A construction of one-dimensional affine flag-transitive linear spaces

Michael Pauley

School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, W.A. 6014, Australia.

John Bamberg

Department of Pure Mathematics, Ghent University, Galglaan 2, B-9000 Ghent, Belgium.

Abstract

The finite flag-transitive linear spaces which have an insoluble automorphism group were given a precise description in [BDD$^+$90], and their classification has recently been completed (see [Lie98] and [Sax02]). However, the remaining case where the automorphism group is a subgroup of one-dimensional affine transformations has not been classified and bears a variety of known examples. Here we give a construction of new one-dimensional affine flag-transitive linear spaces via the André/Bruck-Bose construction applied to transitive line-spreads of projective space.

Key words: flag-transitive, linear space, 2-design, t-spread
2000 MSC: Primary 05B05, 05B25, 51E20, 12C05

1 Introduction

A linear space $\mathcal{L}$ is an incidence structure of points and lines such that every two points lie on a unique line, every point lies on at least two lines, and every line is incident with at least two points. Furthermore, $\mathcal{L}$ is nondegenerate if it

Email addresses: pauley@maths.uwa.edu.au (Michael Pauley), bamberg@cage.ugent.be (John Bamberg).

[1] We would like to give our appreciation and thanks to Simeon Ball, Anne Delandtsheer, Bill Kantor, Tim Penttila, and Michael Zieve for sharing their wisdom with us.

possesses a quadrangle; i.e., four points, no three collinear. A *flag* of $\mathcal{L}$ is an incident point and line pair.

By a result of Higman and McLaughlin [HM61], any group of automorphisms G acting transitively on the flags of $\mathcal{L}$ must act primitively on the points of $\mathcal{L}$. Moreover, it was shown in [BDD88] by using the O'Nan-Scott Theorem, that G is of affine or almost simple type. In the almost simple case (see [Sax02]), G has socle isomorphic to $\mathrm{PSL}_n(q)$, $\mathrm{PSU}_n(q^2)$, or ${}^2G_2(q)$, from which it can be deduced that the flag-transitive linear spaces of almost simple type are projective spaces, Witt-Bose-Shrikhande spaces, Hermitian unitals, or Ree unitals. In the affine case (see [Lie98]), if G is a subgroup of $\mathrm{A\Gamma L}_d(p)$, where p is a prime and d is at least two, but G is not contained in $\mathrm{A\Gamma L}_1(p^d)$, then the possibilities for $\mathcal{L}$ are the desarguesian affine spaces, the Lüneburg planes, the nearfield planes of order 9, the Hering plane of order 27, or one of two linear spaces constructed by Hering which are not planes [Her85]. The latter are interesting in that they arise by considering a transitive line-spread of the projective space $\mathsf{PG}_5(3)$ (see [Bue91]) and applying a construction of André [And54]. In this paper, we adopt a similar approach to produce new flag-transitive linear spaces via line-spreads of projective space admitting a transitive one-dimensional semilinear group of collineations.

There are many flag-transitive linear spaces of one-dimensional affine type known – translation affine planes, generalised Netto systems, and "inflations" of such examples – however, a full classification seems intractable (c.f., [Kan93, III.C]). Other than the families of examples given by Kantor [Kan93] and Munemasa [Mun99], the authors are not aware of any construction of one-dimensional affine flag-transitive linear spaces, which are not planes, that do not depend on special number theoretic conditions. Here, we present a method of deriving one-dimensional flag transitive linear spaces where the input is a polynomial that induces a permutation of a projective line. Furthermore, in Section 5 we show that our method produces linear spaces for each prime power q. Thus, to the authors' knowledge, there arise infinitely many new flag-transitive linear spaces. Below we paraphrase the main result of the paper, Theorem 1.

Main Theorem

Let q be a prime power. If P is an irreducible polynomial over $\mathsf{GF}(q^2)$ of degree d such that for all nonzero $x, y \in \mathsf{GF}(q^2)$ we have that

$$\frac{x^d P(x^{q-1})}{y^d P(y^{q-1})} \in \mathsf{GF}(q) \text{ implies that } \frac{x}{y} \in \mathsf{GF}(q),$$

then there arises a flag-transitive linear space with a one-dimensional affine automorphism group, and q^{2d} points and q^2 points on each line.

