, 22, 8, 4, 26)	(1, 54, 17, 25, 52)
$q = 89$	(1, 79, 36, 40, 83)	(1, 30, 69, 30, 35)	(1, 43, 85, 81, 61)
	(1, 25, 55, 29, 77)	(1, 56, 28, 2, 83)	(1, 6, 34, 36, 52)
	(1, 29, 2, 15, 6)	(1, 3, 50, 84, 7)	(1, 61, 64, 87, 31)
	(1, 10, 20, 14, 83)	(1, 13, 0, 45, 38)	(1, 11, 88, 31, 14)
	(1, 20, 47, 11, 63)	(1, 74, 26, 33, 86)	(1, 49, 37, 3, 86)
	(1, 16, 57, 55, 54)	(0, 0, 0, 0, 1)	(1, 40, 83, 22, 63)
	(1, 23, 38, 71, 38)	(1, 12, 63, 70, 86)	(1, 21, 7, 19, 86)
	(1, 14, 0, 18, 15)	(1, 45, 42, 39, 41)	(1, 63, 42, 8, 46)
	(1, 59, 74, 72, 66)	(1, 8, 38, 61, 26)	(1, 51, 19, 7, 83)
	(1, 19, 68, 83, 29)	(1, 70, 47, 86, 48)	(1, 4, 51, 53, 35)
	(1, 67, 0, 41, 12)	(1, 62, 25, 65, 62)	(1, 68, 43, 28, 74)
	(1, 2, 67, 77, 74)	(1, 26, 83, 17, 56)	(1, 35, 66, 49, 70)
	(1, 83, 20, 62, 61)	(1, 84, 18, 20, 43)	(1, 66, 56, 38, 52)
	(1, 86, 27, 48, 38)	(1, 60, 34, 68, 15)	(1, 44, 12, 6, 37)
	(1, 75, 78, 23, 23)	(1, 73, 11, 50, 56)	(1, 80, 70, 79, 83)
	(1, 28, 57, 76, 52)	(1, 27, 23, 78, 35)	(1, 53, 17, 88, 31)
	(1, 39, 64, 54, 28)	(1, 88, 9, 51, 59)	(1, 78, 55, 64, 82)
	(1, 15, 73, 32, 65)	(1, 87, 52, 60, 86)	(1, 72, 9, 13, 51)
	(1, 81, 60, 42, 29)	(1, 48, 60, 10, 14)	(1, 52, 67, 58, 60)
	(1, 38, 82, 34, 83)	(1, 64, 34, 56, 66)	(1, 31, 55, 27, 54)
	(1, 55, 77, 37, 46)	(1, 9, 26, 69, 38)	(1, 47, 9, 67, 63)
	(1, 18, 64, 16, 66)	(1, 24, 17, 46, 31)	(1, 71, 50, 26, 15)
	(1, 32, 49, 66, 26)	(1, 37, 61, 43, 28)	(1, 58, 25, 35, 15)
	(1, 41, 21, 12, 46)	(1, 42, 25, 59, 12)	(1, 34, 25, 74, 63)
	(1, 69, 33, 44, 58)	(1, 57, 35, 73, 43)	(1, 36, 46, 24, 46)
	(1, 77, 14, 85, 23)	(1, 65, 25, 57, 31)	(1, 85, 67, 9, 86)
	(1, 50, 52, 80, 60)	(1, 7, 55, 52, 82)	(1, 5, 59, 75, 60)
	(1, 17, 24, 21, 46)	(1, 82, 74, 47, 15)	(1, 46, 72, 5, 15)
	(1, 76, 7, 82, 38)	(1, 33, 33, 1, 35)	(1, 1, 71, 63, 58)

8.2 The new example for $q = 125$

The techniques discussed in the previous chapter rely heavily upon the implementation in MAGMA of the groups $PGO(5, q)$. As q gets large, say $q > 59$, the techniques are no longer as effective in terms of the computing time required, and for $q > 97$ we no longer have available these in-built groups. Thus to search over these higher order fields, we may start with certain hypotheses upon the examples we wish to find, or instead change techniques altogether. For example, the three examples found for $q = 71, 83$ and 89 required a hypothesis concerning the group of the example, as we indicate in the final chapter. Motivated by the construction of an infinite family of BLT-sets from an example for $q = 27$, which we discuss in the final chapter also, an attempt was made to construct BLT-sets for $q = 125$. Working with the underlying vector spaces, matrix groups and the classical BLT-set over $GF(5)$, the following example was discovered.

