Flag-Transitive Linear Spaces and Line Spreads of Projective Spaces

Michael Pauley

April 28, 2006

Abstract

A linear space is an incidence structure of points and lines having the property that there is exactly one line incident with any two given points. Finite linear spaces can be used to make experimental designs and error correcting codes.

The collineations of a linear space are the bijections from the linear space to itself which preserve incidence. A linear space is called *flag-transitive* if for any pair of points P, Q and any lines l through P and m through Q there is a collineation mapping P to Q and l to m. Flag-transitive linear spaces have a very high level of symmetry.

Using the classification of finite simple groups, Buekenhout, Delandtsheer, Doyen, Kleidman, Liebeck and Saxl have essentially given a classification of the finite flag-transitive linear spaces. The only remaining case is when the transitive group is a subgroup of the one dimensional affine group $A\Gamma L_1(q)$. This is called the *one dimensional affine case*. Kantor has given some classes of one dimensional affine linear spaces, but there are many more which do not fit into any of these classes.

A line spread is a set of lines which partition the projective space $PG_d(q)$. A line spread which admits a transitive group can be used to construct a flag-transitive linear space. Using the GAP computer algebra system, we will search for and classify transitive line spreads of some projective spaces and we will construct an infinite class of transitive line spreads which give new one dimensional affine linear spaces.

Acknowledgments

First and foremost, I thank my supervisor John Bamberg, for your encouragement and help in this project. Thanks to you I learned heaps of great maths, and I had a lot of fun with this project. Thanks to Maska Law for proof reading and lots of great suggestions, Tim Penttila for some helpful suggestions regarding searching for line spreads, and to Sven Reichard for helping me read [32].

Contents

Chapter 1

Introduction

A linear space is an incidence structure of points and lines such that between any two points there is a unique line. Flag-transitive linear spaces are those whose automorphism groups act transitively on their flags, that is, their point-line incidence pairs. The classification of finite flag-transitive linear spaces was announced in 1990 in [8], and it claimed, "Details of the proof of the theorem will appear elsewhere," citing a reference titled "The classification of flag-transitive finite linear spaces" by the same authors. To this date, this reference has not appeared. A single complete proof has never been published – the proofs of various parts of the theorem were slowly published over the years – and it was not until twelve years later that the final piece of the puzzle was published in [31] by Saxl, who wrote,

> The results of this paper were announced in [BDDKLS], as part of the classification of flag-transitive linear spaces. It was then intended to publish the complete proof of this classification in book form, by these six authors. However, that project has fallen through for various reasons, and it appears that the proof will now be published in parts.

The proof begins with the Higman-McLaughlin Theorem, which tells us that the automorphism group must be primitive. The O'Nan-Scott theorem can then be applied, and various cases can be eliminated until only two remain: either the automorphism group is *almost simple* or it is *affine*. In the almost simple case, the flag-transitive linear spaces have been completely classified, but one situation remains open in the affine case: the points of the linear space form a field, and the automorphism group is a subgroup of $A\Gamma L_1(q)$, the group of one-dimensional semilinear affine transformations. This is called the *one-dimensional affine* case, and in this

thesis we will examine the one-dimensional affine case and construct some new linear spaces of this kind.

In Chapter 2 we will develop the necessary group and field theory to study flag-transitive linear spaces. In Chapter 3 we will introduce the flag-transitive linear spaces and discuss the results of the classification theorem. Chapter 4 will introduce the technique that we will use to construct flag-transitive linear spaces of the one-dimensional affine type: it is called the André/Bruck-Bose construction and it was created in [1] and [5]. The construction begins with a t-spread: a partition of the projective space $\mathrm{PG}_d(q)$ into projective subspaces of a fixed dimension t. A new linear space $\mathscr{S}$ is formed: the *points* of $\mathscr{S}$ are the points of the projective space $\mathrm{PG}_{d+1}(q)$ which do not lie in $\mathrm{PG}_d(q)$, and the *lines* of $\mathscr{S}$ are the subspaces of $\mathrm{PG}_{d+1}(q)$ which meet $\mathrm{PG}_d(q)$ in an element of a spread. A line and a point of $\mathscr{S}$ are incident if the subspace contains the point in $\mathrm{PG}_{d+1}(q)$. The usefulness of the André/Bruck-Bose construction to our situation comes from the fact that *if the t-spread is transitive, then the resulting linear space will be flag-transitive.* In Chapter 5 we will examine the specific case when $t = 1$. In this case the t-spread is called a *line spread*, and we will use the GAP computer algebra package to search for line spreads, and we will construct an infinite class of line spreads which, submitted to the André/Bruck-Bose construction, give new flag-transitive linear spaces of the one-dimensional affine type. These results form part of a paper in preparation [26].

Chapter 2

Algebra

The combinatorial objects that will take centre stage in this thesis have a high degree of symmetry, and to study this symmetry we must begin with a look at group actions. We will introduce the notion of a transitive group action, and examine some properties of transitivity.

The construction of our objects will start from a finite field, and as such we need some tools for working with finite fields. In particular, we will introduce the norm and trace functions of a finite field, and we will see a link between the norm function and the minimal polynomials of field elements over subfields. We will then look at linear and semilinear transformations of finite fields, and the groups of invertible such transformations.

2.1 Group actions

Let G be a group, and let Ω be a set. An **action** of G on Ω is a homomorphism $\Phi : G \to \mathrm{Sym}(\Omega)$. If $g \in G$ and $\omega \in \Omega$ then we write

$$\omega^g$$

to mean $\Phi(g)(\omega)$, when Φ is understood. If H is a subgroup of G we write ω^H for the orbit of ω under H.

Example 2.1. Let G be a group. Then G has an action Φ on itself where

$$\Phi(g)(h) = g^{-1}hg.$$

This is called the *action by conjugation*.

Example 2.2. Let G be a group. Then G has an action Φ on itself by right multiplication:

$$\Phi(g)(h) = hg$$

In the case of a group acting on itself, the notation h^g explicitly refers to conjugation as in Example 2.1. If a group G acts on a set Ω, the **stabiliser** $\mathrm{Stab}_G(\omega)$ of a point $\omega \in \Omega$ is the subgroup of elements of G which fix ω. If S is a subset of Ω, then the stabiliser $\mathrm{Stab}_G(S)$ is the subgroup of elements of G which preserve S, that is, carry S to itself. If T is a *set of subsets* of Ω, then the stabiliser $\mathrm{Stab}_G(T)$ of T is the subgroup of elements of G which preserve T, that is, the subgroup of elements of G which carry every element of T to an element of T.

An action $\Phi : G \to \mathrm{Sym}(\Omega)$ is **faithful** if $\ker \Phi$ is the trivial group. So Φ is faithful if the only element of G fixing every point of Ω is the identity of G. In this case, G can be thought of as a subgroup of $\mathrm{Sym}(\Omega)$. If G is a group acting on a set Ω, we say that G acts **transitively** on Ω if for any $\alpha, \beta \in \Omega$ there exists $g \in G$ such that $\alpha^g = \beta$. This is equivalent to saying that G has only one orbit on Ω. If G is finite then the Orbit-Stabiliser Theorem tells us that $|\Omega| \,\big|\, |G|$. A group G acts **semiregularly** on a set Ω if only the identity element fixes any point of Ω. The group G acts **regularly** on Ω if it is both semiregular *and* transitive, that is, if for any $\alpha, \beta \in \Omega$ there exists *exactly one* $g \in G$ such that $\alpha^g = \beta$.

Example 2.3. The action by right multiplication of Example 2.2 is regular. The unique $g \in G$ such that $\alpha g = \beta$ is $g = \alpha^{-1}\beta$.

Lemma 2.4. *Let G be a group acting on a set Ω. If the action is transitive and faithful, and G is abelian, then the action is regular.*

Proof. Let $\omega \in \Omega$. Suppose that $g \in G$ such that $\omega^g = \omega$. Then, since the action is transitive, any point ν can be written as ω^f for some $f \in G$. But then $\nu^g = \omega^{fg} = \omega^{gf} = \omega^f = \nu$. Since this is true for any ν and the action is faithful, this means that g is the identity. □

Suppose G is a group, and A and B are subgroups of G. We say that A and B are **permutable** if AB (that is, the set of all products ab for $a \in A$ and $b \in B$) is equal to BA.

Lemma 2.5. *Suppose G is a group, and A and B are subgroups of G. Then A and B are permutable if and only if AB is a group.*

Proof. Suppose first that A and B are permutable. Let $x_1, x_2 \in AB$. Write $x_1 = a_1b_1$ and $x_2 = a_2b_2$ where $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then

$$x_1x_2 = a_1b_1a_2b_2.$$

Now $b_1a_2 \in BA = AB$, so we can write $b_1a_2 = a_3b_3$ for some $a_3 \in A$ and some $b_3 \in B$. Thus $x_1x_2 = a_1a_3b_3b_2 \in AB$. Furthermore,

$$\begin{aligned} x_1^{-1} &= (a_1b_1)^{-1} \\ &= b_1^{-1}a_1^{-1} \in BA = AB \end{aligned}$$

Hence AB is closed under multiplication and inversion (and $1 = 1.1 \in AB$) and so it is a group.

Now suppose that AB is a group. Let $a \in A$ and $b \in B$. Then $a = a.1 \in AB$ and $b = 1.b \in AB$ and so, since AB is a group, $ba \in AB$. This shows that $BA \subseteq AB$. Now if $x \in AB$, then since AB is a group, $x^{-1} \in AB$, and so x^{-1} can be written as ab for some $a \in A$ and some $b \in B$. Thus $x = b^{-1}a^{-1}$ which is in BA, showing that $AB = BA$. □

Lemma 2.6. *Suppose that G is transitive on Ω. Suppose that N is a normal subgroup of G, and let $\alpha \in \Omega$. Then the following are equivalent:*

(i) $G = N\mathrm{Stab}_G(\alpha)$*;*

(ii) N *is transitive;*

(iii) $G = \mathrm{Stab}_G(\alpha)N$.

Proof. *((i) $\Longrightarrow$ (ii).)* It suffices to prove that for any $\omega \in \Omega$ there exists $n \in N$ such that $\omega^n = \alpha$. Since G is transitive, there exists $g \in G$ such that $\omega^g = \alpha$. Write $g = ng'$ where $n \in N$ and $g' \in \mathrm{Stab}_G(\alpha)$. Then $\omega^{ng'} = \alpha$, but g'^{-1} fixes α, so $\omega^n = \omega^{ng'g'^{-1}} = \alpha$.

((ii) $\Longrightarrow$ (iii).) Let $g \in G$. Then there exists $n \in N$ such that

$$\alpha^g = \alpha^n.$$

So $gn^{-1} \in \mathrm{Stab}_G(\alpha)$. Thus $g \in \mathrm{Stab}_G(\alpha N)$.

((iii) $\Longrightarrow$ (i).) If $\mathrm{Stab}_G(\alpha)N$ is a group, then $\mathrm{Stab}_G(\alpha)$ and N are permutable, so $N\mathrm{Stab}_G(\alpha)$ is the same group. □

Suppose G is a group acting transitively on a set Ω. A **block of imprimitivity** is a nonempty subset $B \subseteq \Omega$ such that for every $g \in G$, either

- $B^g = B$, or
- $B^g \cap B = \varnothing$.

A group G acts **primitively** on a set Ω if the only blocks of imprimitivity are the singleton sets and Ω.

Lemma 2.7. *Let G be a group acting faithfully and primitively on a set Ω. Then any nontrivial normal subgroup of G acts transitively on Ω.*

Proof. Let $\omega \in \Omega$. We will show that the orbit ω^N of ω under N is all of Ω. For any $g \in G$ we have $(\omega^N)^g = (\omega^g)^N$ because N is normal. But $(\omega^g)^N$ is an orbit under N, so it is either *equal* to ω^N or *disjoint* from ω^N. Hence ω^N is a block of imprimitivity of G. But since G is primitive, ω^N is Ω or just $\{\omega\}$. But if $\omega^N = \{\omega\}$ then this must be true for *all* $\omega \in \Omega$, and so since G is faithful, and N is not the trivial group, $\omega^N = \Omega$, and N is transitive. □

2.2 Frobenius groups

Suppose that G is a group acting on a set Ω. If $g \in G$, then a **fixed point** of g is an element $\omega \in \Omega$ such that $\omega^g = \omega$. A **Frobenius group** is a group G acting on a set Ω with the property that *no non-identity element of G fixes more than one point*.

Theorem 2.8 (Frobenius). *Suppose G is a Frobenius group acting on Ω. Let*

$$H = \{g \in G : g \text{ fixes no point}\} \cup \{1\}.$$

Then H is a normal subgroup of G.

The proof of this theorem depends on character theory, and can be seen, for example, in [15, Theorem 16.8.8].

2.3 Group partitions

A **partition** of a group G is a set P of nontrivial subgroups of G such that

- $A \cap B = \{1\}$ for any $A, B \in P, A \neq B$
- for any $g \in G$ there exists $A \in P$ such that $g \in A$.

A partition is *nontrivial* if it has at least two elements. An *equal partition* is a partition into subgroups which are all the same size. A survey of group partitions is available in [35].

Example 2.9. There exists a nonabelian group G of order 27 with the following property: every element except the identity has order 3. (This is called the *extra-special group of order* 27.) The subgroups of G of order 3 form an equal partition of G.

2.4 The automorphism group of a group

Let G be a group. An **automorphism** of G is an isomorphism from G to itself. The set of all automorphisms of G form a group under composition, and we call this group the **automorphism group**, $\mathrm{Aut}(G)$ of G. Suppose G is a simple group. The centre Z of G is a normal subgroup, thus it is either 1 or G. If $Z = G$ then G is abelian, and hence it is a cyclic group of prime order. Otherwise, the map

$$\begin{aligned} f : G &\to G \\ g &\mapsto aga^{-1} \end{aligned}$$

is a nontrivial automorphism whenever $a \neq 1$. Thus G can be thought of as a subgroup of $\mathrm{Aut}(G)$. We define a group H to be **almost simple** if there is some simple group G such that $G \leq H \leq \mathrm{Aut}(G)$.

2.5 Division rings and fields

A **division ring** is a ring with a multiplicative identity, in which every nonzero element has a multiplicative inverse. A **field** is a division ring in which multiplication commutes. If $\mathbb{F}$ is a field and $\mathbb{K}$ is a subfield of $\mathbb{F}$, we can consider $\mathbb{F}$ to be a vector space over $\mathbb{K}$, that is, the elements of $\mathbb{F}$ are the *vectors* of this vector space, and the elements of $\mathbb{K}$ are the *scalars*.

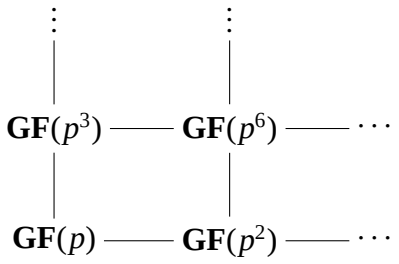
Suppose that $\mathbb{F}$ is a field and V is a vector space over $\mathbb{F}$. We define the **general linear group** $\mathrm{GL}(V)$ to be the group of invertible linear transformations $V \to V$. If $G \leq \mathrm{GL}(V)$ then we define the **endomorphism ring** $\mathrm{End}_G(V)$ to be the ring of linear transformations $\phi : V \to V$ such that $\phi g = g\phi$ for all $g \in G$, with operations composition and addition. If $G \leq \mathrm{GL}(V)$ we call G **irreducible** if G does not fix any nonzero proper subspace of V.

Lemma 2.10 (Schur's Lemma for vector spaces). *Suppose V is a finite-dimensional vector space. If G is an irreducible subgroup of* $\mathrm{GL}(V)$ *then* $\mathrm{End}_G(V)$ *is a division ring.*

Proof. Certainly the identity map is in $\mathrm{End}_G(V)$. Suppose that $\Phi \in \mathrm{End}_G(V)$, and that $z \in \ker \Phi$. Then $\Phi(z) = 0$, so for any $g \in G$, $g\Phi(z) = 0$. But then $\Phi g(z) = 0$ and so $gz \in \ker \Phi$. Thus $\ker \Phi$ is G-invariant, and so it is either V or the trivial subspace. In the first case, Φ is zero, and in the second case, it is invertible. □

The fields we are interested in have finitely many points. These are known as the **Galois fields** and Galois' Theorem tells us that (up to isomorphism) there is precisely one of order q

for each prime power q, and there are no others. We will write $\mathbf{GF}(q)$ to denote the Galois field of order q. When $q = p^n$ for a prime p we call p the **characteristic** of the field. $\mathbf{GF}(p^n)$ has a subfield of order p^m if and only if $m \mid n$. We can treat this field as $\mathbf{GF}(p^m)$ itself, and so the fields of a given characteristic are naturally embedded in each other.



2.5.1 Irreducible polynomials

An **irreducible polynomial**[1] over a field $\mathbb{F}$ is a polynomial P which cannot be written as a product of two smaller degree non-constant polynomials. If P is an irreducible polynomial of degree d over $\mathbf{GF}(q)$ then the roots of P are in $\mathbf{GF}(q^d)$, treating $\mathbf{GF}(q)$ as a subfield of $\mathbf{GF}(q^d)$.

Suppose that $\mathbf{GF}(q) \subseteq \mathbf{GF}(q^d)$ and $a \in \mathbf{GF}(q)$. The **minimal polynomial** of a is the monic polynomial P of smallest degree over $\mathbf{GF}(q)$ such that a is a root of P. The minimal polynomial always exists, because if it did not then $1, a, a^2, a^3, \cdots$ would all be different elements and so $\mathbf{GF}(q^d)$ would be an infinite field. The minimal polynomial is unique because if P and Q are monic polynomials such that $P(a) = Q(a) = 0$ then $(P - Q)(a) = 0$ and $P - Q$ is a polynomial of lower degree (which can then be scaled so as to make it monic.) Best of all: monic polynomials are *irreducible* because if $P(a)Q(a) = 0$ then since the only divisor of 0 is 0, it must be that $P(a) = 0$ or $Q(a) = 0$. So we see that a monic polynomial of degree d over $\mathbf{GF}(q)$ is irreducible if and only if it is the minimal polynomial of some element of $\mathbf{GF}(q^d)$.

Let P be a monic irreducible polynomial of degree d over $\mathbf{GF}(q)$, and let a be a root of P in $\mathbf{GF}(q^d)$. Then

$$a, a^q, a^{q^2}, \cdots, a^{q^{d-1}}$$

will be the d different conjugates of a, and since they are all roots of P, the polynomial P factorises over $\mathbf{GF}(q)^d$ as

$$P(x) = (x - a)(x - a^q)(x - a^{q^2}) \cdots (x - a^{q^{d-1}}).$$

[1] No relation to irreducible groups!