We show in Section 5 that infinitely many such polynomials exist.

2 Background

Let V be the d-dimensional vector space over the finite field of q elements. The projective space $\mathsf{PG}_{d-1}(q)$ is the incidence geometry obtained by defining the points to be the one-dimensional subspaces of V, the lines as the two-dimensional subspaces of V, and incidence as symmetrised inclusion. One can extend the structure of $\mathsf{PG}_{d-1}(q)$ to have *subspaces* (planes, solids, etc) by also considering the vector subspaces of V with dimension more than 2. The projective dimension of a subspace of $\mathsf{PG}_{d-1}(q)$ is one less than the dimension of its preimage in V, and we will use projective dimension whenever we are referring to a subspace of $\mathsf{PG}_{d-1}(q)$.

A *t-spread* of a vector space $V = \mathsf{GF}(q)^d$ is a set of $(t+1)$-dimensional subspaces of V which pairwise intersect trivially and which cover all the vectors of V. Necessarily $t+1$ must divide d for a t-spread to exist. If d is even and $t+1$ is half of d, the t-spread is referred to simply as a *spread*. The construction of André/Bruck-Bose creates a linear space from a t-spread $\mathcal{S}$ of a vector space V as follows: the *points* of our linear space are the elements of V; the *lines* of our linear space are all translates of all elements of $\mathcal{S}$, that is, all sets $S + c$ where $S \in \mathcal{S}$ and $c \in V$. The resulting linear space is a $2-(q^d, q^{t+1}, 1)$ design. The traditional definition of a t-spread is a set of t-dimensional subspaces of the projective space $\mathsf{PG}_{d-1}(q)$ which are disjoint and cover all of the points of the projective space. The above construction of a linear space is given in [BB64] in terms of the traditional definition: $\mathsf{PG}_{d-1}(q)$ is first embedded naturally in $\mathsf{PG}_d(q)$ and then the *points* of the linear space are the points of $\mathsf{PG}_d(q) \backslash \mathsf{PG}_{d-1}(q)$ while the *lines* of the linear space are the t-dimensional subspaces of $\mathsf{PG}_d(q)$ which meet $\mathsf{PG}_{d-1}(q)$ in an element of the spread, with incidence being containment. (Note that [BB64] only concerns itself with spreads, in which case the resulting linear space is an affine plane.) These constructions are equivalent, and in what follows we will use the former definition. Frequently we will treat a field $\mathsf{GF}(q^d)$ as a d-dimensional vector space over a subfield $\mathsf{GF}(q)$, and work with t-spreads of this vector space.

We say that a t-spread $\mathcal{S}$ of $\mathsf{GF}(q)^d$ is *transitive* if the stabiliser of $\mathcal{S}$ in $\Gamma\mathrm{L}_d(q)$ acts transitively on the elements of $\mathcal{S}$. Applying the André/Bruck-Bose construction to a transitive t-spread produces a flag-transitive linear space. A t-spread is *desarguesian* if its corresponding linear space is a desarguesian affine space. We will say that two t-spreads $\mathcal{S}_1$ and $\mathcal{S}_2$ are *equivalent* if the André/Bruck-Bose construction produces isomorphic linear spaces. If there is such an isomorphism, then since the linear spaces are point-transitive, there is an isomorphism which fixes 0. This isomorphism maps $\mathcal{S}_1$ to $\mathcal{S}_2$.

A map f on a vector space V over a field $\mathbb{F}$ is called *semilinear* if there is an automorphism σ of $\mathbb{F}$ such that for all $v, w \in V$ and $\lambda \in \mathbb{F}$ we have $f(v+w) = f(v)+f(w)$ and $f(\lambda v) = \lambda^\sigma f(v)$. Semilinear maps can be written as $v \mapsto Mv^\sigma$ where M is a linear transformation and σ is an automorphism which is applied to each component of v. Moreover, if V is a finite vector space of dimension d over $\mathsf{GF}(q)$, the semilinear transformations form the group $\Gamma\mathrm{L}_d(q)$. Given a field $\mathbb{F}$ and a subfield $\mathbb{K}$, the relative norm $\mathsf{N}_{\mathbb{F}\to\mathbb{K}}$ is the multiplicative function which maps an element $x \in \mathbb{F}$ to the product of its conjugates of $\mathbb{F}$ over $\mathbb{K}$. If $\mathbb{F} = \mathsf{GF}(q^d)$ and $\mathbb{K} = \mathsf{GF}(q)$, we write $\mathsf{N}_{q^d\to q}(x) = x^{1+q+\cdots+q^{d-1}}$ for this map.