Let $q = 125$ and define $Q(4, q)$ by the quadratic form $Q : x_0x_5 + x_2x_4 + x_3^2$. Then the following defines a BLT-set of $Q(4, 125)$.

$$X_{72} = \{\langle(1, t, f(t), -g(t), tg(t) - f(t)^2)\rangle : t \text{ in } GF(q)\} \cup \{\langle(0, 0, 0, 0, 1)\rangle\}$$

where f and g are as follows :

$$\begin{aligned} f = \quad & x^{59} + 2x^{57} + 4x^{55} + 2x^{53} + x^{51} + 3x^{49} + 4x^{45} + 4x^{43} + 4x^{39} + 2x^{37} \\ & +4x^{35} + 3x^{33} + 4x^{31} + 4x^{29} + 3x^{25} + 4x^{23} + x^{19} + 4x^{17} + 4x^{15} + 4x^{13} \\ & +3x^{11} + 2x^{9} + x^{7} + 4x^{5} + 4x \end{aligned}$$

$$\begin{aligned} g = \quad & x^{117} + 3x^{115} + x^{113} + x^{107} + 3x^{105} + 3x^{103} + 3x^{101} + 3x^{95} + 2x^{91} + 4x^{87} \\ & +2x^{85} + 3x^{83} + 2x^{77} + 2x^{75} + 4x^{73} + 4x^{71} + x^{67} + 2x^{65} + 2x^{61} + 4x^{59} \\ & +x^{57} + x^{55} + 4x^{53} + 4x^{49} + 3x^{47} + 2x^{45} + 4x^{43} + 2x^{41} + 4x^{39} + x^{33} \\ & +2x^{31} + 4x^{29} + 3x^{25} + 4x^{23} + x^{21} + x^{19} + 4x^{17} + x^{15} + 3x^{13} + 4x^{11} \\ & +2x^{7} + 4x^{3} + 4x. \end{aligned}$$

To determine the group of this example, an adaptation of the conic invariant of Williams (1998) was used. This involves counting the number of points of a BLT-set which lie on the conic in the plane spanned by three distinct elements of the BLT-set, for all triples in the BLT-set. From this, we have a unique conic C meeting X_{72} in 6 points, these being the points over $GF(5)$, and all others meeting X_{72} in at most 4 points. Hence the stabiliser H of X_{72} in $P\Gamma O(5, 125)$ is contained in the stabiliser G of $X_{72} \cap C$ in $P\Gamma O(5, 125)$. Since $|G| = 4320$, we can loop over all elements of G and see if they stabilise X_{72} in order to determine H. We find that $|H| = 72$, which distinguishes X_{72} from the known examples over $q = 125$. Furthermore, $H \cong S_4 \times C_3$, with orbit structure $\{72, 24^2, 6\}$. The four orbits are actually distinguished by how many conics meeting X_{72} in 4 points a point lies on. Noting that the points of the BLT-set other than $(\infty) = \langle(0,0,0,0,1)\rangle$ are indexed by the elements of $GF(125)$ (with respect to the second coordinate), we describe the orbits on X_{72} as a partition of $GF(125) \cup \{\infty\}$, where $w^3 = 2w + 2$:

$\{0, 1, 2, 3, 4, (\infty)\}$,

$\{w^6, w^{19}, w^{21}, w^{26}, w^{29}, w^{30}, w^{33}, w^{34}, w^{41}, w^{43}, w^{44}, w^{46}, w^{68}, w^{81}, w^{83}, w^{88}, w^{91}, w^{92}, w^{95}, w^{96}, w^{103}, w^{105}, w^{106}, w^{108}\}$,

$\{w^7, w^9, w^{17}, w^{23}, w^{35}, w^{37}, w^{39}, w^{45}, w^{51}, w^{53}, w^{57}, w^{61}, w^{69}, w^{71}, w^{79}, w^{85}, w^{97}, w^{99}, w^{101}, w^{107}, w^{113}, w^{115}, w^{119}, w^{123}\}$,

$\{w, w^2, w^3, w^4, w^5, w^8, w^{10}, w^{11}, w^{12}, w^{13}, w^{14}, w^{15}, w^{16}, w^{18}, w^{20}, w^{22}, w^{24}, w^{25}, w^{27}, w^{28}, w^{32}, w^{36}, w^{38}, w^{40}, w^{42}, w^{47}, w^{48}, w^{49}, w^{50}, w^{52}, w^{54}, w^{55}, w^{56}, w^{58}, w^{59}, w^{60}, w^{63}, w^{64}, w^{65}, w^{66}, w^{67}, w^{70}, w^{72}, w^{73}, w^{74}, w^{75}, w^{76}, w^{77}, w^{78}, w^{80}, w^{82}, w^{84}, w^{86}, w^{87}, w^{89}, w^{90}, w^{94}, w^{98}, w^{100}, w^{102}, w^{104}, w^{109}, w^{110}, w^{111}, w^{112}, w^{114}, w^{116}, w^{117}, w^{118}, w^{120}, w^{121}, w^{122}\}$.

Analysis of some examples

One of the important motivations behind searching for new examples of BLT-sets is the possibility of generalising examples to infinite families of BLT-sets. Of course, some examples may not belong to an infinite family of BLT-sets, and so we also look for evidence which suggests that an example is sporadic (as a BLT-set). For example, the three new examples for $q = 71, 83$ and 89 presented in the previous chapter were discovered using similar orbit-stitching techniques as discussed earlier, but required starting with a particular subgroup. Analysis of some other examples suggested the possibility of further examples arising from a subgroup of the stabiliser of the Fisher-Thas-Walker/Kantor BLT-set isomorphic to A_4. The recent discovery of these examples, working with this hypothesis, highlights the opportunities available from analysing known examples, and why it is worthwhile searching for new examples in the first place. In this final chapter we consider some of the other examples presented earlier. In particular, we have been able to generalise the new example for $q = 27$ to an infinite family of BLT-sets in characteristic 3.