If P is a polynomial of degree d and a is a root of P, a test for the irreducibility of P is as follows: show that a lies in $\mathbf{GF}(q^d)$ but no proper subfield of $\mathbf{GF}(q^d)$. Then a will have d distinct conjugates, and they will all be roots of P, so that P will be the minimal polynomial of a (possibly scaled by a constant) and will therefore be irreducible.

If P is a polynomial of degree d that is irreducible over $\mathbf{GF}(q)$, then P is also irreducible over $\mathbf{GF}(q^k)$ whenever k is coprime to d. This is because the smallest field containing $\mathbf{GF}(q^k)$ which also contains a root of P is $\mathbf{GF}(q^{kd})$.

Finding irreducible polynomials can be rather a challenge, and in general we need to look at polynomials on an individual basis to see if they are irreducible. However, here we will construct a class of irreducible polynomials – one of degree p over $\mathbf{GF}(p)$ for each prime p – which we will use later to construct linear spaces.

Lemma 2.11. *Let*

$$P(x) = x^p + x^{p-1} + \cdots + x^2 + x - 1 \tag{2.5.1}$$

Then P is irreducible over $\mathbf{GF}(p)$.

Proof. Let z be a root of P. We will show that z is in $\mathbf{GF}(p^p)$ but not in any proper subfield of it. Now z is not 1 because $P(1) = \underbrace{1 + 1 + \cdots + 1 + 1}_{p \text{ times}} - 1 = -1$. So using the rule for a geometric series,

$$P(z) = \frac{z^{p+1} - 1}{z - 1} - 2. \tag{2.5.2}$$

The only proper subfield of $\mathbf{GF}(p^p)$ is $\mathbf{GF}(p)$, and if $z \in \mathbf{GF}(p)$ then $z^p = z$ and so

$$P(z) = \frac{z^2 - 1}{z - 1} - 2 = z - 1$$

which is not zero because $z \neq 1$. It remains to show that z is in $\mathbf{GF}(p^p)$. Indeed, if z is a root of P then writing $z^p z$ for z^{p+1} in (2.5.2),

$$\frac{z^p z - 1}{z - 1} - 2 = 0$$

and so

$$z^p = \frac{2z - 1}{z} \tag{2.5.3}$$

Now we will see that a general formula for z^{p^i} is

$$z^{p^i} = \frac{(i+1)z - i}{iz - (i-1)} \tag{2.5.4}$$

Certainly the formula holds for $i = 1$ by (2.5.3). Given that it is true for i, we have

$$\begin{aligned}
z^{p^{i+1}} &= \left(\frac{(i+1)z - i}{iz - (i-1)}\right)^p \\
&= \frac{(i+1)z^p - i}{iz^p - (i-1)} && \text{since } z \mapsto z^p \text{ is an automorphism} \\
&= \frac{(i+1)^{\frac{2z-1}{z}} - i}{i^{\frac{2z-1}{z}} - (i-1)} && \text{by equation 2.5.3} \\
&= \frac{(i+1)(2z-1) - iz}{i(2z-1) - (i-1)z} && \text{multiplying top and bottom by } z \\
&= \frac{(i+2)z - (i+1)}{(i+1)z - i}
\end{aligned}$$

and the formula holds for $i + 1$. Thus by induction, equation 2.5.4 holds for any integer $i \geq 1$. In particular,

$$z^{p^p} = \frac{(p+1)z - p}{pz - (p-1)} = z$$

So z is fixed by the automorphism $x \mapsto x^{p^p}$ so it is in $\mathbf{GF}(p^p)$. □

2.5.2 Norm and trace

The field of complex numbers contains the field of real numbers, and as a result the field of complex numbers can be treated as a vector space over the field of reals. If c is a complex number and its complex conjugate is $\bar{c}$, then we can calculate its *real part*:

$$\Re(c) = \frac{1}{2}(c + \bar{c})$$

and we can also calculate its *modulus*:

$$|c| = \sqrt{c\,\bar{c}}.$$

These are two functions which map $\mathbb{C}$ to $\mathbb{R}$. The first one is additive, ie. $\Re(c+d) = \Re(c) + \Re(d)$, and the second one is multiplicative, ie. $|cd| = |c||d|$. It would be nice if we could have analogous functions for finite fields!

Let $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^d)$. The automorphisms of $\mathbb{L}$ fixing $\mathbb{K}$ are the maps $\phi : x \to x^{q^k}$ for each k between 0 and $d-1$. The conjugates of an element are its images of an automorphism. We define the **norm** and **trace** maps N and Tr by

$$\begin{aligned} N_{L/K} : \mathbb{L} &\to \mathbb{K} \\ x &\to x x^q x^{q^2} \cdots x^{q^{d-1}} \\ Tr_{L/K} : \mathbb{L} &\to \mathbb{K} \\ x &\to x + x^q + x^{q^2} + \cdots + x^{q^{d-1}} \end{aligned}$$

That is, the norm of x is the product of all its conjugates, and the trace of x is the sum of all its conjugates. Since automorphisms preserve addition and multiplication, we can see that N is a multiplicative function and Tr is an additive function. The norm N is the finite field analogue of the modulus $|\cdot|$, except that we do not take a square root. The trace Tr is the finite field analogue of the real part $\Re$, except that we do not divide by two.

If we write a complex number as $a + bi$ (where i is the imaginary constant) then a property of the modulus is that

$$|a + bi| = \sqrt{a^2 + b^2}.$$

This property has an analogue in the following lemma:

Lemma 2.12. *Let $\mathbb{L} = \mathbf{GF}(q) \subset \mathbb{F} = \mathbf{GF}(q^m)$ Let $b \in \mathbb{F}$ such that the minimal polynomial P of b over L has degree d. Then for any $u, v \in \mathbb{L}$,*

$$N(u - bv) = v^m P(uv^{-1})^{m/d}$$

Proof. Let σ be the Frobenius automorphism of $\mathbb{F}$ over $\mathbb{L}$, and let $u, v \in \mathbb{L}$. Then

$$\begin{aligned} N(u - bv) &= \prod_{i=0}^{m-1} (u - bv)^{\sigma^i} \\ &= \prod_{i=0}^{m-1} (u - b^{\sigma^i} v) && \text{since } \sigma \text{ is an automorphism fixing } \mathbb{L} \\ &= \prod_{i=0}^{m-1} \left(v(uv^{-1} - b^{\sigma^i}) \right) \end{aligned}$$

Now, $b^{\sigma^d} = b$ and so the above is just m/d copies of

$$\prod_{i=0}^{d-1} \left(v(uv^{-1} - b^{\sigma^i})\right)$$
$$= v^d P(uv^{-1})$$

and so the result follows. □

Example 2.13. Let $P(x) = x^3 + x^2 + x - 1$ over the field **GF**(3). We know this polynomial is irreducible by Lemma 2.11. Let b be a root of P in the field **GF**(3^3). Then for any $u, v \in$ **GF**(3) we have

$$N(u - bv) = u^3 + u^2v + uv^2 - v^3.$$

2.6 Linear and semilinear groups

The general linear group of a vector space gives us the group of transformations which preserve addition and scaling. When our vector space is over a field which has nontrivial automorphisms, we can form a slightly larger group of transformations which preserve addition and *almost* preserve scaling. A **semilinear transformation** on a vector space V over a field $\mathbb{F}$ is a map $f : V \to V$ such that for any $x, y \in V$ and any $\alpha \in \mathbb{F}$

$$f(x + y) = f(x) + f(y)$$
$$f(ax) = a^\sigma f(x)$$

where σ is some fixed automorphism of $\mathbb{F}$. When $\mathbb{F} =$ **GF**(q) and $V = \mathbb{F}^d$, the semilinear transformations of V are the maps

$$f : V \to V$$
$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto A \begin{pmatrix} x_1^\sigma \\ \vdots \\ x_n^\sigma \end{pmatrix}$$

for some matrix A and some automorphism σ. We define $\Gamma\mathrm{L}(V)$ to be the group of all invertible semilinear transformations $V \to V$. In particular, if p is a prime then $\Gamma\mathrm{L}_1(p^d)$ is the group of maps

$$f : \mathbb{F} \to \mathbb{F}$$
$$x \mapsto \alpha x^{p^i}$$

for $\alpha \in \mathbb{F}^*, i \in \{0, \cdots, d-1\}$. Now $\mathbf{GF}(p^d)$ is a d-dimensional vector space over $\mathbf{GF}(p)$, and the semilinear transformations of $\mathbf{GF}(p^d)$ are additive, so they are linear with respect to $\mathbf{GF}(p)$. Thus, treating $\mathbf{GF}(p^d)$ as the vector space $\mathbf{GF}(p)^d$ over $\mathbf{GF}(p)$,

$$\Gamma\mathrm{L}_1(p^d) \leq \mathrm{GL}_d(p).$$

Now $\mathrm{GL}_1(p^d)$ is the group of maps $f : x \mapsto \alpha x$ for $\alpha \in \mathbb{F}^*$ so this group is contained in $\Gamma\mathrm{L}_1(p^d)$. Furthermore we have the following relationship:

Proposition 2.14. *Let p be a prime and d be a positive integer. Then, treating $\mathbf{GF}(p^d)$ as the vector space over $\mathbf{GF}(p)$,*

$$N_{\mathrm{GL}_d(p)}(\mathrm{GL}_1(p^d)) = \Gamma\mathrm{L}_1(p^d)$$

where $N_{\mathrm{GL}_d(p)}(\mathrm{GL}_1(p^d))$ is the normaliser of $\mathrm{GL}_1(p^d)$ in $\mathrm{GL}_d(p)$.

Proof. Let $f \in N_{\mathrm{GL}_d(p)}(\mathrm{GL}_1(p^d))$. The group $\mathrm{GL}_d(p)$ is the group of additive maps on $\mathbf{GF}(p^d)$, so for any $x, y \in \mathbf{GF}(p^d)$,

$$f(x+y) = f(x) + f(y).$$

Let $g \in \mathrm{GL}_1(p^d)$. Then g is of the form

$$\begin{aligned} g : \mathbb{F} &\to \mathbb{F} \\ x &\mapsto ax \end{aligned}$$

and so, since f normalises g, there is some b such that

$$f(ax) = bf(x)$$

for all x. Substituting $x = 1$ gives $f(a) = bf(1)$ so $b = f(a)/f(1)$. Let

$$\begin{aligned} h : \mathbb{F} &\to \mathbb{F} \\ x &\mapsto f(x)/f(1). \end{aligned}$$

Then h is additive because f is additive. But

$$\begin{aligned} h(ax) &= \frac{f(ax)}{f(1)} \\ &= \frac{(f(a)/f(1))\, f(x)}{f(1)} \\ &= \frac{f(a)}{f(1)} \frac{f(x)}{f(1)} \\ &= h(a)h(x). \end{aligned}$$

This is true for any $a \in \mathbb{F}^*$ (and $h(0x) = 0 = h(0)h(x)$) and so h is multiplicative. Thus h is an automorphism σ and so, letting $\alpha = f(1)$, f is the map $f : x \mapsto \alpha x^\sigma$. □

The two groups $\mathrm{GL}_d(q)$ and $\Gamma\mathrm{L}_d(q)$ can be extended to their **affine** versions:

$$\mathrm{AGL}_d(q) = \{x \mapsto x^g + c : g \in \mathrm{GL}_d(q), c \in \mathbf{GF}(q)^d\}$$
$$\mathrm{A}\Gamma\mathrm{L}_d(q) = \{x \mapsto x^g + c : g \in \Gamma\mathrm{L}_d(q), c \in \mathbf{GF}(q)^d\}$$

Since multiplication and automorphisms both preserve addition, we can see that $\mathrm{GL}_d(q) \trianglelefteq \mathrm{AGL}_d(q)$ and $\Gamma\mathrm{L}_d(q) \trianglelefteq \mathrm{A}\Gamma\mathrm{L}_d(q)$.

Chapter 3

Linear spaces

A familiar place where geometry is done is the Euclidean plane. It has the following property: given any two points, there is a *exactly one* line between them. A linear space is a geometric object in which the rule *between any two points there is a unique line* applies[1]. In this thesis we are particularly interested in *finite* linear spaces, that is, linear spaces with finitely many points and finitely many lines. An example of such a linear space is in Figure 3.1.

In this chapter we will introduce linear spaces and give some constructions. We will introduce the notion of a *flag-transitive* linear space, and present the theorem of Buekenhout, Delandtsheer, Doyen, Kleidman, Liebeck and Saxl, which classifies the finite flag-transitive linear spaces, up to the single remaining case of the one-dimensional affine linear spaces.

3.1 Point-line incidence structures and linear spaces

An **incidence structure** $\mathscr{S}$ is made of three things:

- A set $\mathscr{P}$ of objects called **points**;
- A set $\mathscr{B}$ of objects called **blocks**;
- A relation between $\mathscr{P}$ and $\mathscr{B}$ called **incidence**. If a point p is incident with a block B we write p I B.

Suppose that $\mathscr{S}_1$ and $\mathscr{S}_2$ are incidence structures. An **isomorphism** ϕ between $\mathscr{S}_1$ and $\mathscr{S}_2$ is an invertible map which takes the points of $\mathscr{S}_1$ to points of $\mathscr{S}_2$, and takes the blocks of $\mathscr{S}_1$ to

[1] "Linear space" is used by some authors as a synonym for vector space.

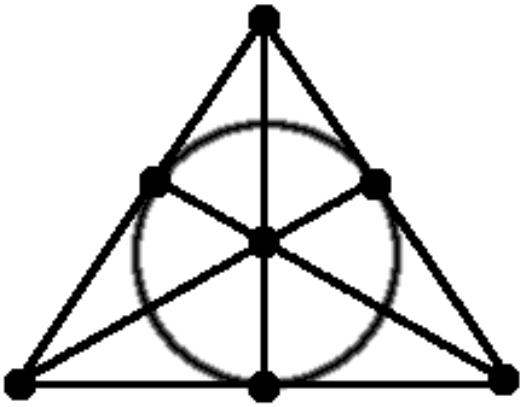


Figure 3.1: The Fano plane, the smallest example of a projective plane. This projective plane has 7 points and 7 lines, counting the circle as a line.

blocks of $\mathscr{S}_2$, and which satisfies

$$p \mathrel{\mathrm{I}} B \iff \phi(p) \mathrel{\mathrm{I}} \phi(B).$$

The following situation is common: $\mathscr{B}$ is a set of subsets of $\mathscr{P}$, and a point and a block are incident whenever the block contains the point. If this is the case for two linear spaces $\mathscr{S}_1$ and $\mathscr{S}_2$ then an isomorphism from $\mathscr{S}_1$ to $\mathscr{S}_2$ can simply be a bijection from the points of $\mathscr{S}_1$ to the points of $\mathscr{S}_2$ such that the image of a line in $\mathscr{S}_1$ is a line in $\mathscr{S}_2$.

An incidence structure is called a **linear space** if it satisfies the following:

- Every block is incident with at least two points;
- For any two distinct points, there is exactly one block incident with both of them.

In this situation we refer to the blocks as **lines**, and when a point and a line are incident, we say that the point *lies on* the line, or the line *runs through* the point. A linear space is **nontrivial** if some line runs through at least three points. If a set of points lie on a common line, we say they are **collinear**. A linear space is **nondegenerate** if it contains a set of four points, no three of which are collinear.

Any two lines of a linear space share at most one point in common. For if ℓ and m were two lines meeting in two points P and Q, then there would not be exactly one line through P and Q. If two lines ℓ and m share a point P in common, we say they **meet** at P. If P and Q are two points of a linear space $\mathscr{S}$ then we write PQ to denote the unique line that runs through both of them.

Example 3.1. Let V be a vector space over a field $\mathbb{F}$. The points of our linear space are all the elements of V. The lines are all the sets $\{a + b\lambda : \lambda \in \mathbb{F}\}$ for $a, b \in V$. A point $x \in V$ is incident with a line $\ell \subset V$ if $x \in \ell$. The space thus formed is called a **desarguesian affine space** . If d is the dimension of V then we write this space as $\mathrm{AG}_d(\mathbb{F})$, and if $\mathbb{F}$ is a finite field of order q then we can also write it as $\mathrm{AG}_d(q)$. If in this example we take V to be $\mathbb{R}^2$, then the resulting linear space is the Euclidean plane.

Example 3.2. A vector space V of dimension at least 2 can be turned into another kind of linear space, $\mathrm{PG}_{d-1}(\mathbb{F})$ (or $\mathrm{PG}_{d-1}(q)$ when $F = \mathbf{GF}(q)$.) The points of this space will be the one-dimensional subspaces of V. The lines are the two-dimensional subspaces of V. (Note that if the dimension of V is two then the resulting linear space will consist of a single line, so it will be degenerate.) A point P is incident with a line ℓ if P is a subspace of ℓ. In particular, if we take $V = \mathbb{R}^3$, then the resulting linear space is the *real projective plane*.

A **flag** of a linear space is an *incident point-line pair*, that is, a pair (P, ℓ) where P is a point, ℓ is a line, and P and ℓ are incident. A linear space is **regular**[2] if every line runs through the same number of points. If $\mathbb{F} = \mathbf{GF}(q)$ then the linear space of Example 3.1 is regular because every line has q points, and the linear space of Example 3.2 is regular because every line has

$$(q^d - 1)/(q - 1)$$

points. A $t - (v, k, \lambda)$ **block design** is an incidence structure in which

- there are v points;
- every block is incident with exactly k points;
- given any set of t points, there are precisely λ blocks which are incident with all of them.

If we think of lines as a kind of block, then the class of linear spaces and the class of $t - (v, k, \lambda)$ block designs have non-trivial intersection: this is the class of *regular linear spaces* or $2 - (v, k, 1)$*-designs*.

Proposition 3.3. *Suppose that $\mathscr{S}$ is a regular linear space with v points and k points on each line. Then the number of lines through each point is*

$$\frac{v - 1}{k - 1} \tag{3.1.1}$$

[2]This is an unfortunate collision of definitions, because there is no guarantee that a regular linear space admits a regular group, nor that any linear space admitting a regular group must be regular.

and the number of lines is

$$\frac{v(v-1)}{k(k-1)}. \tag{3.1.2}$$

Proof. The first statement follows from the fact that if α is a point of our linear space, then the lines through α partition the points other than α. The second statement follows from counting the number of flags in two different ways. □

3.2 Projective spaces

A **triangle** is a set of 3 points which do not lie on a common line. A **quadrangle** is a set of 4 points, no 3 of which lie on a common line. A nondegenerate linear space π is called a **projective plane** if any two lines of π meet.