By the Classification of Flag-Transitive Linear Spaces [BDD$^+$90], if $\mathcal{L}$ is a flag-transitive linear space obtained via a t-spread $\mathcal{S}$ of projective space then either:

(a) $\mathcal{S}$ is desarguesian;
(b) $\mathcal{S}$ is Hering's spread or one of Hering's two line-spreads of $\mathsf{PG}_5(3)$;
(c) $\mathcal{L}$ has p^d points (where p is a prime) and the collineations stabilising $\mathcal{S}$ form a subgroup of $\Gamma\mathrm{L}_1(p^d)$. Moreover, the automorphism group of $\mathcal{L}$ is contained in $\mathrm{A}\Gamma\mathrm{L}_1(p^d)$.

The "remark on isomorphism testing" in [Kan93] gives us a way of checking for an equivalence of two spreads $\mathcal{S}_1$ and $\mathcal{S}_2$ in $\mathsf{GF}(q^d)$ as a vector space over $\mathsf{GF}(q)$: if ϕ is an isomorphism of the resulting linear spaces $\mathcal{L}_1$ and $\mathcal{L}_2$ (and since these linear spaces are point-transitive we may assume that ϕ maps 0 to 0) then $\phi\mathsf{Aut}(\mathcal{L}_1)\phi^{-1} = \mathsf{Aut}(\mathcal{L}_2)$. Now these automorphism groups have the additive group of $\mathsf{GF}(q^d)$ as their unique minimal normal subgroups, and so ϕ normalises this group. As a result, ϕ is additive on $\mathsf{GF}(q^d)$. Zsigmondy's Theorem [Roi97] tells us that (except in the case $(q, d) = (2, 6)$, and some other cases when $d = 2$ where every t-spread is desarguesian) there exists a prime number s which is a *primitive prime divisor* of $q^d - 1$, that is s divides $q^d - 1$ but not $q^i - 1$ for $i < d$. The number of lines through 0 is divisible by s, and since both automorphism groups are transitive on these lines, they contain Sylow s-subgroups. A property of primitive prime divisors of $q^d - 1$ is that they are coprime to both q and d. The only s-subgroups of $\Gamma\mathrm{L}_1(q^d)$ are in $\mathsf{GF}(q^d)^*$, which is cyclic, and so $\mathsf{Aut}(\mathcal{L}_1)$ and $\mathsf{Aut}(\mathcal{L}_2)$ have the same Sylow s-subgroup. Thus ϕ normalises this group, and by a well known result in representation theory (see for example [Pin96, Theorem 20, p. 7]), ϕ is semilinear. Thus ϕ can be written as $x \mapsto \alpha x^\sigma$ for some field element α and some automorphism σ.

3 A line-spread admitting a transitive cyclic group

For the remainder of this paper, we will assume the following:

(i) a natural tower of fields $\mathsf{GF}(q) \subset \mathsf{GF}(q^2) \subset \mathsf{GF}(q^{2m})$ wherever it arises, with the "bar" map $\bar{\cdot} : x \mapsto x^q$ the unique automorphism of order 2 of $\mathsf{GF}(q^2)$ (we also suppose that $m \geqslant 2$ and $q^{2m} \neq 64$ so that we do not encounter values of q and m for which a certain primitive prime divisor does not exist);

(ii) for an element b of $\mathsf{GF}(q^{2m})$, with $b^{q+1} \neq 1$, we denote by ℓ_b the two-dimensional subspace $\{x - b\bar{x} : x \in \mathsf{GF}(q^2)\}$ of $\mathsf{GF}(q^{2m})$;

(iii) C is the subgroup of nonzero elements z of $\mathsf{GF}(q^{2m})$ satisfying $\mathsf{N}_{q^{2m}\to q^2}(z) \in \mathsf{GF}(q)$. Note that C has order $(q-1)(q^{2m}-1)/(q^2-1)$ and is the cyclic group generated by ω^{q+1}, where ω is a primitive element of $\mathsf{GF}(q^{2m})$.