9.1 An infinite family of BLT-sets in characteristic 3

We have seen in Section 6.3 that BLT-sets may be parametrised in the same manner as the associated q-clans and flocks. Thus given coordinates for the points of a BLT-set, as for example in the previous chapter, we may attempt to find such a parametrisation which is useful in describing the example in more general terms.

We do this by first moving the BLT-set onto the points $P_\infty = (0, 0, 0, 0, 1)$ and $P_0 = (1, 0, 0, 0, 0)$, and then, for the points of the BLT-set other than P_∞, interpolating the second and third coordinates and the second and fourth coordinates to obtain polynomial functions describing the BLT-set. These can then be translated into the q-clan model, and the condition on the matrices of the q-clan can be easily checked. However, this process is far from unique. There is a choice of which points to move to the special points, and we may also then change coordinates in any way that fixes these points, before interpolating, and consequently we cannot afford to check all possible interpolations. Instead, we hope to find an interpolation which provides a form which can be generalised in some manner, depending upon the situation.

Such experimentation was successfully performed on the new example X_6 for $q = 27$. This example has two fixed points, an orbit of length 2 and four of length 6 under its stabiliser $P\Gamma O(5, q)_{X_6}$. As a general rule of thumb, we choose a point in the shortest orbit to map to the point P_∞, and then choose a point in the shortest orbit of $P\Gamma O(5,q)_{X_6,P_\infty}$ on $X_6\backslash\{P_\infty\}$ to map to P_0 in order to preserve as much symmetry of X_6 as possible. We also choose to change coordinates in such a way that the semisimilarity

$$(x_0,x_1,x_2,x_3,x_4)\mapsto(x_0^3,x_1^3,x_2^3,x_3^3,x_4^3)$$

preserves X_6 (which now contains P_∞ and P_0) since then the functions appearing in the q-clan will be polynomial over $GF(3)$. Interpolating as above, and a bit of luck, led to a q-clan for which $-\det(A_s-A_t)=-S(s,t)$, where $S(s,t)$ was the square of a polynomial over $GF(3)$. As -1 is a nonsquare in $GF(3)$, $-\det(A_s-A_t)$ remains equal to $-S(s,t)$ for all odd degree extensions of $GF(3)$, and so gives an infinite family of q-clans for $q=3^h$, h odd. Motivated by the known infinite families which are described for a particular characteristic only (namely, Kantor/Knuth semifield, Kantor likeable, and Ganley semifield), we can generalise to the use of an arbitrary nonsquare in place of -1 and then attempt to remove the hypothesis of h odd. This led to the following infinite family of BLT-sets in characteristic 3, described using the q-clan model.

Theorem 9.1. *For $t\in GF(q)$ with $q=3^h$, and n a fixed nonsquare of $GF(q)$, let*

$$A_t=\begin{bmatrix} t & t^4+nt^2\\ t^4+nt^2 & -n^{-1}t^9+t^7+n^2t^3-n^3t\end{bmatrix}.$$

Then $\mathcal{C}=\{A_t : t\in GF(q)\}$ is a q-clan.

Proof :

$$\begin{aligned}
&(b_s-b_t)^2-4(a_s-a_t)(c_s-c_t)\\
=\;&(-s^4-ns^2+t^4+nt^2)^2\\
&-4(s-t)(-n^{-1}s^9+s^7+n^2s^3-n^3s+n^{-1}t^9-t^7-n^2t^3+n^3t)\\
=\;&(s-t)^2(s+t)^2(n+s^2+t^2)^2\\
&+n^{-1}(s-t)^2(s^8+s^7t+s^6t^2+s^5t^3+s^4t^4+s^3t^5+s^2t^6+st^7+t^8\\
&-n(s^6+s^5t+s^4t^2+s^3t^3+s^2t^4+st^5+t^6)-n^3(s^2+st+t^2)+n^4)\\
=\;&n^{-1}(s-t)^2(s^8+s^7t+s^6t^2+s^5t^3+s^4t^4+s^3t^5+s^2t^6+st^7+t^8\\
&+n(s^5t+2s^4t^2+2s^2t^4+st^5)+n^2(2s^4+s^3t+s^2t^2+st^3+2t^4)+n^3st+n^4)\\
=\;&n^{-1}(s-t)^2(s^4-s^3t-st^3+t^4-nst+n^2)^2
\end{aligned}$$

We must also show that this is nonzero for $s\neq t$. This is if and only if $(s-t)^4-$

$nst + n^2$ is nonzero. So suppose $(s-t)^4 - nst + n^2 = 0$. Then

$$\begin{aligned} n &= -st \pm \sqrt{s^2t^2 - (s-t)^4} \\ &= -st \pm (s+t)\sqrt{-(s^2+t^2)} \\ &= \left((s+t) \mp \sqrt{-(s^2+t^2)}\right)^2. \end{aligned}$$

contradicting the fact that n is a nonsquare.