Proposition 3.4. *Let π be a projective plane. Then there is a constant n such that every line of π runs through $n+1$ points, every point of π lies on $n+1$ lines, and π has n^2+n+1 points and n^2+n+1 lines.*

Proof. Let P be a point of π, and let ℓ be a line which does not run through P. For every point Q on ℓ, there is a unique line between P and Q. Thus the lines through P and the points on ℓ are in one-to-one correspondence. Given any two points P and Q, choose a line ℓ that does not run through either of them. The number of lines through P equals the number of points on ℓ which equals the number of lines through m. Thus the number of lines through P equals the number of lines through Q. Similarly, let ℓ and m be lines. Choose a point P which does not lie on either ℓ or m. The number of points on ℓ equals the number of lines through P which equals the number of points on m. Thus any two points have the same number $n+1$ of lines through them, and any two lines have the same number $m+1$ of points on them, and choosing an arbitrary point and a line not through it shows that $m+1=n+1$.

Now suppose that every line has $n+1$ points on it and every point has $n+1$ lines through it. If v is the number of points, then by Equation 3.1.1,

$$n+1=\frac{v-1}{n}$$

and so $v=n^2+n+1$. If r is the number of lines, then by Equation 3.1.2,

$$r=\frac{(n^2+n+1)(n^2+n)}{(n+1)n}=n^2+n+1.$$

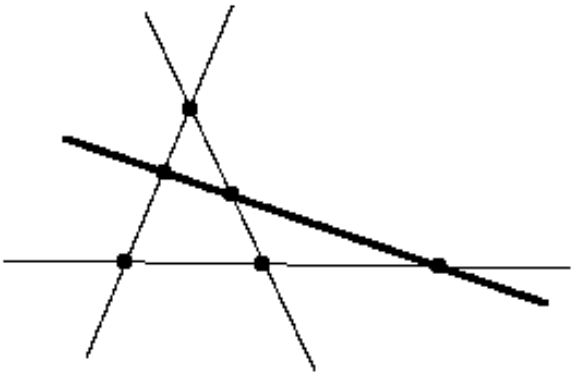


Figure 3.2: Veblen's axiom.

□

A projective plane with $n + 1$ points on each line is said to have **order** n. For example the Fano plane in Figure 3.1 is a projective plane of order 2. A linear space is called a **projective space** if it satisfies the **axiom of Veblen**: If a line meets two sides of a triangle, not at a vertex of the triangle, then it meets the third side. Veblen's axiom is shown in Figure 3.2. The axiom of Veblen can be thought of as saying "any two coplanar lines meet" without having a definition of a plane.

Suppose that two triangles $A_1B_1C_1$ and $A_2B_2C_2$ share no common vertex or side. We say that $A_1B_1C_1$ and $A_2B_2C_2$ are **in perspective from a point** P if the lines A_1A_2, B_1B_2, C_1C_2 have a common point P. This is the situation in Figure 3.3. Note that the line C_2A_2 meets two sides of the triangle PA_1C_1 and so by Veblen's axiom, it meets the third side, C_1A_1. Similarly, A_2B_2 meets A_1B_1 and B_2C_2 meets B_1C_1. We say that two triangles are **in perspective from a line** if the corresponding sides meet and the meeting points are collinear.

Desargues' Theorem is a theorem originating from the real projective plane. It tells us that *if two triangles are in perspective from a point then they are in perspective from a line.* Desargues' Theorem can be seen in Figure 3.4. A projective space is **desarguesian** if Desargues' Theorem holds.

Recall the constructions of Example 3.2. As it happens, these linear spaces satisfy Veblen's Axiom and Desargues' Theorem. Thus they are desarguesian projective spaces. In fact, when Hilbert axiomatised Euclidean geometry in 1899, he proved that these are the *only* desarguesian projective spaces:

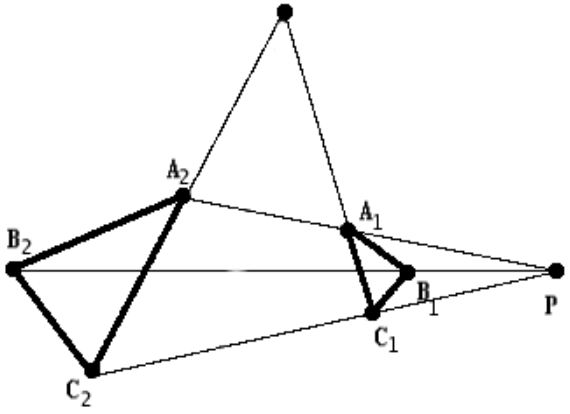


Figure 3.3: Two triangles in perspective from a point *P*.

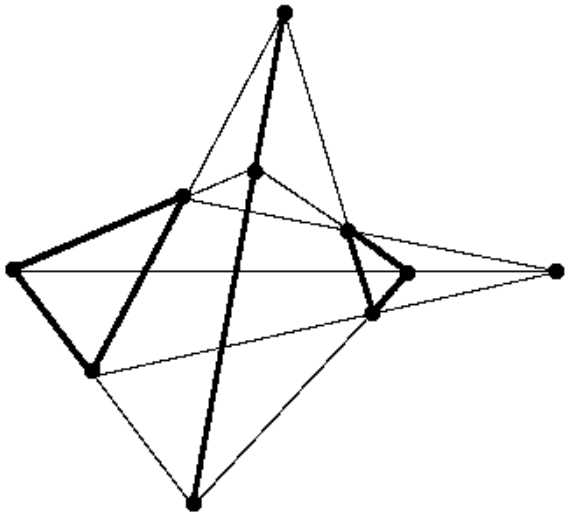


Figure 3.4: Desargues' Theorem

Theorem 3.5. *Every desarguesian projective space is isomorphic to an incidence structure whose points are the one-dimensional subspaces of a vector space V over a field and whose lines are the two-dimensional subspaces of V.*

As a corollary of this, any two desarguesian projective spaces with the same number of points and the same number of points on each line are isomorphic. Veblen and Young proved [34] that every projective space which is *not a single line or a projective plane* satisfies Desargues' theorem. As a result, we have the following theorem:

Theorem 3.6. *Every projective space is either:*

- *a single line with any number of points on it – a "projective line";*
- *a projective plane;*
- *a desarguesian projective space.*

The **projective dimension** of a desarguesian projective space is one less than the dimension of the vector space from which it came. Whenever the construction in Example 3.2 can be applied to a vector space V to form a desarguesian projective space $\mathcal{P}$, the construction can also be applied to the subspaces of V, and the resulting projective spaces will be contained in $\mathcal{P}$. We call them **subspaces** of $\mathcal{P}$. A **hyperplane** $\mathcal{H}$ of $\mathcal{P}$ is a maximal subspace of $\mathcal{P}$, that is, a subspace of $\mathcal{P}$ such that the only subspaces of $\mathcal{P}$ containing $\mathcal{H}$, are $\mathcal{P}$ and $\mathcal{H}$ themselves.

Remark 3.7. The projective space $\mathrm{PG}_d(q)$ has a rather natural embedding in the projective space $\mathrm{PG}_e(q)$ whenever $e > d$. For the vectors of $\mathbf{GF}(q)^{d+1}$ can be padded with zeros to make them vectors of $\mathbf{GF}(q)^{e+1}$, in the following manner:

$$(x_1, x_2, \cdots, x_{d+1})^T \mapsto (x_1, x_2, \cdots, x_{d+1}, 0, \cdots, 0)^T$$

and we will use this embedding later to perform the André/Bruck-Bose construction.

3.3 Affine spaces

An **affine plane** is a linear space satisfying **Playfair's axiom**: If P is a point, and ℓ is a line which does not run through P, then there is a unique line m such that m runs through P and m does not meet ℓ. From this definition, we can see that if ℓ is a line of an affine plane π, then the lines which do not meet ℓ cover all the points of π. This set of lines is called a **parallel class**.

Proposition 3.8. *Let π be an affine plane. For each parallel class of π, add a new point to π which is incident with all lines of the parallel class (these points are called the* ***points at infinity****.) Add one line, the* ***line at infinity****, which is incident with all of the points at infinity. The space thus constructed is a projective plane. Conversely, if π is a projective plane, then removing one line and all the points on it yields an affine plane.*

Now we can consider affine planes and projective planes to be two different ways of looking at the same thing – one is with the line at infinity, the other without. Note that there are many affine planes embedded in a given projective plane. The affine plane *corresponding* to a projective plane π is the affine plane formed by removing a line from π.

Proposition 3.9. *An affine plane has the same number n of points on each line, it has $n+1$ lines through each point, and n^2 points in total.*

The **order** of an affine plane is the number n of points on each line. An affine plane of order n corresponds with a projective plane of order n.

Proposition 3.10. *A projective plane is desarguesian if and only if its corresponding affine plane is desarguesian.*

An **affine space** is a linear space formed by removing a hyperplane from a projective space. Every affine space is either a single line, an affine plane, or a desarguesian affine space as constructed in Example 3.1.

3.4 Automorphism groups

Let $\mathscr{S} = (\mathscr{P}, \mathscr{L}, \mathrm{I})$ be a linear space. A **collineation** of $\mathscr{S}$ is an isomorphism $\mathscr{S} \to \mathscr{S}$. The group of all collineations of a linear space is called the **automorphism group** $\mathrm{Aut}(\mathscr{S})$ (also known as the **collineation group**) of the space.

Theorem 3.11. *If $d \geq 2, q \geq 3$ then*

$$\mathrm{Aut}(\mathrm{AG}_d(q)) = \mathrm{A\Gamma L}_d(q)$$

Note that $\mathrm{AG}_d(2)$ is the complete graph on 2^d vertices, and hence has automorphism group S_{2^d}, the symmetric group on 2^d elements. Now let $\mathrm{P\Gamma L}_d(\mathbb{F}) = \Gamma\mathrm{L}_d(\mathbb{F})/Z(\Gamma\mathrm{L}_d(\mathbb{F}))$ where $Z(\mathrm{GL}_d(\mathbb{F}))$ is the centre of $\Gamma\mathrm{L}_d(\mathbb{F})$, and also write $\mathrm{P\Gamma L}_d(\mathbb{F}) = \mathrm{P\Gamma L}_d(q)$ when $\mathbb{F} = \mathbf{GF}(q)$. Then

Theorem 3.12. *If $d \geq 2$ then*

$$\mathrm{Aut}(\mathrm{PG}_d(q)) = \mathrm{P\Gamma L}_{d+1}(q)$$

For proofs of these theorems, see for example [33, Chapters 2,3].

Let $\mathscr{S}$ be a linear space and let $G \leq \mathrm{Aut}(\mathscr{S})$. We say that G is **point transitive** (or just **transitive**) on $\mathscr{S}$ if, for any points P_1, P_2 there is a $g \in G$ such that $P_1^g = P_2$, and that G is **line transitive** on $\mathscr{S}$ if for any lines ℓ_1, ℓ_2 there is a $g \in G$ such that $\ell_1^g = l_2$. We say that G is **flag-transitive** if for any flags $(P_1, l_1), (P_2, l_2)$ of $\mathscr{S}$ there is a $g \in G$ such that $P_1^g = P_2$ and $\ell_1^g = l_2$.

Flag-transitivity is a very strong type of symmetry. It implies both point transitivity and line transitivity. This thesis is concerned with linear spaces which are flag-transitive. We will now see some examples of such spaces.

3.5 Examples of finite flag-transitive linear spaces

Here is a list of examples of flag-transitive linear spaces. References to some groups will be made; for a description of these groups see [12].

Desarguesian projective spaces These are the projective spaces which can be constructed as $\mathrm{PG}_d(q)$ of a vector space $\mathbf{GF}(q)^d$.

Hermitian and Ree unital spaces Let π be a projective plane of order $n = q^2$ for some prime power q. A **unital** of π is a set of $q^3 + 1$ points that meets every line of π in either 1 or $q + 1$ points.

A linear space $\mathscr{S}$ can be formed from a unital: The points of $\mathscr{S}$ are the points of the unital, and the lines of $\mathscr{S}$ are the lines of π which meet the unital in $q+1$ points. Incidence in $\mathscr{S}$ is the same as incidence in π. This space has $q^3 + 1$ points and $q + 1$ points on each line.

The **Hermitian unital** $U_H(q)$ is a unital which can be constructed from a Hermitian form. Any group G satisfying $\mathrm{PSU}_3(q) \leq G \leq \mathrm{P\Gamma U}_3(q)$ acts flag-transitively on the linear space formed from the Hermitian unital.

If $q = 3^{2e+1}$ for some integer $e \geq 0$, the Ree group ${}^2G_2(q)$ has a 2-transitive action on a set of $q^3 + 1$ points. Any pair of points is fixed by a unique involution (group element of order 2) and this involution fixes precisely $q + 1$ points. We form the **Ree unital space**

U_R: The points of U_R are the $q^3 + 1$ points of the set, and the lines are the $q + 1$ points fixed by the unique involution fixing a pair of points.

This is also a linear space with $q^3 + 1$ points and $q + 1$ points on each line, so we call it a "unital space" even though it does not come from a unital of a projective plane.

Any group G with ${}^2G_2(q) \leq G \leq \mathrm{Aut}({}^2G_2)$ acts flag-transitively on $U_R(q)$.

Witt-Bose-Shrikhande spaces A **hyperoval** in the desarguesian projective plane $\mathrm{PG}_2(q)$ is a set of $q + 2$ points of $\mathrm{PG}_2(q)$ such that no 3 are collinear. Hyperovals exist only for q a power of 2. From a hyperoval of $\mathrm{PG}_2(q)$ we can construct the **Witt-Bose-Shrikhande** spaces $W(q)$ as follows: the *points* of $W(q)$ are the lines of $\mathrm{PG}_2(q)$ which do not meet the hyperoval at any point, the *lines* of $W(q)$ are the points of $\mathrm{PG}_2(q)$ not in the hyperoval, and incidence is symmetrised inclusion, that is, a point and a line of $W(q)$ are incident if the original line and point were incident.

The Witt-Bose-Shrikhande spaces are flag-transitive linear spaces with $\frac{1}{2}(q^2 - q)$ points and $q/2$ points on every line.

Desarguesian Affine Spaces A desarguesian projective space minus a hyperplane. These are the linear spaces constructed in Example 3.1.

Hering Spaces In [16] the **Hering spreads** are constructed. There is a subgroup G of $\mathrm{GL}_6(3)$ which is isomorphic to $\mathrm{SL}_2(13)$ and is transitive on the non-zero vectors of $\mathbf{GF}(3)^6$. Examining the action of this subgroup on the lines of $\mathrm{PG}_5(3)$ we discover that two of its orbits are partitions of $\mathrm{PG}_5(3)$ into lines. Similarly, examining the action of the subgroup on the planes of $\mathbf{GF}(3)^6$, we can find an orbit which is a partition of $\mathrm{PG}_5(3)$ into planes.

With any of these partitions, we can construct a linear space $\mathscr{S}$. Embed $\mathrm{PG}_5(3)$ in $\mathrm{PG}_6(3)$. The points of $\mathscr{S}$ are the points of $\mathrm{PG}_6(3)$ which do not lie in our embedding of $\mathrm{PG}_5(3)$. The lines of $\mathscr{S}$ are the subspaces in $\mathrm{PG}_6(3)$ which intersect $\mathrm{PG}_5(3)$ in exactly one member of the spread. All of these linear spaces have 3^6 points and 3^3 points on each line, and they are called the **Hering spaces**.

3.6 The classification of finite flag-transitive linear spaces

The starting point for the classification of finite flag-transitive linear spaces was made in 1961 by Higman and McLaughlin [17].

Theorem 3.13 (Higman-McLaughlin). *Suppose that G acts flag-transitively on a linear space $\mathscr{S}$. Then G acts primitively on the points of $\mathscr{S}$.*

Using this and the O'Nan-Scott theorem on the structure of finite primitive groups, Buekenhout, Delandtsheer and Doyen [7] proved that, for a group G acting acting flag-transitively on a linear space, either:

- G is almost simple or
- $\mathscr{S}$ has p^d points and $G \leq \mathrm{AGL}_d(p)$, where p is a prime and d is a positive integer.

In 1990, Buekenhout, Delandtsheer, Doyen, Kleidman, Liebeck and Saxl announced the classification of flag-transitive linear spaces.

Theorem 3.14. *Suppose that G is a flag-transitive group of automorphisms of a nontrivial finite linear space $\mathscr{S}$. Then either*

- *$\mathscr{S}$ is one of the examples in Section 3.5, or*
- *The points of $\mathscr{S}$ are the elements of a field $\mathbf{GF}(q)$ and $T \leq G \leq A\Gamma\mathrm{L}_1(q)$, where q is a prime power, and T is the group of all translations of $\mathbf{GF}(q)$, that is, the maps*

$$x \mapsto x + c$$

for $c \in \mathbf{GF}(q)$.

The second item here serves as our motivation for the remainder of this thesis. This is the "too-hard basket" of the classification. They are referred to as **one dimensional affine linear spaces**. Kantor [21] says that it is unlikely that there will ever be a complete classification of these spaces, because the methods of constructing them admit too many subtle variations.

Suppose that $\mathscr{S}$ is a linear space of this type, i.e., the points of $\mathscr{S}$ are elements of a field $\mathbf{GF}(q)$, and some subgroup of $A\Gamma\mathrm{L}_1(q)$ acts transitively on $\mathscr{S}$. The lines through 0 partition the points of $\mathbf{GF}(q)\backslash 0$. Furthermore, since $\mathscr{S}$ is flag-transitive, each of these lines has the same number of points. When these lines are closed under addition, they are *subspaces* of dimension $t+1$ of $\mathbf{GF}(q)$ as a vector space over a smaller field, and we call the partition a *t*-**spread**. We will search for linear spaces of this type, and create a new infinite class of them.

Chapter 4

t-spreads and Translations

Our objective now is to construct some new flag-transitive linear spaces of the one-dimensional affine kind. We will do this by using a geometrical object called a *t-spread*. A t-spread is a partition of the projective space $\mathrm{PG}_d(q)$ into subspaces $\mathrm{PG}_t(q)$. The André/Bruck-Bose construction turns any t-spread of $\mathrm{PG}_d(q)$ into a linear space with q^{d+1} points and q^{t+1} points on each line, and if the t-spread is *transitive* (the concept of a transitive t-spread will be introduced later) then the resulting linear space will be flag-transitive!

But first, a digression, which we will use to introduce spreads.

4.1 Rao's solution of the Kirkman schoolgirl problem

Is there a way for fifteen girls to walk to school in five rows of three every day for a week, so that no two girls walk in the same row twice?