A *line-spread* is a 1-spread. Note that any line-spread of $\mathsf{GF}(q^{2m})$ admitting a transitive group $G \leqslant \Gamma\mathrm{L}_{2m}(q)$ is equivalent to one of the form ℓ_b^G for some b.

We now state the main theorem of this paper.

Theorem 1 *Let b be an element of $\mathsf{GF}(q^2)$ with $b^{q+1} \neq 1$, let P be the minimal polynomial of b over $\mathsf{GF}(q^2)$, and let d be the degree of P. Then ℓ_b^C is a line-spread of $\mathsf{GF}(q^{2m})$ if and only if for any nonzero $x, y \in \mathsf{GF}(q^2)$ we have that*

$$\frac{x^m P(x^{q-1})^{m/d}}{y^m P(y^{q-1})^{m/d}} \in \mathsf{GF}(q) \text{ implies that } \frac{x}{y} \in \mathsf{GF}(q). \tag{1}$$

Moreover, the following are equivalent:

(i) $b \in \mathsf{GF}(q^2)$;
(ii) ℓ_b^C *is desarguesian;*
(iii) ℓ_b^C *admits a subgroup of* $\mathsf{GF}(q^{2m})^*$ *larger than* C;
(iv) $\ell_b = \ell_c$ *for some* $c \neq b$.

PROOF. Since every element of ℓ_b^C is a $\mathsf{GF}(q)$-subspace of $\mathsf{GF}(q^{2m})$, multiplication by elements of $\mathsf{GF}(q)$ fixes every element of ℓ_b^C. The size of C is $(q^{2m}-1)(q-1)/(q^2-1)$ and the number of nonzero elements of ℓ_b is q^2-1. Thus the set ℓ_b^C will cover all of the nonzero vectors of $\mathsf{GF}(q^{2m})$ provided its elements pairwise intersect in the zero subspace. There are two elements $s_1\ell_b$ and $s_2\ell_b$ of ℓ_b^C with nontrivial intersection if and only if there is $s = s_1/s_2 \in C$ such that $s\ell_b$ and ℓ_b have nontrivial intersection. Such an s exists if and only if there are nonzero x and y in $\mathsf{GF}(q^2)$ such that $s(x - b\bar{x}) = y - b\bar{y}$. This is

true if and only if

$$\mathsf{N}_{q^{2m}\to q^2}\left(\frac{x-b\bar{x}}{y-b\bar{y}}\right)\in\mathsf{GF}(q). \tag{2}$$

Now, by the definition of $\mathsf{N}_{q^{2m}\to q^2}$,

$$\mathsf{N}_{q^{2m}\to q^2}\left(\frac{x-b\bar{x}}{y-b\bar{y}}\right)=\prod_{i=0}^{m-1}\left(\frac{x-b\bar{x}}{y-b\bar{y}}\right)^{q^{2i}}$$

and since $x\to x^{q^{2i}}$ is a field automorphism which fixes elements of $\mathsf{GF}(q^2)$, this is equal to

$$\frac{\prod_{i=0}^{m-1}\left(\bar{x}(x/\bar{x}-b^{q^{2i}})\right)}{\prod_{i=0}^{m-1}\left(\bar{y}(y/\bar{y}-b^{q^{2i}})\right)}.$$

Now since $\prod_{i=0}^{d-1}(x/\bar{x}-b^{q^{2i}})=P(x/\bar{x})$, we see that equation (2) is equivalent to

$$\frac{\bar{x}^m P(x/\bar{x})^{m/d}}{\bar{y}^m P(y/\bar{y})^{m/d}}\in\mathsf{GF}(q).$$

Applying the "bar" map to x and y gives the hypothesis of Condition (1). Therefore, if Condition (1) is true, $s\ell_b$ and ℓ_b can only have nontrivial intersection when $s\in\mathsf{GF}(q)$, and if Condition (1) fails for a particular x and y, there exists $s=(y-b\bar{y})/(x-b\bar{x})\in C$ such that $s\ell_b$ and ℓ_b have nontrivial intersection. So in the projective space $\mathsf{PG}_{2m-1}(q)$, we have that ℓ_b^C induces a line-spread if and only if Condition (1) is satisfied.