For $q = 3$ the BLT-set in the family is classical, and for $q = 9$ it is Fisher. We know from the work in the previous chapter that the example for $q = 27$ is new, and suspected that the family was new in general for $q > 27$. The infinite family was published in a paper by Penttila and the present author (2001), with a conjecture that the full stabiliser of the BLT-set for $q = 3^h > 9$ is cyclic of order $2h$. By the so-called Orbit Counting Lemma, this would imply that at least $\frac{q+1}{2h}$ distinct, non-isomorphic flocks arise from each BLT-set, unlike all previously known families which had at most two flocks arising in any case.

This was indeed proven to be the case by Payne (2001) who calculated the collineation group of the associated GQ using the Fundamental Theorem of q-clan geometry (see Chapter 5). Hence the number of distinct flocks arising from each BLT-set grows with the field order q. Furthermore, if h is the power of an odd prime, Payne (2001) shows that many of the flocks arising have trivial automorphism group. This provides the first infinite family of such flocks.

9.2 Possibly sporadic examples

As discussed above, some examples of BLT-sets admit evidence that they may not belong to an infinite family of BLT-sets, and so we say that these BLT-sets are *possibly sporadic* (as BLT-sets). The example of Penttila and Royle PR_{1152} over the field of order 23, and the example of De Clerck and Penttila DCP_{2304} over the field of order 47, have arisen in a study of hyperbolic reflections preserving a BLT-set of $Q(4,q)$, by Bader, Durante, Lunardon, Penttila and the present author ([8]). In this paper, these two BLT-sets are linked with two of the exceptional flocks of the hyperbolic quadric (Section 3) via root systems of the Euclidean space $\mathbb{R}^4$, providing evidence that they are indeed sporadic as BLT-sets.

A further example in the data of the previous chapter appears to be possibly sporadic as a BLT-set. We give here a description of the new example X_{720} over the field of order 29, which suggests that this may be the case.

Let V be $GF(29)^6$ and Q be the quadratic form on V given by

$$Q(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2.$$

Then $Q(1,1,1,1,1,1)$ is not 0, so $W = \{x | x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 0\}$ is a nondegenerate subspace. Let $\mathcal{P}$ be the set of all images of the point $(1,1,1,1,7,18)$ under permutations of the coordinates. Then $\mathcal{P}$ is a set of 30 points of W. We now prove that $\mathcal{P}$ is a BLT-set of W (considered as $O(5,29)$) whose group is S_6.

Theorem 9.2. *Let $V = GF(29)^6$ and $Q\colon V \to GF(29)$ be given by*

$$Q(x_1, x_2, x_3, x_4, x_5, x_6) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2.$$

Let $e = (1,1,1,1,1,1)$ and $W = e^\perp$, so that W is a nondegenerate subspace of V. Let S_6 act on V by permuting the coordinates. Let $\mathcal{P}$ be the orbit of $(1,1,1,1,7,18)$ under S_6. Then $\mathcal{P}$ is a BLT-set of W, and the full stabiliser of $\mathcal{P}$ in $PGO(5,29)$ is S_6.

Proof : The polar form of Q is $f(x,y) = 2x_1y_1+2x_2y_2+2x_3y_3+2x_4y_4+2x_5y_5+2x_6y_6$. S_6 fixes W and $f(e,(1,1,1,1,7,18)) = 0 (\mathrm{mod}\ 29)$, so $\mathcal{P}$ is a subset of W. A calculation shows that the discriminant of the restriction of Q to W is a nonsquare, so by Corollary 6.2 we must show that $f(x,y)f(x,z)f(y,z)$ is a nonsquare, for all distinct $x, y, z \in \mathcal{P}$. It is sufficient to show that $f(x,y)$ is a nonsquare, for distinct $x, y \in \mathcal{P}$. There are 5 cases :

$f(x,y) = 2(18^2 + 7.1 + 1.7 + 1^2 + 1^2 + 1^2) = 15 (\mathrm{mod}\ 29)$;
$f(x,y) = 2(18.7 + 7.18 + 1^2 + 1^2 + 1^2 + 1^2) = 19 (\mathrm{mod}\ 29)$;
$f(x,y) = 2(18.7 + 7.1 + 1.18 + 1^2 + 1^2 + 1^2) = 18 (\mathrm{mod}\ 29)$;
$f(x,y) = 2(18.1 + 7.7 + 1.18 + 1^2 + 1^2 + 1^2) = 2 (\mathrm{mod}\ 29)$;
$f(x,y) = 2(18.1 + 7.1 + 1.18 + 1.7 + 1^2 + 1^2) = 17 (\mathrm{mod}\ 29)$.

These are all nonsquares modulo 29, so $\mathcal{P}$ is a BLT-set. $\mathcal{P}$ admits S_6, which is a maximal subgroup of $PGO(5,29)$, and so the full stabiliser of $\mathcal{P}$ in $PGO(5,29)$ is S_6.

The previously known BLT-sets in $Q(4,29)$ are the classical BLT-set, with a group of order 1461600, the Fisher-Thas/Walker/Kantor BLT-set, with a group of order 24360, the Fisher BLT-set, with a group of order 1800, and the Penttila BLT-set, with a group of order 60 (which can be calculated using MAGMA). Hence $\mathcal{P}$ is a new BLT-set.