This question is known as the Kirkman schoolgirl problem. There are several solutions to it, and here is a particularly elegant one, given by Rao [28]. A primitive element of **GF**(8) is β whose minimal polynomial over **GF**(2) is $x^3 + x^2 + 1$. Since $\beta^3 = -\beta^2 - 1$, we can write each power of β as a linear combination of β^2, β and 1:

$\beta^0 = 1$	$(0,0,1)$		
$\beta^1 = \beta$	$(0,1,0)$	$\beta^4 = \beta^2 + \beta + 1$	$(1,1,1)$
$\beta^2 = \beta^2$	$(1,0,0)$	$\beta^5 = \beta + 1$	$(0,1,1)$
$\beta^3 = \beta^2 + 1$	$(1,0,1)$	$\beta^6 = \beta^2 + \beta$	$(1,1,0)$

The three dimensional vector to the right of each value is formed from the coefficients of the terms β^2, β and 1.

Similarly, a primitive element of **GF**(16) is γ whose minimal polynomial over **GF**(2) is $x^4 + x^3 + 1$. We can write the powers of γ as a linear combination of $\gamma^3, \gamma^2, \gamma$ and 1.

$\gamma^0 = 1$	$(0,0,0,1)$		
$\gamma^1 = \gamma^1$	$(0,0,1,0)$	$\gamma^8 = \gamma^3 + \gamma^2 + \gamma$	$(1,1,1,0)$
$\gamma^2 = \gamma^2$	$(0,1,0,0)$	$\gamma^9 = \gamma^2 + 1$	$(0,1,0,1)$
$\gamma^3 = \gamma^3$	$(1,0,0,0)$	$\gamma^{10} = \gamma^3 + \gamma$	$(1,0,1,0)$
$\gamma^4 = \gamma^3 + 1$	$(1,0,0,1)$	$\gamma^{11} = \gamma^3 + \gamma^2 + 1$	$(1,1,0,1)$
$\gamma^5 = \gamma^3 + \gamma + 1$	$(1,0,1,1)$	$\gamma^{12} = \gamma + 1$	$(0,0,1,1)$
$\gamma^6 = \gamma^3 + \gamma^2 + \gamma + 1$	$(1,1,1,1)$	$\gamma^{13} = \gamma^2 + \gamma$	$(0,1,1,0)$
$\gamma^7 = \gamma^2 + \gamma + 1$	$(0,1,1,1)$	$\gamma^{14} = \gamma^3 + \gamma^2$	$(1,1,0,0)$

The set $\{0, \gamma^0, \gamma^5, \gamma^{10}\}$, which can be written as the vectors $\{\mathbf{0}, (0,0,0,1), (1,0,1,1), (1,0,1,0)\}$ form a subspace of $\mathbf{GF}(2)^4$. Multiplication by γ is a linear transformation, so the orbit of this set is 5 subspaces of $\mathbf{GF}(2)^4$, and these subspaces intersect only in the zero element, and cover all the points. Such a cover we call a **spread**. Given an element of $\mathbf{GF}(2)^4$, the last three components can be treated as an element of **GF**(8), and multiplying by β (while leaving the first component the same) gives a linear transformation of order 7. In disjoint cyclic notation, this transformation is:

$$(\gamma^0\ \gamma^1\ \gamma^2\ \gamma^9\ \gamma^7\ \gamma^{12}\ \gamma^{13})(\gamma^4\ \gamma^{10}\ \gamma^{14}\ \gamma^{11}\ \gamma^6\ \gamma^5\ \gamma^8)$$

The orbit of our spread under the group generated by this transformation is a set of 7 spreads covering all 35 lines of $PG_3(2)$. If we associate each of our 15 girls with one of the 15 points of $PG_3(2)$, associate each row with a line, and each day with a spread, then we have a solution to the Kirkman schoolgirl problem.

4.2 Spreads and affine planes

If $\mathcal{P}$ is a projective space of odd projective dimension d, then a **spread** of $\mathcal{P}$ is a partition of $\mathcal{P}$ into subspaces of projective dimension $\frac{1}{2}(d-1)$.

We can also give the definition of a spread in terms of the original vector space. If V is a vector space of even dimension d, then a spread of V is a set S of subspaces of dimension $\frac{1}{2}d$ such that

- for any $x \in V$ there is a $U \in S$ such that $x \in U$,
- if $U, V \in S$ and $U \neq V$ then $U \cap V = \{0\}$.

Spreads are greatly studied because they can be used to construct non-desarguesian affine planes. There are two ways to do this construction.

Construction 1 Let $\mathrm{PG}_d(q)$ be embedded in $\mathrm{PG}_{d+1}(q)$, as in remark 3.7. Let S be a spread of $\mathrm{PG}_d(q)$. Form a new point-line incidence structure $\mathscr{S}_1$ as follows: The points of $\mathscr{S}_1$ are the points of $\mathrm{PG}_{d+1}(q)$ that are not in $\mathrm{PG}_d(q)$. The lines of $\mathscr{S}_1$ are the $\frac{1}{2}(d+1)$ dimensional subspaces of $\mathrm{PG}_{d+1}(q)$ which meet $\mathrm{PG}_d(q)$ in an element of S. Incidence is containment.

Construction 2 Let S be a spread of the vector space V (of dimension $d+1$.) Form a new point-line incidence structure $\mathscr{S}_2$ as follows: The points of $\mathscr{S}_2$ are the points of V. The lines of $\mathscr{S}_2$ are all translates of all elements of S. Incidence is containment.

Proposition 4.1. *Constructions 1 and 2, applied to the same spread, yield isomorphic point-line incidence structures.*

Proof. Recall that the points of the projective space $\mathrm{PG}_{d+1}(q)$ are the one-dimensional subspaces of the vector space $\mathbf{GF}(q)^{d+2}$. The points of the projective space $\mathrm{PG}_d(q)$ embedded in $\mathrm{PG}_{d+1}(q)$ are those one-dimensional subspaces of $\mathbf{GF}(q)^{d+2}$ whose vectors have a zero in the last co-ordinate. Thus the points of $\mathrm{PG}_{d+1}(q) \backslash \mathrm{PG}_d(q)$ each have a representative of the form

$$(x_1, x_2, \cdots, x_{d+1}, 1)^T$$

and we will define our isomorphism ϕ by

$$\phi : \mathrm{PG}_{d+1}(q) \backslash \mathrm{PG}_d(q) \to \mathbf{GF}(q)^d$$
$$\mathrm{span}(x_1, x_2, \cdots, x_{d+1}, 1)^T \mapsto (x_1, x_2, \cdots, x_{d+1})$$

that is, it drops the 1 off the representative vector. This map is certainly a bijection from $\mathrm{PG}_{d+1}(q) \backslash \mathrm{PG}_d(q)$ to $\mathbf{GF}(q)^{d+1}$. Thus it remains to show that ϕ maps lines to lines. Let ℓ be a line of the linear space $\mathscr{S}_1$ formed in Construction 1. Then ℓ is the join $P + U$ of some point P

in $\mathrm{PG}_{d+1}(q)\backslash\mathrm{PG}_d(q)$ with an element U of the spread. So if Q is a point of ℓ then the representative vector of Q will be the sum of the representative vector of P with some element of U. So $\phi(\ell) = U + \phi(P)$, thus it is a translate of an element of the spread. □

The above construction, in either form, is known as the **André/Bruck-Bose construction**, as it originated (seemingly independently) in [1] and [5]. Its motivation was the construction of translation planes. A **translation plane** is an affine plane whose translations (see Section 4.3) form a group acting regularly on the points.

Proposition 4.2. *The André/Bruck-Bose construction yields a translation plane.*

Theorem 4.3 (The fundamental theorem of translation planes). *All translation planes can be made from a spread via the André/Bruck-Bose construction.*

For a proof of these, see [4]. A *t-spread* is a set of t-dimensional subspaces partitioning $\mathrm{PG}_d(q)$, or equivalently, a set of $(t+1)$-dimensional subspaces partitioning $\mathbf{GF}(q)^{d+1}$. The André/Bruck-Bose construction generalises to t-spreads, although it does not generally construct a translation plane, but a more general type of transitive linear space. These are the linear spaces we will be concerned with.

Proposition 4.4. *A necessary condition for the existence of a t-spread of* $\mathrm{PG}_d(q)$ *is that*

$$(t+1) \mid (d+1).$$

Proof. The number of elements of $\mathrm{PG}_d(q)$ is $(q^{d+1}-1)/(q-1)$. The number of elements of a t-dimensional subspace of $\mathrm{PG}_d(q)$ is $(q^{t+1}-1)/(q-1)$. If a t-spread of $\mathrm{PG}_d(q)$ exists, then

$$(q^{t+1}-1)/(q-1) \mid (q^{d+1}-1)/(q-1)$$

and so

$$(q^{t+1}-1) \mid (q^{d+1}-1).$$

But doing the long division shows that this can only be true if $(t+1) \mid (d+1)$. □

From now on we will generally work with Construction 2. Although Construction 1 is more aesthetically pleasing – spreads of a projective space are actual partitions, rather than partitions of nonzero elements – Construction 1 is computationally easier to work with.

4.3 Dilatations and translations

A **dilatation** of a linear space $\mathscr{S}$ is a collineation g of $\mathscr{S}$ such that for any point P and any line ℓ,

$$P \mathrel{\mathrm{I}} \ell \mathrel{\mathrm{I}} P^g \implies \ell^g = \ell.$$

If g is a dilatation and if P is a fixed point of g, then g leaves every line through P invariant.

Proposition 4.5. *Let $\mathscr{S}$ be a linear space. Any non-identity dilatation of $\mathscr{S}$ fixes at most one point.*

Proof. Suppose that g is a dilatation which fixes two points P and Q. Let R be some other point. g leaves the lines PR and QR invariant. If these are two different lines, then R^g lies on their unique intersection, which is R. If PR and QR are the same line, then let S be some point not on this line. Now S is fixed by the above argument, and PR and SR are two different lines, so by the above argument R is fixed. □

A **translation** is either the identity or a dilatation which fixes no point.

Lemma 4.6. *Let $\mathscr{S}_1$ and $\mathscr{S}_2$ be linear spaces, and let ϕ be an isomorphism from $\mathscr{S}_1$ to $\mathscr{S}_2$. If t is a translation of $\mathscr{S}_2$, then $\phi t \phi^{-1}$ is a translation of $\mathscr{S}_1$.*

Proof. Let P be a point in $\mathscr{S}_1$ and let ℓ be a line in $\mathscr{S}_1$ which passes through P and $P^{\phi t \phi^{-1}}$. Then ℓ^ϕ passes through P^ϕ and $P^{\phi t}$. Since t is a translation, we see that t leaves ℓ^ϕ invariant. But then

$$\ell^{\phi t \phi^{-1}} = ((\ell^\phi)^t)^{\phi^{-1}} = \ell$$

thus $\phi t \phi^{-1}$ leaves ℓ invariant, and $\phi t \phi^{-1}$ is a dilatation. Also, if $\phi t \phi^{-1}$ fixes a point P, then $t = \phi^{-1}(\phi t \phi^{-1})\phi$ fixes P^ϕ, a contradiction. Therefore $\phi t \phi^{-1}$ fixes no point and so it is a translation. □

By letting $\mathscr{S}_1 = \mathscr{S}_2$ in the above lemma, we see:

Corollary 4.7. *Let $\mathscr{S}$ be a linear space. The translations of a linear space form a **normal set** in* Aut($\mathscr{S}$)*, that is, the set of translations is invariant under conjugation.*

The dilatations of a linear space are not guaranteed to form a group. For example, as proved in [32], the dilatations of the unitals of Section 3.5 do not form a group. If they *do* form a group, then by Proposition 4.5 it is a Frobenius group, and so by Theorem 2.8 the translations also form a group. This group is semiregular by definition. We can construct linear spaces with transitive translation group in the following way:

Proposition 4.8. *Let G be a group, and let P be a nontrivial equal partition of G. Form an incidence structure whose* points *are the elements of G, and the* lines *are the right cosets of elements of P. This incidence structure is a regular linear space.*

Proof. Since P is nontrivial, there are at least two lines. Since every element of P is nontrivial, every line has at least two points. It remains to show that there is a unique line between any two given points. Let g, h be points of our linear space (that is, elements of G.) There is a unique element A of P containing gh^{-1}, and Ah is a coset of A that contains both g and h. This shows that there is a line through g and h. Suppose that ℓ and m are lines through g and h. Then ℓ can be written as Ah for some $A \in P$, and m can be written as Bh for some $B \in P$. But if $Ah \neq Bh$ then $A \neq B$, but both A and B contain gh^{-1}. Thus $A \cap B$ is nontrivial and so P is not a partition, a contradiction. Thus there is a unique line through any two given points. □

Example 4.9. Recall our equal partition of a group G of order 27 from Example 2.9. Applying the above construction to this partition of G gives a regular linear space with 27 points and 3 points on each line.

Schulz [32] showed that the constructions of Proposition 4.8 have as transitive translation group the group G from which they were constructed. In fact, these are the *only* regular linear spaces with transitive translation groups. These results are relayed in English in [11, ¶2.3.25, 2.4.29].

In the case when G is an **elementary abelian** p-group, that is, an abelian p-group of exponent p, we can think of it as the additive group of a finite dimensional vector space over a finite field. In this case, the above construction becomes the André/Bruck-Bose construction.

Theorem 4.10. *Let $V = \mathbf{GF}(p)^d$ be a vector space, let S_1 and S_2 be t-spreads of V, and let $\mathscr{S}_1$ and $\mathscr{S}_2$ be the linear spaces arising from S_1 and S_2 respectively via the André/Bruck-Bose construction. If $\phi : V \to V$ is an isomorphism from $\mathscr{S}_1$ to $\mathscr{S}_2$, and $\phi(0) = 0$, then ϕ is additive, that is, for any $x, y \in V$,*

$$\phi(x + y) = \phi(x) + \phi(y).$$

Proof. By Schulz' Theorem, the translations of $\mathscr{S}_1$ and $\mathscr{S}_2$ are the maps

$$x \mapsto x + c$$

for $c \in V$. By Lemma 4.6, ϕ normalises the set of translations. Hence for any $c \in V$, there is a $d \in V$ such that

$$\phi(x + c) = \phi(x) + d$$

for any $x \in V$. Substituting $x = 0$ shows us that $\phi(c) = d$, and so

$$\phi(x + c) = \phi(x) + \phi(c).$$

Since this is true for any $c \in V$, we see that ϕ is additive. □

A t-spread S of $\mathbf{GF}(q)^d$ is **transitive** if the stabiliser of S in $\Gamma\mathrm{L}_d(q)$ is transitive on the elements of S.

Theorem 4.11. *Let p be a prime. Let $V = \mathbf{GF}(p)^d$ be a vector space, and let S be a t-spread of V. If S is a transitive t-spread, then the linear space $\mathscr{S}$ formed from S by the André/Bruck-Bose construction is flag-transitive, and*

$$\mathrm{Aut}(\mathscr{S}) = T.\mathrm{Stab}_{\mathrm{GL}_d(p)}(S).$$

where T is the set of maps $t : x \mapsto x + c$ for $c \in V$.

Proof. By the Higman-McLaughlin Theorem (Theorem 3.13,) $\mathrm{Aut}(\mathscr{S})$ is primitive. By Corollary 4.7, the group T is a normal subgroup of $\mathrm{Aut}(\mathscr{S})$, and so it is transitive by Lemma 2.7. So by Lemma 2.6 we can write

$$\mathrm{Aut}(\mathscr{S}) = T.\mathrm{Stab}_{\mathrm{Aut}(\mathscr{S})}(0).$$

Now it suffices to show that $\mathrm{Stab}_{\mathrm{Aut}(\mathscr{S})}(0) = \mathrm{Stab}_{\mathrm{GL}_d(p)}(S)$ and that this group is transitive on the lines through 0.

Suppose $f \in \mathrm{Stab}_{\mathrm{GL}_d(p)}(S)$. Let ℓ be a line in $\mathscr{S}$. Then ℓ can be written as $A + h$ where A is a subspace of V. But then since f is additive,

$$f(A + h) = f(A) + f(h)$$

and since f stabilises the spread, $f(A)$ is an element of the spread, and so $f(A) + f(h)$ is a line of $\mathscr{S}$. Hence $\mathrm{Stab}_{\mathrm{GL}_d(p)}(S) \leq \mathrm{Stab}_{\mathrm{Aut}(\mathscr{S})}(0)$. Furthermore, $\mathrm{Stab}_{\mathrm{GL}_d(p)}(S)$ is transitive on S, and so it is transitive on lines through the origin.

Now the stabiliser of the point $0 \in V$ in the group $\mathrm{Aut}(\mathscr{S})$ must normalise T by Lemma 4.7. Hence if $f \in \mathrm{Stab}_{\mathrm{Aut}(\mathscr{S})}(0)$, by Theorem 4.10, f is additive, so $f \in \mathrm{GL}_d(p)$. Furthermore, since f must map lines through the origin to lines through the origin, f stabilises the t-spread S. Thus $\mathrm{Stab}_{\mathrm{Aut}(\mathscr{S})}(0) = \mathrm{Stab}_{\mathrm{GL}_d(p)}(S)$. □

Chapter 5

Constructions of transitive line spreads

The André/Bruck-Bose construction applied to a t-spread of $\mathrm{PG}_d(q)$ is a rather general construction for linear spaces. The case when $t = d$ is uninteresting: it gives a degenerate linear space. The next largest possible case is $t = \frac{1}{2}(d-1)$; this is the case of a *spread* and it has been widely studied. We will now jump to the other extreme – when t is as small as possible. If $t = 0$ then the case also becomes uninteresting: the only 0-spread of $\mathrm{PG}_d(q)$ is the partition of $\mathrm{PG}_d(q)$ into its constituent points, and applying the André/Bruck-Bose construction yields a desarguesian affine space. The next smallest case is $t = 1$: here d must be odd, and our 1-spread is a partition of $\mathrm{PG}_d(q)$ into lines. We call this a **line spread**.

In this chapter we will examine the constructions that Kantor gave in [21], and construct some transitive line spreads of our own. By Theorem 3.14, if $\mathscr{S}$ is a finite flag-transitive linear space coming from a t-spread S, then either

- $\mathscr{S}$ is a desarguesian affine space,
- S is one of the Hering t-spreads, or
- the points of the linear space $\mathscr{S}$ form a field $\mathbf{GF}(p^d)$ where p is a prime, and $\mathrm{Aut}(\mathscr{S}) \leq \mathrm{A\Gamma L}_1(p^d)$.