(i) $\Longrightarrow$ *(ii):* If $b\in\mathsf{GF}(q^2)$ and ℓ_b is a 2-dimensional $\mathsf{GF}(q)$-subspace of $\mathsf{GF}(q^{2m})$ then $\ell_b=\mathsf{GF}(q^2)$ (incidentally this is true whenever $b\bar{b}\neq 1$.) Thus ℓ_b^C is the set of 1-dimensional $\mathsf{GF}(q^2)$-subspaces of $\mathsf{GF}(q^{2m})$, and the resulting linear space is a desarguesian affine space.

(ii) $\Longrightarrow$ *(iii):* A desarguesian line-spread admits $\mathsf{GF}(q^{2m})^*$.

(iii) $\Longrightarrow$ *(iv):* Suppose ℓ_b^C admits a group $G\leqslant\mathsf{GF}(q^{2m})^*$ and $z\in G\backslash C$. Let K be the kernel of the action of G on ℓ_b^C. Then G/K is an abelian group acting faithfully and transitively on ℓ_b^C and any such group is regular. Thus letting $z'=z^{(q^{2m}-1)/(q^2-1)}=z^{|G/K|}$ we have $z'\in K$, so $z'\ell_b=\ell_b$. Now $z'\ell_b=\{z'x-z'b\bar{x}:x\in\mathsf{GF}(q^2)\}=\{y-(bz'/\overline{z'})\bar{y}:y\in\mathsf{GF}(q^2)\}=\ell_{bz'/\overline{z'}}$. But since $z\notin C$ we have $z'\notin\mathsf{GF}(q)$ and so $bz'/\overline{z'}\neq b$.

(iv) $\Longrightarrow$ *(i):* Suppose $\ell_b=\ell_c$. Then (since any $\mathsf{GF}(q)$-linear map from $\mathsf{GF}(q^2)$ to $\mathsf{GF}(q^2)$ can be written uniquely as $x\mapsto ux-v\bar{x}$) there exist $u,v\in\mathsf{GF}(q^2)$ such that

$$x-c\bar{x}=(ux-v\bar{x})-b\overline{(ux-v\bar{x})}$$

for any $x\in\mathsf{GF}(q^2)$. Matching the coefficients of x in this equation, we have $1=u+b\bar{v}$ and so either $b\in\mathsf{GF}(q^2)$ or $\bar{v}=0$ and $u=1$. But in the latter case matching the coefficients of $\bar{x}$ gives $c=v+b\bar{u}=b$.

□

So in particular, we have by the André/Bruck-Bose construction a flag-transitive linear space with a one-dimensional affine automorphism group with q^{2m} points and q^2 points on each line. The following proposition provides a method for testing equivalence of line-spreads produced by Theorem 1. We will use the fact that a $\mathsf{GF}(q)$-linear map from $\mathsf{GF}(q^2)$ to $\mathsf{GF}(q^2)$ can be written uniquely as $x \mapsto ux - v\bar{x}$, and this map is a bijection if and only if $u\bar{u} \neq v\bar{v}$. We will also use the fact that for a given $c \in \mathsf{GF}(q^{2m})$, and $\sigma \in \mathsf{Aut}(\mathsf{GF}(q^{2m}))$,

$$(\ell_c)^\sigma = \{x^\sigma - c^\sigma \overline{x^\sigma} : x \in \mathsf{GF}(q^2)\} = \{y - c^\sigma \bar{y} : y \in \mathsf{GF}(q^2)\} = \ell_{c^\sigma}.$$

Proposition 2 *Suppose ℓ_b^C and ℓ_c^C are line-spreads in $\mathsf{GF}(q^{2m})$. Then ℓ_b^C and ℓ_c^C are equivalent if and only if*

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

for some $u, v \in \mathsf{GF}(q^2)$ with $u\bar{u} \neq v\bar{v}$ and some $\sigma \in \mathsf{Aut}(\mathsf{GF}(q^{2m}))$.