Since S_6 acts transitively on $\mathcal{P}$, there arises exactly one flock of the quadratic cone of PG$(3,29)$.

Bibliography

[1] R. W. Ahrens, G. Szekeres : On a combinatorial generalization of 27 lines associated with a cubic surface, J. Austral. Math. Soc., 10:485–492, 1969.

[2] E. Artin : *Geometric algebra*, Interscience Publishers, Inc., New York-London, 1957.

[3] M. Aschbacher : *Finite group theory*, Cambridge Studies in Advanced Mathematics, 10, Cambridge University Press, Cambridge, 1986.

[4] J. André : Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe, Math. Z., 60:156–186, 1954.

[5] L. Bader : Some new examples of flocks of $Q^+(3,q)$, Geom. Dedicata, 27(2):213–218, 1988.

[6] L. Bader : On the flocks of the quadratic cone. Boll. Un. Mat. Ital. A 2(3):371–375, 1988.

[7] L. Bader, N. Durante, M. Law, G. Lunardon, T. Penttila : Flocks and partial flocks of hyperbolic quadrics via root systems, J. Algebraic Combin., 16(1):21–30, 2002.

[8] L. Bader, N. Durante, M. Law, G. Lunardon, T. Penttila : Symmetries of BLT-sets, Des. Codes Cryptogr., (accepted).

[9] L. Bader, D. Ghinelli, T. Penttila : On monomial flocks, European J. Combin., 22(4):447–454, 2001.

[10] L. Bader, G. Lunardon : On the flocks of $Q^+(3,q)$, Geom. Dedicata, 29(2):177–183, 1989.

[11] L. Bader, G. Lunardon : On non-hyperelliptic flocks, European J. Combin., 15(5):411–415, 1994.

[12] L. Bader, G. Lunardon, S. E. Payne : On q-clan geometry, $q = 2^e$, Simon Stevin, 1:301–328, 1994.

[13] L. Bader, G. Lunardon, I. Pinneri : A new semifield flock, J. Combin. Theory Ser. A, 86(1):49–62, 1999.

[14] L. Bader, G. Lunardon, J. A. Thas : Derivation of flocks of quadratic cones, Forum Math., 2(2):163–174, 1990.

[15] L. Bader, C. M. O'Keefe, T. Penttila : Some remarks on flocks, Australas. J. Combin., (to appear).

[16] R. Baer : *Linear algebra and projective geometry*, Academic Press Inc., New York, N. Y., 1952.

[17] R.D. Baker, J. M. Dover, G. L. Ebert, K. L. Wantz : Hyperbolic fibrations of PG$(3, q)$, Europ. J. Combin., 19:1–16, 1998.

[18] R. D. Baker, G. L. Ebert : A nonlinear flock in the Minkowski plane of order 11, Congr. Numer., 58:75–81, 1987.

[19] R. D. Baker, G. L. Ebert : A new class of translation planes, Ann. Discrete Math., 37:7–20, North-Holland, Amsterdam, 1988.

[20] R. D. Baker, G. L. Ebert, T. Penttila : Hyperbolic fibrations and q-clans, (submitted to J. Geom.).

[21] A. Barlotti : Un'estensione del teorema di Segre-Kustaanheimo, Boll. Un. Mat. Ital. 10(3):498–506, 1955.

[22] O. E. Barriga : On the planes of Narayana Rao and Satyanarayana, J. Combin. Theory Ser. A, 45(1):148–151, 1987.

[23] D. Betten : 4-dimensionale Translationsebenen mit 8-dimensionaler Kollineationsgruppe. Geometriae Dedicata, 2:327–339, 1973.

[24] A. Beutelspacher, U. Rosenbaum : *Projective geometry: from foundations to applications*, Cambridge University Press, Cambridge, 1998.

[25] G. Birkhoff, J. von Neumann : The logic of quantum mechanics, Ann. of Math., 37(4):823–843, 1936.

[26] A. Blokhuis, M. Lavrauw, S. Ball : On the classification of semifield flocks, (submitted).

[27] A. Bonisoli : On the sharply 1-transitive subsets of PGL$(2, p^m)$, J. Geom., 31(1-2):32–41, 1988.

[28] R. H. Bruck, R. C. Bose : The construction of translation planes from projective spaces, J. Algebra, 1:85–102, 1964.

[29] A. A. Bruen, J. W. P. Hirschfeld : Applications of line geometry over finite fields, II, The Hermitian surface, Geom. Dedicata 7:333–353, 1978.

[30] F. Buekenhout (Ed.) : *Handbook of Incidence Geometry*, Buildings and foundations, North-Holland, Amsterdam, 1995.

[31] F. Buekenhout, E. E. Shult : On the foundations of polar geometry, Geom. Ded., 3:155–170, 1974.

[32] J. Cannon, C. Palyoust : An introduction to MAGMA, University of Sydney, Australia, 1993.

[33] P. J. Cameron : Projective and polar spaces, QMW Maths Notes, 13, Queen Mary and Westfield College, School of Mathematical Sciences, London, (year unknown).