It is the last case which concerns us, and we will call such spreads **soluble**[1]. In the latter case, by Theorem 4.11, the stabiliser of S in $\mathrm{GL}_d(p)$ is transitive on S, and it is a subgroup of $\mathrm{Stab}_{\mathrm{A\Gamma L}_1(p^d)}(0) = \Gamma\mathrm{L}_1(p^d)$. From now on, we will think of a line spread as a set of two-dimensional subspaces of a *field* as a vector space over a smaller field. In particular, let $\mathbb{K} =$

[1] This is because the group of automorphisms is *soluble*.

$\mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$. Then one element of our line spread will be the image of $\mathbb{L}$ under some $\mathbb{K}$-linear map $h : \mathbb{L} \to \mathbb{F}$, and the line spread itself will be the orbit of this subspace under some group $G \leq \Gamma\mathrm{L}_1(q^{2m})$. We will make frequent use of the "bar" or "involutory" automorphism of $\mathbb{L}$ which is the unique automorphism of $\mathbb{L}$ of order 2, which we write

$$x \mapsto \overline{x}.$$

We will call a t-spread **desarguesian** if the linear space formed by applying the André/Bruck-Bose construction is a desarguesian affine space.

5.1 The constructions of Kantor

We shall now see the constructions of t-spreads in [21]. We shall restrict these constructions to the case when $t = 1$. For the more general constructions, as well as proofs that they actually construct t-spreads, see [21]. Kantor lists 7 types of constructions of flag-transitive linear spaces – type 1 is the "generalised Netto system" which is a construction that does not use t-spreads. Type 2 is a special case of Type 7, which we refer to here as the *inflation trick*.

In all of these constructions, $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$, and line spreads will be constructed of $\mathbb{F}$ as a vector space over $\mathbb{K}$. Thus the linear spaces formed by the André/Bruck-Bose construction will have q^{2m} points and q^2 points on each line. In each of the constructions, s is any element of $\mathbb{F}$ whose multiplicative order is $(q^{2m} - 1)(q - 1)/(q^2 - 1)$. (Hence $s^{(q^{2m}-1)/(q^2-1)}$ is an element of $\mathbb{K}$, so it preserves the t-spread.)

5.1.1 Type 3

This type of construction requires powers $f > 1$ and $q > 1$ of a prime p such that firstly, $p \nmid (t + 1)$ and secondly, $((q^{(t+1)} - 1)/(q - 1), f - 1) = 1$. When $t = 1$ the first condition implies that q and f are odd, and the second condition implies that $(q + 1, f - 1) = 1$. But if q and f are odd then $(q + 1, f - 1) \geq 2$. So there are no line spreads of this type.

5.1.2 Type 4

Let $\mathbb{F} = \mathbf{GF}(q^{2m}), \mathbb{L} = \mathbf{GF}(q^2), \mathbb{K} = \mathbf{GF}(q)$ with m an odd number dividing $q - 1$. Let $k \in \mathbb{K}^*$ be an element of order m. If b is an element of $\mathbb{F}$ such that $b^{q^2} = kb$, then letting $h(x) = x - b\overline{x}$

and $U = h(L)$, the orbit of U under the subgroup of $\mathbb{F}^*$ generated by s is a line spread of $\mathbb{F}$ as a vector space over $\mathbb{K}$.

5.1.3 Type 5

Let $\mathbb{F} = \mathbf{GF}(q^{2m}), \mathbb{L} = \mathbf{GF}(q^2), \mathbb{K} = \mathbf{GF}(q)$ with m dividing $q-1$. If m is even, assume $q \equiv 1 \bmod 2m$. Let $k \in \mathbb{K}^*$ be an element of order m. If b is an element of $\mathbb{F}$ such that $b^{q^2} = kb$, then letting $h(x) = x - b\,\overline{x}$ and $U = h(L)$, and letting σ be an automorphism of $\mathbb{F}$ fixing the elements $\mathbb{K}$ but acting nontrivially on $\mathbb{L}$, the orbit of U under the subgroup of $\Gamma\mathrm{L}$ generated by the maps $z \to s^m z$ and $z \to bz^\sigma$ is a line spread of $\mathbb{F}$ as a vector space over $\mathbb{K}$.

5.1.4 Type 6

Let $\mathbb{F} = \mathbf{GF}(q^{2m}), \mathbb{L} = \mathbf{GF}(q^2), \mathbb{K} = \mathbf{GF}(q)$ with m dividing $q-1$. Let $k \in \mathbb{K}^*$ be an element of order m. If b is an element of $\mathbb{F}$ such that $b^{q^2} = kb$, then letting $h(x) = x - b\,\overline{x}$ and $U = h(L)$, and letting $\mu \in \mathbb{F}^*$ such that $N_{\mathbb{F}/\mathbb{L}}(\mu) \in \mathbb{K}$ but $N_{\mathbb{F}/\mathbb{L}}(\mu)^j$ is not an mth power in L whenever $1 \le j < m$, the orbit of U under the subgroup of $\Gamma\mathrm{L}$ generated by the maps $z \to s^m z$ and $z \to \mu z^{q^2}$ is a line spread of $\mathbb{F}$ as a vector space over $\mathbb{K}$.

5.1.5 Inflation

Given a line spread of a projective space, we can sometimes turn it into a line spread of a larger projective space. The following method is referred to as Kantor's "inflation trick" in [8] or his "free lunch trick" in [21].

Suppose $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{F}_0 = \mathbf{GF}(q^{2m}) \subset \mathbb{F} = \mathbf{GF}(q^{2md})$. Suppose that S_0 is a line spread of $\mathbb{F}_0$, and that

$$(d, q+1) = 1. \tag{5.1.1}$$

Let G be a subgroup of $\Gamma\mathrm{L}_1(q^{2md})$ such that

- G acts transitively on the "cosets" $\{c\mathbb{F}_0 : c \in \mathbb{F}^*\}$ of $\mathbb{F}_0$ in $\mathbb{F}$;
- $\mathrm{Stab}_G(\mathbb{F}_0)$ acts transitively on the line spread S_0.

Then the union of the images of S_0 under elements of G forms a line spread of $\mathbb{F}$ as a vector space over $\mathbb{K}$, and G acts transitively on this line spread.

5.2 Searching for transitive line spreads

Our purpose here is to develop a technique for searching for transitive line spreads of a field $\mathbb{F} = \mathbf{GF}(q^{2m})$ as a vector space over a field $\mathbb{K} = \mathbf{GF}(q)$ computationally. A straightforward solution is this: enumerate the subgroups of $\Gamma\mathrm{L}_1(q^{2m})$, and search for orbits of these subgroups which partition the points of $\mathbb{F}$. Having done this, we will have a list of all transitive line spreads. Great! But then we hit a snag: how do we know whether we have *essentially different* line spreads in the sense that they will give us nonisomorphic linear spaces? Suppose that there exists an isomorphism ϕ between two linear spaces $\mathscr{S}_1$ and $\mathscr{S}_2$ arising from t-spreads S_1 and S_2. Since $\mathscr{S}_1$ and $\mathscr{S}_2$ are transitive, we can assume without loss of generality that $\phi(0) = 0$. Then by Theorem 4.10, the function ϕ is additive, and so $\phi \in \mathrm{GL}_{2md}(p)$, where $q = p^d$ for a prime p. Furthermore, since $\phi(0) = 0$, it must be that ϕ maps any line through 0 to a line through 0. Hence ϕ maps S_1 to S_2. So the problem of testing whether two t-spreads of $\mathbf{GF}(q)^{2m}$ give isomorphic linear spaces has been reduced to the problem of testing whether there is a map in $\mathrm{GL}_{2md}(p)$ from one to the other. We will call two t-spreads **equivalent** if such a map exists.

Unfortunately, the general linear group is (generally) huge. Searching it for equivalences is infeasible. In order to make this problem computationally feasible, we will make use of the *Samosa Lemma*, which gives us a much smaller group to search.

Let $a \geq 2, d \geq 2$. A **primitive prime divisor** (or **ppd**) of $a^d - 1$ is a prime number which divides $a^d - 1$ but does not divide $a^k - 1$ for $k < d$. For a discussion of ppds, see Appendix A. In particular, it is proved that:

Theorem 5.1 (Zsigmondy). *Suppose $a \geq 2, n \geq 2$ are integers. There is a primitive prime divisor of $a^n - 1$ except in the following cases:*

- *$a = 2^s - 1$ for some integer $s \geq 2$, and $n = 2$*
- *$a = 2$ and $n = 6$*

As a by-product of the proof, we get Wedderburn's Theorem.

Theorem 5.2 (Wedderburn). *If E is a finite division ring then E is a field.*

Lemma 5.3. *Let p be a primitive prime divisor of $q_0^d - 1$ where q_0 is a prime. Let p^i be the largest power of p dividing $q_0^d - 1$. Then there is a unique subgroup of $\Gamma\mathrm{L}_1(q_0^d)$ with order p^i.*

Proof. Suppose that P is a Sylow p subgroup of $\Gamma\mathrm{L}_1(q_0^d)$ and that $g : z \mapsto \alpha z^\phi$ is an element of P. Then $g^{p^d} = 1$ and so $\phi^{p^d} = 1$. But by Remark A.10, our primitive prime divisor p is coprime

to d, and ϕ is in a cyclic group of order d, so $\phi = 1$. Hence P is a Sylow subgroup of the group of linear maps $\mathbb{F} \to \mathbb{F}$. But this group is (isomorphic to) $\mathbb{F}^*$ and so it is abelian. By Sylow's Theorem, all Sylow subgroups of a group are conjugate, and so P is unique. □

In the following lemma, $N_G(H)$ is the normaliser of H in G, that is, the group of elements $g \in G$ such that $H^g = H$ under the action by conjugation. This lemma is a part of the "Samosa Lemma" appearing in [27], which gives the structure of centralisers and normalisers of Sylow ppd-subgroups of the general linear group. Tim Penttila was asked where the name came from. He explained that he and David Evans once tried to prove it after seeing it in [19]. After being stuck on the problem for hours, they went out for dinner at Uddins, the nearby Indian restaurant they favoured. They finally came up with a proof over the first course – samosas! As they later needed to refer to it, they called it the Samosa Lemma. Penttila began calling it by that name when he taught it, and Ivano Pinneri used the name in [27]. Penttila's research associate Matt Brown, having read the name "Samosa Lemma" in [27], spent a fruitless day trying to look it up by that name in the library! Penttila says, "It's a tasty lemma, and samosas are tasty."

Lemma 5.4 (The Meat of the Samosa Lemma). *Let q be a prime. Let $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{F} = \mathbf{GF}(q^d)$. Suppose that p is a primitive prime divisor of $q^d - 1$, and let G be the Sylow p subgroup of $\mathbb{F}^*$. Then, treating $\mathbb{F}$ as the vector space $\mathbf{GF}(q)^d$, we have*

$$N_{\mathrm{GL}_d(q)}(G) = \Gamma\mathrm{L}_1(q^d).$$

Proof. We will first show that G is irreducible. Suppose that G fixes a nonzero proper subspace U of $\mathbb{F}$ (as a vector space over $\mathbb{K}$.) Now $\mathbb{F}^*$ acts regularly on $\mathbb{F}\backslash\{0\}$ by multiplication, so G acts semiregularly on $\mathbb{F}\backslash\{0\}$. Hence the orbits of G on $\mathbb{F}\backslash\{0\}$ have size divisible by p. Thus $p \mid |U\backslash\{0\}| = q^k - 1$ with $k < d$. But p is a primitive prime divisor of $q^d - 1$ so it cannot divide $q^k - 1$. Thus G is irreducible.

Since G is irreducible, by Lemma 2.10 the set $\mathrm{End}_G(\mathbb{F})$ of $\mathbb{K}$-linear endomorphisms of $\mathbb{F}$ is a division ring, and by Theorem 5.2 it is a field. In fact, the set of maps

$$\hat{\mathbb{F}} = \{x \mapsto \alpha x : \alpha \in \mathbb{F}\} \tag{5.2.1}$$

is a subfield of $\mathrm{End}_G(\mathbb{F})$ because multiplication by $z \in \mathbb{F}$ is an operation which commutes with g for any $g \in G$.

$\mathrm{End}_G(\mathbb{F})^*$ is the set of *invertible* $\mathbb{K}$-linear transformations of $\mathbb{F}$ which commute with all elements of G. Hence it is the centralizer of G in $\mathrm{GL}_d(q)$. We will now see that $\mathrm{End}_G(\mathbb{F})^*$ is just the set $\hat{\mathbb{F}}^*$. Since it is the multiplicative group of a field, it is abelian, and by Equation 5.2.1 it is transitive on $\mathbb{F}^*$. So by Lemma 2.4, we have $\mathrm{End}_G(\mathbb{F})^*$ is regular on $\mathbb{F}^*$ and so its size is $|\mathbb{F}^*|$. But we already know that $\hat{\mathbb{F}}^* \subseteq \mathrm{End}_G(\mathbb{F})^*$, so $\hat{\mathbb{F}}^* = \mathrm{End}_G(\mathbb{F})^*$. Now we know that the centraliser of G in $\mathrm{GL}_d(q)$ is $\hat{\mathbb{F}}^*$. The normaliser of G must also be the normaliser of $\hat{\mathbb{F}}^*$ (because G is abelian.) By Lemma 2.14 this is $\Gamma\mathrm{L}_1(q^d)$. □

Theorem 5.5. *Let $K = \mathbf{GF}(q) \subset F = \mathbf{GF}(q^d)$ where $q^d \neq 64$ and $d > 2$. Let S and T be t-spreads of $\mathbb{F}$ (as a vector space over K) with $t \geq 1$, such that there are subgroups $G, H \in \Gamma\mathrm{L}_1(q)$ acting transitively on S and T respectively. Then S and T are equivalent if and only if there is a map $f \in \Gamma\mathrm{L}_1(q)$ which maps S to T.*

Proof. Both S and T have size $(q^d-1)/(q^{t+1}-1)$. Hence $(q^d-1)/(q^{t+1}-1) \,\big|\, |G|$. Now $q^d \neq 64$, nor is it the square of a prime, for then d would be 1 or 2. So q^d-1 has a primitive prime divisor p. Since $p \nmid q^{t+1}-1$, the size of T is divisible by p^i, the largest power of p dividing q^d-1. But then $p^i \,\big|\, |H|$. Hence H has a subgroup P of order p^i. But by Lemma 5.3 this is the unique Sylow p subgroup of $\Gamma\mathrm{L}_1(q)$.

Suppose that $f : \mathbb{F} \to \mathbb{F}$ maps S to T. Let $g \in P$. Then $gf(S) = T$ so $f^{-1}gf(S) = S$. Thus the conjugation of g by f preserves S, so it is in $\Gamma\mathrm{L}_1(q)$. Now conjugate groups are isomorphic, so $f^{-1}Pf$ is a Sylow p subgroup of $\Gamma\mathrm{L}_1(q)$. But by Lemma 5.3 this is unique, and so $f^{-1}Pf = P$. Thus by Lemma 5.4 f is an element of $\Gamma\mathrm{L}_1(q)$.

The converse is true by definition. □

Theorem 5.5 is the tool we need to classify t-spreads of a particular vector space. We can now list all equivalence classes of soluble t-spreads of a finite field $\mathbb{F}$ as a vector space over a prime field $\mathbb{K}$ by the following method:

1. Begin with a list of all subspaces of $\mathbb{F}$ whose orbits under a subgroup of $\Gamma\mathrm{L}_1(q)$ could potentially be a t-spread.

2. Look at the orbits of these subspaces under the various subgroups of $\Gamma\mathrm{L}_1(q)$, and form a list of those which are t-spreads. We only need examine one subgroup for each conjugacy class, because if G acts transitively on a spread S, then G^a acts transitively on aS.

3. The equivalence class of a t-spread is simply the orbit of that t-spread under $\Gamma\mathrm{L}_1(q)$. So we can return the set of all such orbits as our list of equivalence classes.

This method is implemented in Code Listing I for the case when $\mathbb{K}$ is a prime field. (This restriction avoids some complexity in the code, and besides, when $\mathbb{K} = \mathbf{GF}(p^d)$ is not prime, any t-spread of $\mathbb{F} = \mathbf{GF}(p^{(t+1)dm})$ over $\mathbb{K}$ is just a $((t+1)d-1)$-spread of $\mathbb{F}$ over $\mathbf{GF}(p)$.)

What happens to Theorem 5.5 if $d \leq 2$? If $d = 1$ then $t = 0$ and the t-spread is trivial, while if $d = 2$ then either $t = 1$ and the t-spread is trivial, or $t = 0$ and the t-spread is desarguesian.

5.3 Cyclic line spreads

Lemma 5.6. *Suppose* $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$. *Then any* $\mathbb{K}$*-linear injection* $\mathbb{L} \to \mathbb{F}$ *can be* uniquely *written in the form*

$$x \mapsto ux - v\overline{x}$$

for some $u, v \in \mathbb{F}$.

Proof. Let f be a $\mathbb{K}$-linear injection $\mathbb{L} \to \mathbb{F}$. Choose some element $\ell \in \mathbb{F} - \mathbb{K}$. Then u and v are given by the equations

$$v = \frac{f(\ell) - f(1)}{\ell - \overline{\ell}}$$
$$u = f(1) - \frac{f(\ell) - f(1)}{\ell - \overline{\ell}}.$$

□

The above lemma has the following application: suppose that $a, b, c, d \in \mathbb{F}$ such that

$$ax - b\overline{x} = cx - d\overline{x}$$

for all $x \in \mathbb{L}$. Then $a = c$ and $b = d$. The following proposition will give us a standard form for line spreads.

Proposition 5.7. *Let* $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$. *Up to equivalence, any soluble line spread of* $\mathbb{F}$ *as a vector space over* $\mathbb{K}$ *is of the form*

$$U^G = \{U^g : g \in G\}$$

where $G \leq \Gamma\mathrm{L}_1(q^{2m})$ *and* U *is the set* $\{x - b\overline{x} : x \in \mathbb{L}\}$ *for some* b.

Proof. Let S be a line spread admitting H as a transitive group. Let V be an element of S. Then V is the image of $\mathbb{L}$ under some $\mathbb{K}$-linear injection, and so by Lemma 5.6 it is the set $T = \{ux - v\overline{x} : x \in \mathbb{L}\}$. Let $b = v/u$. Then (with the action of $\mathbb{F}^*$ on $\mathbb{F}$ by multiplication):

$$\begin{aligned}
(T^H)^{u^{-1}} &= \left((T^{u^{-1}}u)^H\right)^{u^{-1}} \\
&= (T^{u^{-1}})^{H^u} && \text{writing } H^u = u^{-1}Hu \\
&= (\{ux - v\overline{x} : x \in \mathbb{L}\}^u)^{H^u} \\
&= \{x - b\overline{x} : x \in \mathbb{L}\}^{H^u}
\end{aligned}$$

and letting $G = H^u$ shows us that S is equivalent (via the map $z \mapsto u^{-1}z$) to a set of the desired form. □

Remark 5.8. In the above proof, we began with a group H transitive on S, and turned it into $G = H^u$ transitive on a spread equivalent to S. So when looking for line spreads admitting a *particular* group G, we need only look for standard form line spreads admitting a group conjugate to G.