PROOF. By Kantor's remark on isomorphism testing, ℓ_b^C and ℓ_c^C are equivalent if and only if there is a map $g : x \mapsto \alpha x^\sigma$ which carries ℓ_c^C to ℓ_b^C. Since C acts transitively on ℓ_b^C, we may assume that such a map g maps ℓ_b to ℓ_c. So $\ell_b = g(\ell_c) = \alpha \ell_c^\sigma = \alpha \ell_{c^\sigma}$.

Suppose such a map g exists. Then there is a $\mathsf{GF}(q)$-linear bijection $f : \mathsf{GF}(q^2) \to \mathsf{GF}(q^2)$ such that

$$\alpha(x - c^\sigma \bar{x}) = f(x) - b\overline{f(x)}$$

for all $x \in \mathsf{GF}(q^2)$. Now f can be written uniquely as $x \mapsto ux - v\bar{x}$ for some choice of u and v with $u\bar{u} \neq v\bar{v}$, so

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

for all $x \in \mathsf{GF}(q^2)$. By equating coefficients, we have $\alpha = u + b\bar{v}$ (and so $u + b\bar{v} \neq 0$) and $\alpha c^\sigma = v + b\bar{u}$. Thus $c^\sigma = (v + b\bar{u})/(u + b\bar{v})$.

Now suppose that $c^\sigma = (v + \bar{u}b)/(u + \bar{v}b)$ where $u\bar{u} \neq v\bar{v}$. Then letting $\alpha = (u + \bar{v}b)$ we have

$$\alpha(x - c^\sigma \bar{x}) = (ux - v\bar{x}) - b\overline{(ux - v\bar{x})}$$

and the map $x \mapsto ux - v\bar{x}$ is a bijection. Thus the map $g : x \mapsto \alpha x$ is an equivalence between $\ell_{c^\sigma}^C$ and ℓ_b^C. □

4 Further remarks

4.1 Permutations of the projective line:

Note that if P satisfies Condition (1), then the map

$$x \mapsto x^m P(\bar{x}/x)^{m/d}$$

induces a permutation of the $q+1$ elements of the projective line $\mathsf{GF}(q^2)/\mathsf{GF}(q)$.

4.2 Inflation:

Here we briefly describe Kantor's "inflation trick" as explained in [Kan93] in the context of line-spreads and how it relates to the line-spreads constructed by the theorem above. Suppose ℓ_b^C is a line-spread of $\mathsf{PG}_{2m-1}(q)$, and that m' is a positive integer coprime to $q+1$. By Theorem 1, if P is the minimal polynomial of b and P has degree d, then

$$\frac{x^m P(x^{q-1})^{m/d}}{y^m P(y^{q-1})^{m/d}} \in \mathsf{GF}(q) \text{ implies that } \frac{x}{y} \in \mathsf{GF}(q).$$

Since m' is coprime to $q+1$ we have that

$$\frac{x^{mm'} P(x^{q-1})^{mm'/d}}{y^{mm'} P(y^{q-1})^{mm'/d}} \in \mathsf{GF}(q) \text{ if and only if } \frac{x^m P(x^{q-1})^{m/d}}{y^m P(y^{q-1})^{m/d}} \in \mathsf{GF}(q)$$

and so, with mm' playing the role of m, we can apply Theorem 1 to produce a line-spread of $\mathsf{PG}_{2mm'-1}(q)$.