[34] W. Cherowitzo : α-flocks and hyperovals, Geom. Dedicata, 72(3):221–246, 1998.

[35] W. Cherowitzo, C. M. O'Keefe, T. Penttila : A unified construction of finite geometries associated with q-clans in characteristic two, Adv. Geom., 3(1):1–21, 2003.

[36] W. Cherowitzo, T. Penttila, I. Pinneri, G. F. Royle : Flocks and ovals, Geom. Dedicata, 60(1):17–37, 1996.

[37] S. D. Cohen, M. J. Ganley : Commmutative semifields, two dimensional over their middle nuclei, J. Algebra, 75:373–385, 1982.

[38] S. D. Cohen, M. J. Ganley : Some classes of translation planes, Quart. J. Math. Oxford Ser. (2), 35(138):101–113, 1984.

[39] F. De Clerck, C. Herssens : Flocks of the quadratic cone in $\mathrm{PG}(3,q)$, for q small, The CAGe Reports, 8, 1992.

[40] F. De Clerck, H. Gevaert, J. A. Thas : Flocks of a quadratic cone in $\mathrm{PG}(3,q)$, $q \leq 8$, Geom. Dedicata, 26(2):215–230, 1988.

[41] F. De Clerck, T. Penttila : personal communication, 1997.

[42] F. De Clerck, L. Storme, J. A. Thas, H. Van Maldeghem (Eds.) : *Generalized polygons, Proceedings of the Academy Contact Forum, 20 October 2000*, Koninklijke Vlaamse Academie van Belgie, Universa Press, Belgium, 2001.

[43] P. Dembowski : *Finite geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer-Verlag, Berlin-New York, 1968.

[44] De Soete, J. A. Thas : A characterization theorem for the generalized quadrangle $T_2^*(O)$ of order $(s, s+2)$, Ars. Comb., 17:225–242, 1984.

[45] L. E. Dickson : On finite algebras, Nachr. kgl. Ges. Wiss. Göttingen, pp. 358–393, 1905.

[46] L. E. Dickson : Linear algebras with associativity not assumed, Duke Math. J., 1:113–125, 1935.

[47] N. Durante : *Piani Inversivi e Flock di Quadriche*, Tesi di laurea in matematica, Università degli Studi di Napoli, and Universiteit Gent, 1992.

[48] W. Feit, G. Higman : The nonexistence of certain generalized polygons, J. Algebra, 1:114–131, 1964.

[49] J. C. Fisher, J. A. Thas : Flocks in PG$(3, q)$, Math. Z., 169(1):1–11, 1979.

[50] M. J. Ganley : Central weak nucleus semifields, European J. Combin., 2(4):339–347, 1981.

[51] H. Gevaert, N. L. Johnson, J. A. Thas : Spreads covered by reguli, Simon Stevin, 62:51–62, 1988.

[52] M. Hall, Jr. : Affine generalized quadrilaterals, Studies in Pure Mathematics, 113–116, Academic Press, London, 1971.

[53] D. G. Higman : Invariant relations, coherent configurations and generalized polygons, Math. Centre Tracts, 57:27–43, Math. Centrum, Amsterdam, 1974.

[54] Y. Hiramine, M. Matsumoto, T. Oyama : On some extension of 1-spread sets, Osaka J. Math., 24(1):123–137, 1987.

[55] J. W. P. Hirschfeld : *Projective geometries over finite fields*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1979, second edition, 1998.

[56] J. W. P. Hirschfeld : *Finite projective spaces of three dimensions*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1985.

[57] J. W. P. Hirschfeld, J. A. Thas : *General Galois geometries*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1991.

[58] D. R. Hughes, F. C. Piper : *Projective planes*, Graduate Texts in Mathematics, Vol. 6. Springer-Verlag, New York-Berlin, 1973.

[59] N. L. Johnson : Semifield flocks of quadratic cones, Simon Stevin, 61(3-4):313–326, 1987.

[60] N. L. Johnson : Sequences of derivable translation planes, Osaka J. Math., 25:519–530, 1988.

[61] N. L. Johnson : Flocks of hyperbolic quadrics and translation planes admitting affine homologies, J. Geom., 34(1-2):50–73, 1989.

[62] N. L. Johnson : Derivation of partial flocks of quadratic cones, Rend. Mat. Appl. (7), 12(4):817–848, 1992.

[63] N. L. Johnson, G. Lunardon, F. W. Wilke : Semifield skeletons of conical flocks, J. Geom., 40(1-2):105–112, 1991.

[64] N. L. Johnson, S. E. Payne : Flocks of Laguerre planes and associated geometries, Lecture Notes in Pure and Appl. Math., 190:51–122, Dekker, New York, 1997.

[65] M. J. Kallaher : *Affine planes with transitive collineation groups*, North-Holland Publishing Co., New York-Amsterdam, 1982.

[66] W. M. Kantor : Generalized quadrangles associated with $G_2(q)$, J. Combin. Theory Ser. A, 29(2):212–219, 1980.

[67] W. M. Kantor : Ovoids and translation planes, Can. J. Math., 34(5):1195–1207, 1982.