Let's examine the case when the group G acting transitively on S is a subgroup of $\mathbb{F}^*$. We will call t-spreads with a cyclic transitive group **cyclic t-spreads** (this condition does not imply that $\mathrm{Stab}_{\Gamma\mathrm{L}_1(q)}(S)$ is cyclic; just that it contains a cyclic group acting transitively on S.) Since any spread of $\mathbb{F}$ as a vector space over $\mathbb{K}$ admits multiplication by elements of $\mathbb{K}^*$, we can assume that $\mathbb{K}^* \leq G$. As spreads of $\mathrm{PG}_{d-1}(q)$ they admit a transitive cyclic group of order divisible by the size of the spread $(q^d - 1)/(q^2 - 1)$, so it must have a subgroup of precisely that order. Thus G contains a subgroup H transitive on S (and containing K^*) such that H/K^* has order $(q^d - 1)/(q^2 - 1)$. Hence H has order $(q^d - 1)(q - 1)/(q^2 - 1)$.

We will now see that this group acting transitively on S is precisely the group

$$\{z \in \mathbb{F}^* : N_{F/L}(z) \in \mathbb{K}\}$$

for $\mathbb{F}^*$ is cyclic and so it has a unique subgroup of order $(q^d - 1)(q - 1)/(q^2 - 1)$. But $N_{F/L}(z) \in \mathbb{K}$ if and only if $z^{(q^d-1)/(q^2-1)} \in \mathbb{K}$ and this is true if and only if $z^{\left((q^d-1)/(q^2-1)\right)(q-1)} = 1$, so the above group has order $(q^d - 1)(q - 1)/(q^2 - 1)$ and so it is H.

The following proposition now gives us a standard form for *cyclic* line spreads.

Proposition 5.9. *Let $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$. Any cyclic line spread of $\mathbb{F}$ as a vector space over $\mathbb{K}$ is equivalent to one of the form*

$$\{x - b\overline{x} : x \in \mathbb{L}\}^C$$

where C is the group $\{z \in \mathbb{F}^* : N_{F/L}(z) \in \mathbb{K}\}$ and b is an element of $\mathbb{F}$.

Proof. Let S be a line spread of $\mathbb{F}$ with cyclic transitive group H. Then by Proposition 5.7, the line spread S is equivalent to a line spread of the form $H^u\{x - b\overline{x} : x \in \mathbb{L}\}$. But H^u is conjugate to H so it is also cyclic. Hence by the above discussion, H contains the group G. □

We will write the standard form of a cyclic line spread as

$$S_b = h_b(\mathbb{L})^C \tag{5.3.1}$$

where $C = \{z \in \mathbb{F}^* : N_{F/L}(z) \in \mathbb{K}\}$ and $h_b = \{x - b\overline{x} : x \in \mathbb{L}\}$. Now we shall find a necessary and sufficient condition for two such line spreads S_b and S_c to be equivalent.

Lemma 5.10. *Let $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$, with $m \geq 2$ and $q^{2m} \neq 64$. Let $b, c \in \mathbb{F} - \mathbb{L}$. Let*

$$S_b = h_b(\mathbb{L})^C$$
$$S_c = h_c(\mathbb{L})^C$$

where $C = \{z \in \mathbb{F}^* : N_{F/L}(z) \in \mathbb{K}\}$, $h_b = \{x - b\overline{x} : x \in \mathbb{L}\}$, and $h_c = \{x - c\overline{x} : x \in \mathbb{L}\}$. Suppose that S_b and S_c are line spreads. Then S_b and S_c are equivalent if and only if

$$b = \frac{v + \overline{u}c^\sigma}{u + \overline{v}c^\sigma}$$

for some $u, v \in \mathbb{L}$, and some $\sigma \in \mathrm{Aut}(\mathbb{F})$.

Proof. We know that S_b and S_c are equivalent if and only if there exists a map

$$g : \mathbb{F} \to \mathbb{F}$$
$$x \mapsto zx^\phi$$

which carries $h_b(\mathbb{L})$ to $h_c(\mathbb{L})$, and this is true if and only if there is an isomorphism f from $\mathbb{L}$ to itself such that $gh_b(\mathbb{L}) = h_c f(\mathbb{L})$. By Lemma 5.6 we can write $f(x)^{\phi^{-1}} = ux - v\overline{x}$ for some $u, v \in \mathbb{L}$. Thus

$$z(x - b\overline{x})^\phi = (ux - v\overline{x})^\phi - c\overline{(ux - v\overline{x})^\phi}$$

for every $x \in \mathbb{L}$. Rearranging,

$$zx - zb\overline{x} = (u + \overline{v}c^{\phi^{-1}})x - (v + \overline{u}c^{\phi^{-1}})\overline{x}$$

and so by the uniqueness part of Lemma 5.6, we have $z = u + \overline{v}\, c^{\phi^{-1}}$ and

$$b = \frac{v + \overline{u}\, c^{\phi^{-1}}}{z} = \frac{v + \overline{u}\, c^{\phi^{-1}}}{u + \overline{v}\, c^{\phi^{-1}}}$$

and letting $\sigma = \phi^{-1}$ gives the desired result. Conversely, if $b - (v + \overline{u}\, c^{\sigma})/(u + \overline{v}\, c^{\sigma})$ then the maps $f(x) = ux - v\overline{x}$ and $g(x) = zx^{\sigma^{-1}}$ satisfy $gh_b(\mathbb{L}) = h_c f(\mathbb{L})$, and so h_b and h_c are equivalent. □

Remark 5.11. In light of Lemma 5.10, if S_b is a spread, then the linear space formed from it by the André/Bruck-Bose construction will be a desarguesian affine space *if and only if* $b \in \mathbb{L}$.

Proposition 5.12. *Let* $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$, *with* $m \geq 2$ *and* $q^{2m} \neq 64$. *Let* $b, c \in \mathbb{F} - \mathbb{L}$. *Let*

$$S_b = h_b(\mathbb{L})^C$$
$$S_c = h_c(\mathbb{L})^C$$

where $C = \{z \in \mathbb{F}^* : N_{F/L}(z) \in \mathbb{K}\}$, $h_b = \{x - b\overline{x} : x \in \mathbb{L}\}$, *and* $h_c = \{x - c\overline{x} : x \in \mathbb{L}\}$. *Suppose that* S_b *and* S_c *are line spreads. Then*

(i) *if* $h_b(\mathbb{L}) = h_c(\mathbb{L})$ *then either* $b = c$ *or* S_b *is desarguesian*

(ii) *if* S_b *admits multiplication by an element* z *such that* $N_{F/L}(z)$ *is* not *in* $\mathbb{K}$, *then* S_b *is desarguesian.*

Proof. (i) Suppose $h_b(\mathbb{L}) = h_c(\mathbb{L})$. Then there is an isomorphism $f : \mathbb{L} \to \mathbb{L}$ such that $h_b(x) = h_c(f(x))$. By Lemma 5.6 there are $u, v \in \mathbb{L}$ such that

$$\begin{aligned} x - b\overline{x} &= (ux - v\overline{x}) - c\,\overline{(ux - v\overline{x})} \\ &= (ux - v\overline{x}) - c(\overline{u}\,\overline{x} - \overline{v}x) \\ &= (u + c\overline{v})x - (v + c\overline{u})\,\overline{x} \end{aligned}$$

By Lemma 5.6 we have $1 = u + c\overline{v}$, so c is in $\mathbb{L}$ and so S_c (and hence S_b) is desarguesian by Remark 5.11.

(ii) Suppose S_b admits multiplication by z, and $N_{F/L}(z)$ is not in $\mathbb{K}$. Let G be the stabiliser of S in $\mathbb{F}^*$, and let H be the kernel of the action of G on S. Then H is normal in G and G/H has a faithful transitive action on S. But G/H is abelian so by Lemma 2.4, G/H is regular on S. Thus G/H has order $(q^{2d} - 1)/(q - 1)$. So any element g of G/H satisfies $g^{(q^{2d}-1)/(q-1)} = 1$. Thus

$\ell = z^{(q^2-1)/(q-1)}$ is in the kernel of the action, that is, it fixes every element of S_b. In particular, it fixes $h_b(\mathbb{L})$. So

$$\begin{aligned} h_b(\mathbb{L}) &= \ell h_b(\mathbb{L}) \\ &= \ell\{x - b\overline{x} \,:\, x \in \mathbb{L}\} \\ &= \{\ell x - b\ell\overline{x}\} \\ &= \{\ell x - (\ell/\overline{\ell})\overline{(\ell x)}\} \\ &= \{y - (\ell/\overline{\ell})b\overline{y} \,:\, y \in \mathbb{L}\} && \text{reparametrising by } y = \ell x \\ &= h_{(\ell/\overline{\ell})b}(\mathbb{L}). \end{aligned}$$

□

Theorem 5.13. *Let $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$. Let $b \in \mathbb{F} - \mathbb{L}$ and let P be the minimal polynomial of b over $\mathbb{L}$, and suppose P has degree d. Let*

$$S_b = h_b(\mathbb{L})^C$$

where $C = \{z \in \mathbb{F}^* : N_{F/L}(z) \in \mathbb{K}\}$ and $h_b = \{x - b\overline{x} \,:\, x \in \mathbb{L}\}$. Then S_b is a line spread if and only if for any $x, y \in \mathbb{L}$,

$$\frac{\overline{x}^m P(x/\overline{x})^{m/d}}{\overline{y}^m P(y/\overline{y})^{m/d}} \in \mathbb{K} \implies \frac{x}{y} \in \mathbb{K}. \tag{5.3.2}$$

Proof. Since every element of S_b is a $\mathbb{K}$-subspace of $\mathbb{F}$, multiplication by elements of $\mathbb{K}$ fixes every element. The size of C is $(q^{2m} - 1)(q - 1)/(q^2 - 1)$ and the size of one element of S_b is $(q^2 - 1)$. Thus S_b will cover all the points if and only if $s_1 h_b(\mathbb{L})$ and $s_2 h_b(\mathbb{L})$ have intersection $\{0\}$ whenever s_1 and s_2 are different elements of C such that $s_1/s_2 \notin \mathbb{K}$. Dividing by s_2 we see that this condition reduces to $h_b(\mathbb{L})$ and $s h_b(\mathbb{L})$ have intersection $\{0\}$ whenever $s \notin \mathbb{K}$.

Suppose that x and y are nonzero elements of $\mathbb{L}$. Then $s h_b(x) = h_b(y)$ for some $s \in C$ if and only if $N_{F/L}(h_b(x)) = N_{F/L}(h_b(y))$ (because C is precisely the group of elements of norm 1.) and this is true if and only if

$$N_{F/L}\left(\frac{x - b\overline{x}}{y - b\overline{y}}\right) \in \mathbb{K}. \tag{5.3.3}$$

By 2.12 this is equivalent to

$$\left(\frac{\overline{x}^m P(x/\overline{x})^{m/d}}{\overline{y}^m P(y/\overline{y})^{m/d}}\right) \in \mathbb{K}. \tag{5.3.4}$$

($\Leftarrow$) If Equation 5.3.2 is true then Equation 5.3.4 implies that $x/y \in \mathbb{K}$. But writing $x = ky$ for some $k \in \mathbb{K}$, we have $s = (ky - b\overline{ky})/(y - b\overline{y}) = k \in \mathbb{K}$. So $h_b(\mathbb{L})$ and $sh_b(\mathbb{L})$ only have nontrivial intersection when $s \in \mathbb{K}$.

($\Rightarrow$) Now we suppose that Equation 5.3.4 holds for some x_0 and y_0 with $x_0/y_0 \notin \mathbb{K}$. Then there is an element $s \in C$ such that

$$s(x_0 - b\overline{x_0}) = (y_0 - b\overline{y_0}). \tag{5.3.5}$$

So for S_b to be a spread, $h_b(\mathbb{L})$ and $sh_b(\mathbb{L})$ must be the exact same subspace. But then s is in the kernel of the action of C on S_b. If $s \in \mathbb{L}$ then Equation 5.3.5 implies that

$$b = \frac{y_0 - sx_0}{\overline{y_0} - s\overline{x_0}} \in \mathbb{L}$$

contradicting our hypothesis, so it must be that $s \notin \mathbb{L}$. But then there is $s \notin \mathbb{K}$ such that $h_b(\mathbb{L})$ and $sh_b(\mathbb{L})$ have nontrivial intersection, and so S_b is not a line spread. □

Theorem 5.13 converts the question of finding cyclic line spreads into another question: finding irreducible polynomials which satisfy Equation 5.3.2. Letting $P'(x) = \overline{x}^m P(x/\overline{x})^{m/d}$, we are forced to ask: what does the condition

$$\frac{P'(x)}{P'(y)} \in \mathbb{K} \implies \frac{x}{y} \in \mathbb{K}$$

actually mean? Certainly polynomials satisfying this remind us of **permutation polynomials**, that is, polynomials R which satisfy

$$\frac{R(x)}{R(y)} = 1 \implies \frac{x}{y} = 1$$

and in fact they turn out to be the projective version of such polynomials, for the map

$$x\mathbb{K} \mapsto P'(x)\mathbb{K}$$

is well defined (because if $k \in \mathbb{K}$ then $P'(kx) = \overline{(kx)}^m P((kx)/\overline{(kx)}) = k^m P'(x)$) and it is a permutation of the $q + 1$ points of the projective line $\mathrm{PG}_1(q)$.

5.4 A new class

Theorem 5.14. *Let p be a prime, and let $\mathbb{K} = \mathbf{GF}(p) \subset \mathbb{L} = \mathbf{GF}(p^2)$. Then the polynomial*

$$P(x) = \frac{x^{p+1} - 1}{x - 1} - 2$$

is irreducible and satisfies Equation 5.3.2 and so the roots of P in $\mathbf{GF}(p^{2p})$ *satisfy the conditions of Theorem 5.13 and can be used to construct line spreads.*

Proof. By Lemma 2.11 P is irreducible so we only need to prove that it satisfies Equation 5.3.2. Suppose that for some $x, y \in \mathbb{L}$

$$\frac{\overline{x}^{\,p} P(x/\overline{x})}{\overline{y}^{\,p} P(y/\overline{y})} \in \mathbb{K}.$$

We will show that $P(x/\overline{x})/P(y/\overline{y}) \in \mathbb{K}$. Then, since $\overline{x}^{\,p} = \overline{\overline{x}} = x$ and similarly $\overline{y}^{\,p} = y$, it will follow that $x/y \in \mathbb{K}$, showing that P satisfies Equation 5.3.2.

Now $x/\overline{x} = x^{-(p-1)}$ and so $(x/\overline{x})^{p+1} = x^{-(p^2-1)} = 1$. So, if $x/\overline{x} \neq 1$ then

$$\begin{aligned} P(x/\overline{x}) &= \frac{(x/\overline{x})^{p+1} - 1}{(x/\overline{x}) - 1} - 2 \\ &= \frac{1-1}{x/\overline{x} - 1} - 2 = 0 - 2 = -2 \end{aligned}$$

while if $x/\overline{x} = 1$ then

$$\begin{aligned} P(x/\overline{x}) = P(1) &= \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} - 1 \qquad \text{since it is Equation 2.5.1} \\ &= -1. \end{aligned}$$

But this means that both $P(x/\overline{x})$ and $P(y/\overline{y})$ are either -1 or -2, and so $P(x/\overline{x})/P(y/\overline{y}) \in \mathbb{K}$. □

5.5 New from old

Here is a new trick which is analogous to Kantor's inflation trick in that it will allow us to form new larger linear spaces from smaller ones. The **order** of a polynomial P is the smallest integer $e \geq 0$ such that P divides the polynomial $q^e - 1$.

Theorem 5.15. *Suppose that $P(x)$ is an irreducible polynomial over* $\mathbf{GF}(q)$ *of degree m and order e. If $t \geq 3$ is odd such that all prime factors of t divide e but not $(q^m - 1)/e$, then $P(x^t)$ is irreducible.*

The proof of this Theorem is contained in [22, Theorem 3.35].

Theorem 5.16. *Suppose that* $\mathbb{K} = \mathbf{GF}(q) \subset \mathbb{L} = \mathbf{GF}(q^2) \subset \mathbb{F} = \mathbf{GF}(q^{2m})$ *and that m is odd. Suppose that $P(x)$ is an irreducible polynomial of degree m over $\mathbb{L}$ satisfying Equation 5.3.2. Let P have order e. If $t \geq 3$ is odd such that all prime factors of t divide e but not $(q^{2m} - 1)/e$ or $q^2 - 1$, then $P(x^t)$ is an irreducible polynomial satisfying Equation 5.3.2.*

Proof. By Theorem 5.15, $P(x^t)$ is irreducible. So it suffices to show that $P(x^t)$ satisfies Equation 5.3.2.

Suppose

$$\frac{\overline{x}^m P((x^t)/(\overline{x}^t))}{\overline{y}^m P((y^t)/(\overline{y}^t))} \in \mathbb{K}.$$

Then, since P satisfies Equation 5.3.2,

$$\frac{x^t}{y^t} \in \mathbb{K}.$$

Now t is coprime to $q^2 - 1$, so the map $x \mapsto x^t$ is a bijection which leaves $\mathbb{K}$ invariant. Hence $x/y \in \mathbb{K}$. □

Example 5.17. The polynomial from Theorem 5.14 when $p = 3$ is

$$P(x) = x^3 + x^2 + x - 1$$

and this polynomial can be computed to have order $e = 13$. Now $3^{3\times 2}-1 = 728$ and $728/13 = 56$ which is not divisible by 13. Also $3^2 - 1 = 8$ is not divisible by 13. Hence by Theorem 5.16, the polynomial

$$P(x^{13^k}) = x^{3\times 13^k} + x^{2\times 13^k} + x^{13^k} - 1$$

is irreducible and satisfies Equation 5.3.2 and so these polynomials can be used to construct line spreads of $\mathrm{PG}_{6\times 13^k-1}(3)$ for every integer $k \geq 1$.