4.3 A look at one of Kantor's examples:

One of the constructions of t-spreads (for arbitrary t) in [Kan93, construction 4] admits a transitive cyclic group which in the case of $t = 1$, is C above. We can treat this construction in terms of Theorem 1. Let ζ be a generator of $\mathsf{GF}(q^2)$. Also let m be an odd divisor of $q-1$. Then the polynomial

$$P(x) = x^m - \zeta$$

is irreducible and satisfies Condition (1). To see that it is irreducible, let z be a root of P. We will show that z lies in $\mathsf{GF}(q^{2m})$ but no smaller extension of

$\mathsf{GF}(q^2)$. Now $z^m - \zeta = 0$ implies that $z^{q^2-1} = \zeta^{(q^2-1)/m}$ so $z^{q^2} = \zeta^{(q^2-1)/m} z$ and so for any i, using the fact that $x \mapsto x^{q^2}$ is an automorphism, we have

$$z^{q^{2i}} = \zeta^{i(q^2-1)/m} z.$$

Thus $z^{q^{2i}} = z$ if and only if i is a multiple of m. Therefore z lies in $\mathsf{GF}(q^{2m})$ but no smaller extension of $\mathsf{GF}(q^2)$ and so P is irreducible.

Now, to see that P satisfies Condition (1), suppose that

$$\frac{x^m(x^{(q-1)m} - \zeta)}{y^m(y^{(q-1)m} - \zeta)} = k \in \mathsf{GF}(q).$$

Then, rearranging, we have

$$x^{qm} - ky^{qm} = \zeta(x^m - ky^m)$$

and since $k^q = k$, the left hand side of the above equation can be written as $(x^m - ky^m)^q$. If $x^m - ky^m \neq 0$ we have $\zeta = (x^m - ky^m)^{q-1}$ and so ζ is not a generator of $\mathsf{GF}(q^2)$. Thus $x^m - ky^m = 0$, and so $(x/y)^m \in \mathsf{GF}(q)$. Since m is an odd divisor of $q-1$, it is coprime to $q+1$, and so $x/y \in \mathsf{GF}(q)$.

4.4 Kantor's other constructions:

Kantor gives seven types of construction of flag-transitive linear spaces with one-dimensional affine groups in [Kan93]. How do we know when Theorem 1 gives us one of these examples? Type 2 is a special case of Type 7, the inflation trick, and this and Type 4 are discussed in Subsection 4.2 as they relate to Theorem 1. Type 1 describes the generalised Netto systems. The number of points on a line in such a linear space divides $v-1$ where v is the total number of points. But the number of points in the linear space arising from Theorem 1 is q^{2q} and the number of points on a line is q^2. If this linear space were isomorphic to one arising from Theorem 1, then we would have that q^2 divides $q^{2q} - 1$; a contradiction.

Type 3 gives a linear space arising from an $n-1$ spread of $\mathsf{GF}(q^{fn})$ as a vector space over $\mathsf{GF}(q)$, where q, f are powers of a prime p and $n > 1$ such that p does not divide n. The construction assumes $(q^n - 1)/(q-1)$ is coprime to $f-1$. One of the lines of this linear space is the set $L = \mathsf{Ker}\, T + r\mathsf{GF}(q)$ where T is the trace map $\mathsf{GF}(q^n) \to \mathsf{GF}(q)$ and r is an element of $\mathsf{GF}(q^f) \backslash \mathsf{GF}(q)$ satisfying certain conditions. Such a linear space cannot be isomorphic to one arising from Theorem 1. Recall that $\ell_c^\sigma = \ell_{c^\sigma}$, so that if ℓ_c^C is equivalent to a space of Type 3 via the map $g : x \mapsto \alpha x^\sigma$ then $\ell_{c^\sigma}^C$ is equivalent to that space via the map $x \mapsto \alpha x$. We shall prove that $\mathsf{Ker}\ T + r\mathsf{GF}(q)$ is not a 2-dimensional subspace of $\mathsf{GF}(q^{fn})$ over any subfield; since the map $x \mapsto \alpha x$