[68] W. M. Kantor : On point-transitive affine planes, Israel J. Math., 42(3):227–234, 1982.

[69] W. M. Kantor : Some generalized quadrangles with parameters q^2, q, Math. Z., 192:45–50, 1986.

[70] W. M. Kantor : Generalized quadrangles, flocks, and BLT sets, J. Combin. Theory Ser. A, 58(1):153–157, 1991.

[71] N. Knarr : A geometric construction of generalized quadrangles from polar spaces of rank three, Results Math., 21(3-4):332–344, 1992.

[72] D. E. Knuth : Finite semifields and projective planes, J. Algebra, 2:182–217, 1965.

[73] M. Lavrauw, T. Penttila : On eggs and translation generalised quadrangles, J. Combin. Theory Ser. A, 96(2):303–315, 2001.

[74] M. Law, T. Penttila : Some flocks in characteristic 3, J. Combin. Theory Ser. A, 94(2):387–392, 2001.

[75] M. Law, T. Penttila : Classification of flocks of the quadratic cone over fields of order at most 29, Adv. Geom., (accepted).

[76] G. Lunardon : A remark on the derivation of flocks, *Advances in finite geometries and designs (Chelwood Gate, 1990)*, 299–309, Oxford Sci. Publ., Oxford Univ. Press, New York, 1991.

[77] G. Lunardon : Flocks, ovoids of $Q(4, q)$ and designs, Geom. Dedicata, 66(2):163–173, 1997.

[78] H. Lüneburg, *Translation planes*, Springer-Verlag, Berlin-New York, 1980.

[79] F. Mylle : *Flocks van Kwadrieken in* $PG(3, q)$, M.S. Thesis, Universiteit Gent, 1991.

[80] M. L. Narayana Rao, K. Satyanarayana, G. Vithal Rao : On a class of translation planes of square order, Discrete Math. 66(1-2):175–190, 1987.

[81] C. M. O'Keefe, T. Penttila : A new hyperoval in $PG(2, 32)$, J. Geom., 44(1-2):117–139, 1992.

[82] C. M. O'Keefe, J. A. Thas : Partial flocks of quadratic cones with a point vertex in $PG(n, q)$, n odd, J. Algebraic Combin., 6(4):377–392, 1997.

[83] W. F. Orr : *The Miguelian inversive plane $IP(g)$ and the associated projective planes*, Ph.D. Thesis, University of Wisconsin, 1973.

[84] T. G. Ostrom : *Finite translation planes*, Lecture Notes in Mathematics, Vol. 158 Springer-Verlag, Berlin-New York 1970.

[85] G. Panella : Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito, Boll. Un. Mat. Ital. 10(3):507–513, 1955

[86] S. E. Payne : The Subiaco notebook : An introduction to q-clan geometry, Unpublished notes. The .ps file is available on S. E. Payne's homepage http://www-math.cudenver.edu/ spayne/.

[87] S. E. Payne : Nonisomorphic generalized quadrangles, J. Algebra, 18:201–212, 1971.

[88] S. E. Payne : Generalized quadrangles as group coset geometries, Congr. Numer., 29:717–734, 1980.

[89] S. E. Payne : A new infinite family of generalized quadrangles, Congr. Numer., 49:115–128, 1985.

[90] S. E. Payne : Spreads, flocks, and generalized quadrangles, J. Geom., 33(1-2):113–128, 1988.

[91] S. E. Payne : The Thas-Fisher generalized quadrangles, Ann. Discrete Math., 37:357–366, North-Holland, Amsterdam, 1988.

[92] S. E. Payne : An essay on skew translation generalized quadrangles, Geom. Dedicata, 32(1):93–118, 1989.

[93] S. E. Payne : Collineations of the generalized quadrangles associated with q-clans, Ann. Discrete Math., 52:449–461, North-Holland, Amsterdam, 1992.

[94] S. E. Payne : The fundamental theorem of q-clan geometry, Des. Codes Cryptogr., 8(1-2):181–202, 1996.

[95] S. E. Payne : The Law-Penttila q-clan geometries, *Finite Geometries (Fourth Isle of Thorns Conference, Sussex, UK, 2000)*, pp. 295–303, Kluwer, Dordrecht, 2001.

[96] S. E. Payne : Flock generalized quadrangles and related structures : an update, *Generalized polygons, Proceedings of the Academy Contact Forum, 20 October 2000*, Koninklijke Vlaamse Academie van Belgie, Universa Press, Belgium, 2001.

[97] S. E. Payne, L. A. Rogers : Local group actions on generalized quadrangles, Simon Stevin, 64(3-4):249–284, 1990.

[98] S. E. Payne, J. A. Thas : *Finite generalized quadrangles*, Research Notes in Mathematics, 110, Pitman, Boston, Massachusetts, 1984.

[99] S. E. Payne, J. A. Thas : Conical flocks, partial flocks, derivation, and generalized quadrangles, Geom. Ded., 38:229–243, 1991.

[100] S. E. Payne, J. A. Thas : Generalized quadrangles, BLT-sets, and Fisher flocks, Congr. Numer., 84:161–192, 1991.