Chapter 6

Concluding remarks

There are a variety of ways to construct a flag-transitive linear space. Of greatest popularity appears to be the use of a transitive spread – perhaps because the resulting flag-transitive linear space is also an affine plane. However, as Kantor says in [21], constructing flag-transitive linear spaces of other kinds has received surprisingly little attention. Transitive line spreads give one such type of linear space. In Theorem 5.14 we have constructed a class of line spreads of projective spaces of different dimensions to Kantor's examples. These line spreads give rise to new flag-transitive linear spaces which are not planes.

In Theorem 5.13 we converted the problem of finding line spreads with a transitive cyclic group into the problem of finding irreducible polynomials which, in a certain way, induce a permutation of the projective line $\mathrm{PG}_1(q)$. This condition helps us search for cyclic line spreads computationally, and GAP code to take advantage of this is in code listing II. It also helps in the proof of Theorem 5.14.

Theorem 5.16 allows us to construct new line spreads from old ones. Further study of this theorem is desired. In particular, it would be good to know how often the conditions are satisfied for the theorem to be invoked. It would also be worth seeing to what extent the theorem can be generalised. The code given in the appendices will be made available for download at

https://www.maths.uwa.edu.au/Members/paulem01/

so the reader can find line spreads of his or her own. Polynomials abound which satisfy the condition of Theorem 5.13 but do not appear to belong to any general class, and this gives more evidence for Kantor's claim that a complete classification of flag-transitive linear spaces seems unlikely – even for the case of cyclic line spreads!

Appendix A

Cyclotomic polynomials, Zsigmondy's Theorem and Wedderburn's Theorem

Suppose $q \geq 2, d \geq 1$ are integers. A **primitive prime divisor** (or **ppd**) of $q^d - 1$ is a prime number which divides $q^d - 1$ but does not divide $q^k - 1$ for $k < d$. Note that primitive prime divisors depend on the numbers q and d, and not just on $q^d - 1$. For example, if we write 63 as $4^3 - 1$ then it has 7 as a ppd, but if we write it as $2^6 - 1$ then it has no ppds. For this reason, it is sometimes written "a ppd of the pair $\langle d, q \rangle$." An equivalent definition for a ppd of $q^d - 1$ is a prime p such that $(q, p) = 1$ and the order of $q \pmod{p}$ is d.

Let ζ_n be some primitive n root of unity. The **cyclotomic polynomial** of order n is the polynomial

$$\Phi_n(x) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (x - \zeta_n^i)$$

Our purpose is to use cyclotomic polynomials to prove:

Zsigmondy's Theorem for any integers $q \geq 2, d \geq 1$, there is a primitive prime divisor of $q^d - 1$, except when $q = 2^s, d = 2$ or when $q = 2, d = 6$.

Wedderburn's Theorem Every finite division ring is a field.

Property A.1.

$$\prod_{d|n} \Phi_d(x) = x^n - 1$$

Proof.

$$\prod_{d|n} \Phi_d(x) = \prod_{d|n} \prod_{\substack{i=1 \\ (i,n)=1}}^{d} (x - \zeta_d^i)$$

The ζ_d^j cover all the roots of unity. So this equals

$$\prod_{j=1}^{n} (a - \zeta_d^j)$$

which is the polynomial factorisation of $a^n - 1$. □

A polynomial is **monic** if the coefficient of its dominant term (that is, the term with the highest power of the indeterminant) is 1.

Lemma A.2. *Suppose that Q and R are monic polynomials with coefficients in the integers, and that $PQ = R$ for a polynomial P. Then P is monic with coefficients in the integers.*

Proof. Suppose that P has order m and Q has order n. Let P_i be the coefficient of the x^i term in P. Then

$$P_m \times Q_n = R_{m+n}$$

so $P_m \times 1 = 1$, and $P_m = 1$, that is P is monic.

Now consider the coefficient of x^{m+n-i} in R. We have

$$R_{m+n-i} = P_m Q_{n-i} + P_{m-1} Q_{n-i+1} + \cdots + P_{m-i+1} Q_{n-1} + P_{m-i} Q_n$$

thus

$$P_{m-i} = \frac{R_{m+n-i} - P_m Q_{n-i} - P_{m-1} Q_{n-i+1} - \cdots - P_{m-i+1} Q_{n-1}}{Q_n}$$

We know that $P_m = 1$, and by this equation we see that if $P_m - j$ is an integer for all $j < i$, then P_{m-i} is an integer. Thus by induction P_i is an integer for all i. □

Property A.3. *The polynomial Φ_n is monic with integer coefficients, and therefore maps integers to integers.*

Proof. By induction. $\Phi_1(x) = x - 1$ so the property holds for $n = 1$. By A.1 we have

$$\Phi_n(x) \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x) = a^n - 1$$

Now $a^n - 1$ is a monic polynomial in the integers, and by the induction hypothesis, $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$ is a monic polynomial in the integers, so by A.2, Φ_d is a monic polynomial in the integers. □

Property A.4. *Suppose that $n = p^i r$ with p prime and $p \nmid r, r \geq 1$. Then*

$$\Phi_n(x) = \frac{\Phi_r(x^{p^i})}{\Phi_r(x^{p^{i-1}})}$$

Proof. The roots of $\Phi_n(x)$ are the primitive n roots of unity. The roots of $\Phi_r(x^{p^i})$ are the p^i roots of primitive r roots of unity. The roots of $\Phi_r(x^{p^{i-1}})$ are the non-primitive p^i roots of unity. So the roots of $\Phi_r(x^{p^i})/\Phi_r(x^{p^{i-1}})$ are the primitive p^i roots of primitive r roots of unity – that is, the primitive n roots of unity. Both sides of the equation have the same roots, and they are both monic polynomials, so they are equal. □

Property A.5. *Let $a \in \mathbb{Z}, n = q^i r$ with q prime, $q \nmid r$. Let $b = a^{q^{i-1}}$. Then*

$$\Phi_n(a) > (b^{q-2}(b-1))^{\phi}(r)$$

where ϕ is the totient function.

Proof. By property A.4,

$$\begin{aligned}
\Phi_n(a) &= \frac{\Phi_r(a^{q^i})}{\Phi_r(a^{q^{i-1}})} = \frac{\Phi_r(b^q)}{\Phi_r(b)} \\
&= \prod_{\substack{j=1 \\ (j,r)=1}}^{r} \frac{b^q - \zeta_r^j}{b - \zeta_r^j} \\
&> \prod_{\substack{j=1 \\ (j,r)=1}}^{r} \frac{b^q - 1}{b - 1} && \text{because it is real} \\
&= \left(\frac{b^q - 1}{b - 1}\right)^{\phi(r)} \\
&> (b^{q-2}(b-1))^{\phi(r)}
\end{aligned}$$

□

I Zsigmondy's Theorem

The proof we present here is based on that given in [29].

Lemma A.6. *Suppose $a \geq 2, n \geq 2$ are integers. Suppose p is a prime factor of $\Phi_n(a)$. Then the following are equivalent:*

(i) p is not a primitive prime divisor of $a^n - 1$

(ii) $p \mid n$

(iii) p is the largest prime divisor of n

Proof. Note that $p \mid \Phi_n(a) \mid a^n - 1$ so $a^n \equiv 1 \pmod{p}$.

((i)⇒(ii)) Suppose that $p|n$. Then

$$\begin{aligned} a^{n/p} &\equiv a^n \pmod{p} && \text{by Fermat's little theorem} \\ &\equiv 1 \pmod{p} \end{aligned}$$

So the order of a is less than n.

((ii)⇒(i)) Now assume that the order of $a \pmod{p}$ is not n. Since n is not the order of a there exists a prime γ dividing n such that $a^{n/\gamma} \equiv 1 \pmod{p}$. Let $c = a^{n/\gamma}$. Now $\Phi_n(a) \mid (a^n - 1)/(a^{n/\gamma})$ so

$$\begin{aligned} p \mid \frac{c^\gamma - 1}{c - 1} &= \sum_{i=0}^{\gamma-1} c^i \\ &\equiv \sum_{i=0}^{\gamma-1} 1 \pmod{p} && \text{since } c \equiv 1 \pmod{p} \\ &\equiv \gamma \pmod{p} \end{aligned}$$

Hence $p \mid \gamma$ and since γ is prime, $\gamma = p$. But then $p \mid n$.

((ii)⇒(iii)) From the proof that ((ii)⇒(i)), we have that $p \mid n$ and for any prime $\gamma \neq p$, $a^{n/\gamma} \not\equiv 1 \pmod{p}$. So the order of $a \pmod{p}$ is of the form n/p^i for some $i \geq 1$, and this divides $p - 1$ (since $a^{p-1} \equiv 1 \pmod{p}$ by Fermat.) So $r = n/p^i$ divides $p - 1$ and p is the largest prime factor of n.

((iii)⇒(i)) Largest prime divisors are divisors. □

Lemma A.7. *Let $a \geq 2, n \geq 2$. Suppose that p is a prime such that $p \mid n$ and $p^2 \mid \Phi_n(a)$. Then $p = n = 2$.*

Proof. If $p > 2$, let $d = a^{n/p} - 1$. So $p \mid d$ (see the ((ii)⇒(i) part of A.6) and

$$\begin{aligned}
\frac{a^n - 1}{a^{n/p} - 1} &= \frac{(1+d)^p - 1}{d} \\
&= \frac{\left(\sum_{i=0}^{p} \binom{p}{i} d^i\right) - 1}{d} \\
&= \frac{\sum_{i=1}^{p} \binom{p}{i} d^i}{d} \\
&= \frac{\binom{p}{1} d + \sum_{i=2}^{p} \binom{p}{i} d^i}{d} \\
&= p + \frac{(\cdots) p d^2}{d} \\
&\equiv p \pmod{p}^2 \qquad \text{because } d \equiv 0 \pmod{p}
\end{aligned}$$

□

Lemma A.8. *If $a \geq 2$ and $n \geq 2$ are integers, and there are no ppds of $a^n - 1$, then $\Phi_n(a)$ is a prime power. If in addition $n > 2$, then $\Phi_n(a)$ is a prime.*

Proof. If $\Phi_n(a)$ is not a prime power, then it has a prime divisor which is not the largest, and that number is a ppd.

If in addition $n > 2$, then $p^2 \nmid \Phi_n(a)$ for any prime p, so $\Phi_n(a)$ is a square-free prime power – a prime. □

Theorem A.9 (Zsigmondy). *Suppose $a \geq 2, n \geq 2$ are integers. There is a primitive prime divisor of $a^n - 1$ except in the following cases:*

- *$a = 2^s - 1$ for some integer $s \geq 2$, and $n = 2$*
- *$a = 2$ and $n = 6$*

Proof. We first prove that the above listed exceptions are truly exceptions. Suppose $a = 2^s - 1$ and $n = 2$. Then $a^n - 1 = (2^s - 1)^2 - 1 = 2^s(2^s - 2)$ So any prime divisor of $a^n - 1$ is either 2 or a divisor of $2^s - 2$. But $2^s - 2 = a - 1$, and it is divisible by 2, so any prime divisor of $a^n - 1$ is a divisor of $a - 1$. Now suppose $a^n - 1 = 2^6 - 1 = 63$. The prime divisors of 63 are 3 and 7 but $3 \mid 3 = 2^2 - 1$ and $7 \mid 7 = 2^3 - 1$ so 63 has no ppds.

Now we shall prove that all other numbers $a^n - 1$ have ppds. Suppose that there are numbers a and n which do not have any ppds. If $n = 2$ (and $\Phi_n(a) = (a - i)(a + i) = a + 1$) then since all

prime factors of $\Phi_n(a)$ are non-ppds, they all divide n by lemma A.6. So $a+1=2^s$ for some s – this is the first exception listed.

Suppose $n>2$. So $\Phi_n(a)$ is a prime p by lemma A.8. If $p=2$ then since it is the largest prime divisor of n, we have $n=2^s$. But then $\Phi_n(a)=(a^{2^s}-1)/(a^{2^{s-1}})=a^{2^{s-1}}+1>2$, a contradiction. So $p\geq 3$. Let $n=p^ir$ where $p\nmid r$. Let $b=a^{p^{i-1}}$. Then by property A.5 we have

$$p>(b^{p-2}(b-1))^{\phi(r)}\geq b^{p-2}$$

Now

$$b^{p-2}<p$$

and $b\geq 2$ so

$$2^{p-2}<p.$$

But if $p\geq 4$ then $2^{p-2}\geq p$, so

$$p=3$$

but then $p^{p-2}<p$ implies that $b<3$, so $b=2$. Since $b=a^{p^{i-1}}$ we have $a=2$.

Finally, since $r\mid(p-1)$, we have $r=1$ or $r=2$. So either $a=2,n=3$ or $a=2,n=6$. In the first case, we have 7 as a ppd of $2^3-1=7$ so $a=2$ and $n=6$. □

Remark A.10. Since $a^n\equiv 1 \pmod p$ when p is a ppd, and $a^{p-1}\equiv 1 \pmod p$ (by Fermat) we see that $n\mid(p-1)$. So when looking for ppds of a^n-1 we need only look at numbers of the form $kn+1$.

II Wedderburn's Theorem

Theorem A.11 (Wedderburn). *If E is a finite division ring then E is a field.*

Proof. Suppose that E is not a field. Let K be the centre of E. Then K is a field of order some prime power q. Treat E as a vector space over K. Then $|E|=q^n$ for some n.

Let $\alpha\in E-K$. The centraliser $C(\alpha)$ of α is a proper subring of E, with order q^d for some d (d depends on α.) Now $|C^*|=q^d-1$ and $|E^*|=q^n-1$. So $q^d-1\mid q^n-1$. This can only be true if $d\mid n$.

The conjugates of α correspond to cosets of C^* in E^*. So every conjugacy class in E^* has size $(q^n-1)/(q^d-1)$ for some proper divisor d of n. The centre, K^*, has size $q-1$.

The centre along with all the conjugacy classes outside the centre form a partition of E. So we have

$$q^n - 1 = |E^*| = \underbrace{\sum_i \frac{q^n - 1}{q^{d_i} - 1}}_{\text{conjugacy classes outside centre}} + \underbrace{q - 1}_{\text{centre}}$$

Now $\Phi_n(q) \mid q^n - 1$ and $\Phi_n(q) \mid \frac{q^n-1}{q^{d_i}-1}$ for proper divisors d_i of n. So $\Phi_n(q) \mid q - 1$. But if $n > 1$ then $|q - \zeta_n^i| > q - 1$ for every factor in $\Phi_n(q)$. So $n = 1$, that is, $E = K$. □

Appendix B

Applications of regular linear spaces

We will now see two applications of regular linear spaces: the construction of experimental designs, and the construction of error correcting codes. Neither of these expositions are particularly deep; more information can be found in, for example, [10] (experimental designs) and [30] (coding and information theory). In both cases we will use the Fano plane for our constructions; this is because it is just the right size – not so small as to solve a trivial problem, but not too large as to convolute the example.

I Experimental designs

Suppose a collection of fertilisers must be tested on crops to determine which one will result in the highest crop yield. An experimental area is divided into plots, and each fertiliser is tested on one plot. A problem arises: what if there is some variation in the yields due to the plots themselves rather than the fertilisers? Perhaps the plots in one part of the experimental area have better soil than the plots in another part. To minimise the effect of this, we divide the experimental area into *blocks*, and further divide each block into plots, comparing the fertilisers within each plot. If the blocks are physically small enough then the variation within a block will be reduced and so the comparisons will be more accurate.

In general a number of *treatments* are to be compared to each other. The plots here are an example of *experimental units*, and experimental units are compared in blocks. Unfortunately it may be infeasible to have every treatment tested in every block.

For example, suppose that 7 different treatments are to be tested on 7 blocks. If we divide each of the 7 blocks into 7 plots, then there will be 49 plots in total! This could be too many

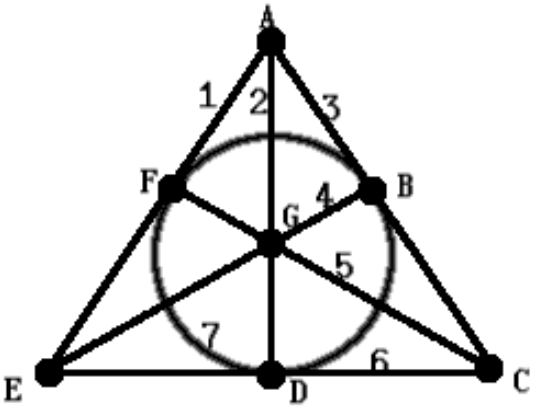


Figure B.1: The Fano plane.

– for example, 49 plots may take up too much space. Instead, we may choose to only have 3 experimental units in each block, and choose just 3 of the 7 treatments to compare in each block. This way we reduce the total number of blocks down to 21. This type of experimental design is called an *incomplete block design*. To make sure that we compare every two treatments with the same degree of accuracy, we may require that our incomplete block design satisfy the condition: *for every two treatments, there is some constant number λ of blocks containing both of them.* The condition just described is precisely the condition for a $2-(v,k,\lambda)$ design, where v is the number of treatments and k is the number of treatments compared in each block. When $\lambda = 1$, any two treatments are compared exactly once, and we have the condition for a regular linear space!

Let's construct an incomplete block design with $v = 7$ and $k = 3$. We begin with our Fano plane, and label the points according to each treatment and the lines according to each block, as in Figure B.1.

We can then form our experimental design: a treatment is tested in a block when the corresponding point lies in the corresponding line, as in Figure B.2.

II Error correcting codes

In digital communication systems a noisy line can lead to an error in a sent message. Suppose that a communication system uses a binary channel – for example, a computer may use a high voltage and a low voltage to send signals of "1" and "0" respectively. Suppose that the proba-

Block	Treatments		
1	A	E	F
2	A	D	G
3	A	B	C
4	B	G	H
5	C	F	G
6	C	D	E
7	B	D	F

Figure B.2: Construction of an experimental design.

bility of an error is a constant p regardless of which signal is sent, that is, the chance of a sent 1 being received as a 0 is p, and the chance of a sent 0 being received as a 1 is p. If p is high then it might be very difficult to send a message through the channel. In order to send a message, we use an *error correcting code*. This is a way of adding redundancy to messages so that the message can still get through even with some individual bits in error.

Suppose we have v different messages that we might like to send. An n-error correcting code is a set of v sequences of bits such that any two such sequences differ by *at least* $2n$ *bits*. We call the elements of the code *codewords*. If a receiver receives a codeword then it can immediately decode it to one of the v different messages. But if a sequence is received which does not match a codeword, then the receiver can guess what the original message was by choosing the codeword which differs from the received signal by the least number of bits. As long as at most n bits are in error, the receiver will correctly decode the message, so if $n > 0$ the chance of an error in the message will be less than the chance of an error in an individual bit.

If $\mathscr{S}$ is a regular linear space with v points and k points on each block, then by Lemma 3.3, the number of lines through each point will be

$$r = \frac{v-1}{k-1}$$

and the number of lines in total will be

$$b = \frac{v(v-1)}{k(k-1)}.$$

From $\mathscr{S}$ we will construct an $(r-1)$-error correcting code with v messages and a codeword length of b. We start by forming a table of the incidences of $\mathscr{S}$: there is a 1 in row i and column

j of the table if point i is incident with line j, and 0 otherwise. (The table here is the table formed from the Fano plane in Figure B.1.)

	1	2	3	4	5	6	7
A	1	1	1	0	0	0	0
B	0	0	1	1	0	0	1
C	0	0	1	0	1	1	0
D	0	1	0	0	0	1	1
E	1	0	0	1	0	1	0
F	1	0	0	0	1	0	1
G	0	1	0	1	1	0	0

Now we can form an error-correcting code: the codewords of our code will be the rows of this table. Because there is exactly one line between any two given points, any two rows must differ in at exactly $2r - 2$ bits. So the code formed in this way is $(r - 1)$-error correcting.

Appendix C

Lists of line spreads

Here we give a list of all line spreads of some projective spaces, found using the code of listing I. We list the line spreads by their group structure. A group G is written as $A : B$ when $G \cap \mathrm{GL}_1(q)$ has order A, and $G/(G \cap \mathrm{GL}_1(q))$ has order B. The group sizes listed are as subgroups of $\Gamma\mathrm{L}_1(q)$. To get the corresponding figures for the projective version, divide the cyclic part of the group by $p - 1$. If the stabiliser in $\Gamma\mathrm{L}_1(q)$ of the spread is $\Gamma\mathrm{L}_1(q)$ then the symbol $\geq \Gamma\mathrm{L}_1(q)$ is written; note that by Theorem 5.12 this is only possible when the spread is desarguesian.

The column "# isomorphism classes" lists the number of isomorphism classes of line spreads whose stabiliser is a group of the given structure. This equals the number of non-isomorphic linear spaces such that the stabiliser of a point has the given structure. (Note that "A:B" does not uniquely define the group: for example $Z_n \times Z_2$ and D_{2n} are both groups whose structure would be written $n : 2$.

I $\mathrm{PG}_3(3)$

t-spread size = $(3^4 - 1)/(3^2 - 1) = 10$.

Group	# isomorphism classes	Type
$10 : 4$	1	Kantor Type 5
$\geq \Gamma\mathrm{L}$	1	Desarguesian

II $\mathrm{PG}_5(3)$

t-spread size = $(3^6 - 1)/(3^2 - 1) = 91$.

Remark C.1. This space also contains the two Hering line spreads which are not soluble.

Group	# isomorphism classes	Type
182 : 2	1	Theorem 5.14
≥ ΓL	1	Desarguesian

III $PG_7(3)$

t-spread size = $(3^8 - 1)/(3^2 - 1) = 820$.

Group	# isomorphism classes	Type
1640	3	
820 : 2	3	
410 : 4	6	
410 : 8	12	
≥ ΓL	1	Desarguesian

IV $PG_3(5)$

t-spread size = $(5^4 - 1)/(5^2 - 1) = 26$.

Group	# isomorphism classes	Type
52 : 4	2	Kantor Type 5
≥ ΓL	1	Desarguesian

V $PG_5(5)$

t-spread size = $(5^6 - 1)/(5^2 - 1) = 651$.

Group	# isomorphism classes	Type
2604 : 2	2	
≥ ΓL	1	Desarguesian

VI $PG_3(7)$

t-spread size = $(7^4 - 1)/(7^2 - 1) = 50$.

Group	# isomorphism classes	Type
150 : 4	3	Kantor Type 5
≥ ΓL	1	Desarguesian

VII $PG_3(11)$

t-spread size = $(11^4 - 1)/(11^2 - 1) = 122$.

Group	# isomorphism classes	Type
610 : 4	5	Kantor Type 5
≥ ΓL	1	Desarguesian

Appendix D

Code listings

I Searching for transitive *t*-spreads

```
# return a finite field, listed in a guaranteed order. This is so that
# we can translate back and forth between linear groups on a field and
# permutation groups on the set [1..n]
ListField := function(F)
    local w;
    w := PrimitiveElement(F);
    return Concatenation([0*w], List([0 .. Size(F)-2], i -> w^i));
end;

# make a list of all potential "seed" spaces for making t-spreads
PotentialSeeds := function(F, e)
    local perpspace, spaces, d, w, p, seeds, one, minimumgroup;
    d := Dimension(F);
    w := PrimitiveElement(F);
    p := Size(PrimeField(F));
    one := w^0;

    # if G is a group acting transitively on a spread S (and G is contained
    # in GammaL) then G must contain the following group.
    minimumgroup := Group(w^(d*(p^e-1)));
```

```
    # find the space perpendicular to the prime field
    perpspace := Subspace(
        F,
        List([1..d-1], i -> wˆi)
        );
    # form all spaces containing the prime field
    spaces := List(
        Subspaces(perpspace,  e-1),
        s -> Subspace(F, Union([one], GeneratorsOfVectorSpace(s)))
        );

    # choose only those such spaces which "allow" multiplication by an element
    # of minimumgroup
    seeds := Filtered(
            spaces,
            S -> not ForAny(
                Difference(minimumgroup,[Identity(minimumgroup)]),
                g -> Size(Intersection(S,g*Set(S))) in [2..Size(S)-1]
                )
            );
    return seeds;
end;

# return (as a permutation group) GammaL(1, F) the one-dimensional semilinear group.
GammaL := function(F)
    local w, sigma, G, hom;
    # a generator of the multiplicative group of F (treated as a group of
    # addditive transformations F -> F
    w := LeftModuleHomomorphismByImages(
        F,
        F,
        List(GeneratorsOfVectorSpace(F)),
```

```
        List(GeneratorsOfVectorSpace(F), x -> x * PrimitiveElement(F))
        );
    # a generator of the automorphism group of F
    sigma := FrobeniusAutomorphism(F);
    # form GammaL, the group generated by the above two additive transformations
    G := Group(w, sigma);

    # return this group as a permutation group.
    return Action(G, ListField(F));
end;

GammaLSubgroupStructure := function(F, subgroup)
    local output, w, sigma, G, hom, gl, z1, z2;
    w := LeftModuleHomomorphismByImages(
        F,
        F,
        List(GeneratorsOfVectorSpace(F)),
        List(GeneratorsOfVectorSpace(F), x -> x * PrimitiveElement(F))
        );
    sigma := FrobeniusAutomorphism(F);
    G := Group(w);
    hom := ActionHomomorphism(G, ListField(F));
    gl := Image(hom);

    z1 := Intersection(subgroup, gl);
    z2 := FactorGroup(subgroup, z1);
    output := "";
    Append(output, String(Size(z1)));
    Append(output, ":");
    Append(output, String(Size(z2)));

    return output;
end;
```

```
# find all t-spreads of F as a vector space over the prime field
DisplayGammaLtSpreads := function(F,t)
    local   p, d,
        SpreadSize, seeds, fieldlist, gammal, subgroups, CanBeStitched,
        J, orbs, partialspreads, newspreads, i, j, spreadstostitch,
        Spreads, SpreadClasses, spreadgroup;

    p := Characteristic(F);
    d := Dimension(F);

    if p = 2 and d = 6 then
        Print("Warning: 2^6-1 has no ppds so this routine does not guarantee\n");
        Print("that it returns distinct classes!\n");
    fi;

    SpreadSize := (p^d - 1) / (p^(t+1) - 1);
    fieldlist := ListField(F);
    Print("Creating seeds...\n");

    # get a list of all potential seeds
    seeds := Set(List(
        PotentialSeeds(F, t+1),
        S -> Set(List(S, x->Position(fieldlist, x)))
        ));
    Print("There are ", Size(seeds), " good seeds.\n");

    Print("Forming potential groups...\n");

    # make all possible subgroups of GammaL(1,F)
    gammal := GammaL(F);
    subgroups := Filtered(
            SubgroupsSolvableGroup(
```

```
            gammal,
            rec(consider := SizeConsiderFunction(SpreadSize))
            ),
        t -> IsInt(Size(t) / SpreadSize)
        );

Sort(subgroups,
    function(G, H) return Size(G) < Size(H); end
    );

Print("There are ", Size(subgroups), " potential groups.\n");

CanBeStitched := [];
Spreads := [];

# for each subgroup G of GammaL(1,F), look at its orbits to see if any of them
# are t-spreads. If G contains a subgroup with no proper partial spreads, then
# G can contain no t-spreads, so we don't need to check it.
for i in [1..Size(subgroups)] do
    Print(i, ")\c ");

    spreadstostitch := false;

    for j in [1..i-1] do
        if IsSubgroup(subgroups[i], subgroups[j]) then
            if CanBeStitched[j] = false then
                Print("Contains group ", j, ". ");
                spreadstostitch := 0;
                break;
            elif spreadstostitch = false then
                spreadstostitch := CanBeStitched[j];
            elif Size(CanBeStitched[j]) < Size(spreadstostitch)
                then
```

```
                spreadstostitch := CanBeStitched[j];
            fi;
        fi;
    od;
    if spreadstostitch = 0 then
        Print("\n");
        Add(CanBeStitched, false);
        continue;
    fi;

    if spreadstostitch = false then
        orbs := Orbits(subgroups[i], seeds, OnSets);
    else
        orbs := Orbits(subgroups[i], spreadstostitch, OnSets);
    fi;
    orbs := Set(List(orbs, t -> Set(List(t, Set))));
    partialspreads := Filtered(orbs, o -> Size(o) <= SpreadSize and
        Size(Union(o)) = Size(o) * (Size(o[1])-1) + 1);
    newspreads := Filtered(partialspreads, o -> Size(o) = SpreadSize);
    if Size(partialspreads) > Size(newspreads) then
        Add(CanBeStitched, List(partialspreads, s -> s[1]));
    else
        Add(CanBeStitched, false);
    fi;
    Print("Found ", Size(newspreads), " spreads and ",
        Size(partialspreads) - Size(newspreads),
        " proper partial spreads.\n");
    Append(Spreads, newspreads);
od;
Spreads := Set(List(Spreads, Set));

# Get one example of each equivalence class of spreads.
# Fantastic fact: Any two spreads generated in the above manner
```

```
    # are equivalent in pgl <=> they are equivalent in N.
    SpreadClasses := Orbits(
                gammal,
                Spreads,
                OnSetsSets
                );
    SpreadClasses := List(SpreadClasses, x -> Set(List(x, Set)));
    Print("Total number of spread equivalence classes: ", Size(SpreadClasses),
        "\n\n");
    for i in [1..Size(SpreadClasses)] do
        Print("Class ",i,":\n");
        Print("    Qty:  ", Size(SpreadClasses[i]), "\n");
        Print("    Group: \c");
        spreadgroup := Stabilizer(gammal, SpreadClasses[i][1],OnSetsSets);
        if IsSubgroup(spreadgroup,gammal) then
            Print("Contains GammaL(1,q)\n");
        else
            # Print(StructureDescription(spreadgroup),"\n");
            Print(GammaLSubgroupStructure(F,spreadgroup),"\n");
        fi;
    od;
    return List(SpreadClasses, o-> o[1]);
end;
```

II Searching for polynomials with the line spread condition

```
q := 5;
d := 6;

# get a list of (equivalence classes of) elements b which can be used to make
# the non-desarguesian cyclic line spreads.
CyclicLineSpreadElements := function(q,d)
    local bar, polys, cosets, cosetreps, goodpolys,
```

```
    roots, goodpairs, bclasses, m, K, L, F;
m := d/2;
K := GF(q);;
L := GF(q^2);;
F := GF(q^d);;

# the involutary automorphism "bar"
bar := FrobeniusAutomorphism(L);;

# get a set of all the irreducible polynomials of degree m over L
polys := List(
    Set(List(
        Difference(Set(F),Set(L)), z -> MinimalPolynomial(L,z)
        )),
    P -> P ^ (d / 2 / Degree(P)));;

# make the set of cosets of K* in L*
cosets := Set(List(
        Difference(Set(L),[Zero(L)]),
        l -> Difference(Set(l * Set(K)), [Zero(L)])
    ));

# get one representative from each set
cosetreps := List(cosets, S -> S[1]);;

# get a list of all the polynomials which satisfy the line spread condition
goodpolys := Filtered(
    polys,
    P -> ForAll(
        Combinations(cosetreps,2),
        A -> not ( (A[1]^bar)^m * Value(P,A[1]/A[1]^bar) ) /
             ( (A[2]^bar)^m * Value( P,A[2]/ A[2]^bar) ) in K
        )
```

```
        );;

    # get the roots of all the good polynomials
    roots := List(goodpolys, P -> RootsOfUPol("split",P));;
    roots := Set(List(
        roots,
        R -> Set(List(
                Group(FrobeniusAutomorphism(F)),
                phi -> (R[1])^phi
                ))
        ));

    # put all the b values into their equivalence classes
    goodpairs := Filtered(
            Cartesian(L,L),
            A -> not ((A[1] * A[1]^bar)=(A[2] * A[2]^bar))
            );;

    bclasses := Set(List(
            roots,
            B -> Set(Union(List(
                B,
                b -> Set(List(
                    goodpairs,
                    A -> (A[2]+b*A[1]^bar) / (A[1]+b*A[2]^bar)
                    ))
                )))
            ));;
    return bclasses;
end;
```

Bibliography

[1] Johannes André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.*, 60:156–186, 1954.

[2] Lynn Margaret Batten and Albrecht Beutelspacher. *The theory of finite linear spaces*. Cambridge University Press, Cambridge, 1993. Combinatorics of points and lines.

[3] Anton Betten, Dieter Betten, and Vladimir D. Tonchev. Unitals and codes. *Discrete Math.*, 267(1-3):23–33, 2003. Combinatorics 2000 (Gaeta).

[4] Mauro Biliotti, Vikram Jha, and Norman L. Johnson. *Foundations of translation planes*, volume 243 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 2001.

[5] R. H. Bruck and R. C. Bose. The construction of translation planes from projective spaces. *J. Algebra*, 1:85–102, 1964.

[6] F. Buekenhout. More geometry for Hering's 3^6: SL$(2, 13)$. In *Advances in finite geometries and designs (Chelwood Gate, 1990)*, Oxford Sci. Publ., pages 57–68. Oxford Univ. Press, New York, 1991.

[7] F. Buekenhout, A. Delandtsheer, and J. Doyen. Finite linear spaces with flag-transitive groups. *J. Combin. Theory Ser. A*, 49(2):268–293, 1988.

[8] Francis Buekenhout, Anne Delandtsheer, Jean Doyen, Peter B. Kleidman, Martin W. Liebeck, and Jan Saxl. Linear spaces with flag-transitive automorphism groups. *Geom. Dedicata*, 36(1):89–94, 1990.

[9] P. M. Cohn. *Algebra. Vol. 2*. John Wiley & Sons Ltd., Chichester, second edition, 1989.

[10] D. R. Cox. *Planning of experiments*. A Wiley Publication in Applied Statistics. John Wiley & Sons Inc., New York, 1958.

[11] P. Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

[12] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[13] Keldon Drudge. On the orbits of Singer groups and their subgroups. *Electron. J. Combin.*, 9(1):Research Paper 15, 10 pp. (electronic), 2002.

[14] The GAP Group. GAP — Groups, Algorithms, and Programming, version 4.4.7. 2006. http://www.gap-system.org.

[15] Marshall Hall, Jr. *The theory of groups*. The Macmillan Co., New York, N.Y., 1959.

[16] Christoph Hering. Two new sporadic doubly transitive linear spaces. In *Finite geometries (Winnipeg, Man., 1984)*, volume 103 of *Lecture Notes in Pure and Appl. Math.*, pages 127–129. Dekker, New York, 1985.

[17] D. G. Higman and J. E. McLaughlin. Geometric *ABA*-groups. *Illinois J. Math.*, 5:382–397, 1961.

[18] Cécile Huybrechts. *Réductions des géométries de type $L \cdot L^*$*. PhD thesis, Université Libre de Bruxelles, Faculté des Sciences, 1995-1996.

[19] W. M. Kantor. *Classical groups from a nonclassical viewpoint*. Oxford University Mathematical Institute, Oxford, 1979.

[20] William M. Kantor. Flag-transitive planes. In *Finite geometries (Winnipeg, Man., 1984)*, volume 103 of *Lecture Notes in Pure and Appl. Math.*, pages 179–181. Dekker, New York, 1985.

[21] William M. Kantor. 2-transitive and flag-transitive designs. In *Coding theory, design theory, group theory (Burlington, VT, 1990)*, Wiley-Intersci. Publ., pages 13–30. Wiley, New York, 1993.

[22] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[23] Richard A. Mollin. *Algebraic number theory*. CRC Press Series on Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 1999.

[24] Akihiro Munemasa. Flag-transitive 2-designs arising from line-spreads in PG$(2n-1,2)$. *Geom. Dedicata*, 77(2):209–213, 1999.

[25] Christine O'Keefe. *t-spreads of* PG$((s+1)(t+1)-1,q)$. PhD thesis, University of Adelaide, 1988.

[26] Michael Pauley and John Bamberg. One-dimensional affine flag-transitive linear spaces. In preparation.

[27] Ivano Pinneri. *Flocks, Generalised Quadrangles and Hyperovals*. PhD thesis, The University of Western Australia, 1996.

[28] C. Radhakrishna Rao. Difference sets and combinatorial arrangements derivable from finite geometries. *Proc. Nat. Inst. Sci. India*, 12:123–135, 1946.

[29] Moshe Roitman. On Zsigmondy primes. *Proc. Amer. Math. Soc.*, 125(7):1913–1919, 1997.

[30] Steven Roman. *Coding and information theory*, volume 134 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[31] Jan Saxl. On finite linear spaces with almost simple flag-transitive automorphism groups. *J. Combin. Theory Ser. A*, 100(2):322–348, 2002.

[32] Ralph-Hardo Schulz. Über Blockpläne mit transitiver Dilatationsgruppe. *Math. Z.*, 98:60–82, 1967.

[33] Donald E. Taylor. *The geometry of the classical groups*, volume 9 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, 1992.

[34] Oswald Veblen and John Wesley Young. *Projective geometry. Vol. 1*. Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[35] Guido Zappa. Partitions and other coverings of finite groups. *Illinois J. Math.*, 47(1-2):571–580, 2003. Special issue in honor of Reinhold Baer (1902–1979).

Index