[101] T. Penttila : Regular cyclic BLT-sets, Rend. Circ. Mat. Palermo (2) Suppl., 53:167–172, 1998.

[102] T. Penttila, G. F. Royle : On hyperovals in small projective planes, J. Geom., 54(1-2), 91–104, 1995.

[103] T. Penttila, G. F. Royle : BLT-sets over small fields, Australas. J. Combin., 17:295–307, 1998.

[104] T. Penttila, B. Williams : Ovoids of parabolic spaces, Geom. Dedicata, 82(1-3), 1–19, 2000.

[105] B. Segre : Ovals in a finite projective plane, Canad. J. Math. 7:414–416, 1955.

[106] B. Segre : Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane, Ann. Mat. Pura Appl. (4), 64:1–76, 1964.

[107] E. Shult : m-systems and the BLT property, Ohio State Univ. Math. Res. Inst. Publ., 4:83–91, de Gruyter, Berlin, 1996.

[108] D. E. Taylor : *The geometry of the classical groups*, Sigma Series in Pure Mathematics, 9, Heldermann Verlag, Berlin, 1992.

[109] J. A. Thas : Flocks of finite egglike inversive planes, *Finite geometric structures and their applications (C.I.M.E., II Ciclo, Bressanone, 1972)*, pp. 189–191, Edizioni Cremonese, Rome, 1973.

[110] J. A. Thas : Flocks of non-singular ruled quadrics in PG$(3, q)$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 59 (1975), no. 1-2, 83–85 (1976).

[111] J. A. Thas : Generalized quadrangles and flocks of cones, European J. Combin., 8(4):441–452, 1987.

[112] J. A. Thas : Maximal exterior sets of hyperbolic quadrics: the complete classification, J. Combin. Theory Ser. A, 56(2):303–308, 1991.

[113] J. A. Thas : A characterization of the Fisher-Thas-Walker flocks, Simon Stevin, 67(3-4):219–226, 1993.

[114] J. A. Thas : Generalized quadrangles of order (s, s^2), I, J. Combin. Theory Ser. A, 67(2):140–160, 1994.

[115] J. A. Thas : Generalized quadrangles of order (s, s^2), II, J. Combin. Theory Ser. A, 79(2):223–254, 1997.

[116] J. A. Thas : Symplectic spreads in PG$(3, q)$, inversive planes and projective planes, Discrete Math., 174(1-3):329–336, 1997.

[117] J. A. Thas : Generalized quadrangles of order (s, s^2), III, J. Combin. Th., Ser. A, 87:247–272, 1999.

[118] J. A. Thas : Characterizations of translation generalized quadrangles, Des. Codes Cryptogr., 23(2):249–257, 2001.

[119] J. A. Thas : Geometrical constructions of flock generalized quadrangles, J. Combin. Theory Ser. A, 94(1):51–62, 2001.

[120] J. A. Thas, C. Herssens, F. De Clerck : Flocks and partial flocks of the quadratic cone in PG$(3, q)$, London Math. Soc. Lecture Note Ser., 191:379–393, Cambridge Univ. Press, Cambridge, 1993.

[121] J. A. Thas, S. E. Payne : Classical finite generalized quadrangles : a combinatorial study, Ars. Comb., 2:57–110, 1976.

[122] J. A. Thas, S. E. Payne : Spreads and ovoids in finite generalized quadrangles, Geom. Dedicata, 52(3):227–253, 1994.

[123] K. Thas : On symmetries and translation generalized quadrangles, *Finite Geometries (Fourth Isle of Thorns Conference, Sussex, UK, 2000)*, pp. 333–345, Kluwer, Dordrecht, 2001.

[124] K. Thas : The classification of generalized quadrangles with two translation points, Beiträge Algebra Geom., (to appear).

[125] K. Thas : On translation generalized quadrangles of which the translation dual arises from a flock, (preprint).

[126] J. Tits : Les groupes de Lie exceptionnels et leur interprétation géométrique, Bull. Soc. Math. Belg., 8:48–81, 1956.

[127] J. Tits : Sur la trialité et certains groupes qui s'en déduisent, 1959.

[128] J. Tits : Buildings of spherical type and finite BN-Pairs, Lecture Notes in Mathematics, vol. 386, Springer-Verlag, Berlin, 1974.

[129] H. van Maldeghem : *Generalized polygons*, Monographs in Mathematics, 93, Birkhäuser Verlag, Basel, 1998.

[130] O. Veblen, J. W. Young : *Projective geometry*, vol. I,II, Ginn and Co., Boston, 1916.

[131] F. D. Veldkamp : Polar Geometry I-V, Nederl. Akad. Wetensch. Proc. Ser. A, 62,63 = Indag. Math., 21:512–551, 22:207–212, 1959.

[132] M. Walker : A class of translation planes, Geometriae Dedicata, 5(2):135–146, 1976.

[133] B. Williams : *Ovoids of parabolic and hyperbolic spaces*, PhD Thesis, University of Western Australia, 1998.

[134] E. Witt : Theorie der quadratischen Formen in beliebigen Körpern, J. reine angew. Math., 176:31–44, 1937.

Index