maps 2-dimensional subspaces to 2-dimensional subspaces, it will follow that a space of Type 3 cannot be constructed by Theorem 1. Firstly, L is not a 2-dimensional subspace over $\mathsf{GF}(q)$, for this would imply that $n = 2$ (as $\mathsf{Ker}\ T$ has dimension $n-1$). Then p is odd, and $q+1 = (q^2-1)/(q-1)$ is coprime to $f-1$. However, this is impossible as $q+1$ and $f-1$ are even. Now we show that L is not a 2-dimensional subspace over $\mathsf{GF}(p^k)$ where $p^k \neq q$ (note then that $q^n = p^{2k}$ and $p^k > q$). Let $z \in \mathsf{GF}(p^k)\backslash\mathsf{GF}(q)$, and so $z \in \mathsf{GF}(q^n)$. If L is closed under multiplication by $\mathsf{GF}(p^k)$, then $zr \in L$ and so $zr = \lambda + \mu r$ where $\lambda \in \mathsf{Ker}\ T$ and $\mu \in \mathsf{GF}(q)$. This implies that $\lambda = r(z-\mu)$ and hence that $\lambda \notin \mathsf{GF}(q^n)$ as $z - \mu \in \mathsf{GF}(q^n)$, $r \in \mathsf{GF}(q^f)\backslash\mathsf{GF}(q)$, and f is coprime to n. However, this is a contradiction since $\mathsf{Ker}\ T \subseteq \mathsf{GF}(q^n)$.

The constructions of Type 5 do not admit a cyclic group acting transitively on the lines through the origin. Since the line-spreads produced by Theorem 1 always give linear spaces with this property, the linear spaces of Type 5 never arise from Theorem 1. Only Type 6 remains, and it is not clear whether these spaces arise from Theorem 1. However, we do know that they contain a line which is equal to one of the lines of Type 4. (This line is $h(\mathsf{GF}(q^2))$ in Kantor's notation, or ℓ_b where b is the root of P given in our discussion of Type 4.) So a linear space of Type 6 can only arise from Theorem 1 (and have a line-spread admitting the group C) if it is also a linear space of Type 4 (which we have treated in Subsection 4.2).

5 Examples

Here we give examples of irreducible polynomials which satisfy Condition (1).

Example 1:

Let p be an odd prime. Then the polynomial

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

is irreducible over $\mathsf{GF}(p)$ and satisfies Condition (1). To see that $P(x)$ is irreducible, we show that a root z of P is in $\mathsf{GF}(p^p)$ but not in any proper subfield of $\mathsf{GF}(p^p)$. First note that $z \neq 1$ since $P(1) = -1$. The only proper subfield of $\mathsf{GF}(p^p)$ is $\mathsf{GF}(p)$, and if $z \in \mathsf{GF}(p)$, then $z^p = z$ and hence $P(z) = \frac{z^2-1}{z-1} - 2 = z - 1$, which is certainly nonzero. It remains to show that z is in

$\mathsf{GF}(p^p)$. Indeed, if z is a root of P, then writing $z^p z$ for z^{p+1} gives

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

and hence $z^p = (2z-1)/z$. It is not difficult to show by induction that for all positive integers i we have

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

So in particular,

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

as required. Now we show that P satisfies Condition (1). Suppose that $x, y \in \mathsf{GF}(p^2)$ and

$$\frac{x^p P(x^{p-1})}{y^p P(y^{p-1})} \in \mathsf{GF}(p).$$

If we can prove that $P(x^{p-1})/P(y^{p-1})$ is an element of $\mathsf{GF}(p)$, then it will follow that $x^p/y^p \in \mathsf{GF}(p)$ and so $x/y \in \mathsf{GF}(p)$. Suppose that $x^{p-1} \neq 1$. Then

$$P(x^{p-1}) = (x^{(p-1)(p+1)} - 1)/(x^{p-1} - 1) - 2 = (1-1)/(x^{p-1} - 1) - 2 = -2.$$

Now suppose $x^{p-1} = 1$. Then

$$P(x^{p-1}) = \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} - 1 = -1.$$

So $P(x^{p-1})$ is either -2 or -1. Similarly $P(y^{p-1})$ is either -2 or -1 and so $P(x^{p-1})/P(y^{p-1}) \in \mathsf{GF}(p)$ as we required.

To show that these linear spaces are not isomorphic to any of Kantor's examples it suffices to compare it to those of Type 4 (see Subsection 4.4). The number of points in this example is p^{2p} and the number of points on a line is p^2 while the number of points in a space of Type 4 is q^{mn} with $n > 1$ and m dividing $q-1$, and the number of points on a line is q^n. An isomorphism would imply $q = p, n = 2$ and $m = p$, in which case p divides $p - 1$; a contradiction.

Example 2:

The following trick is analogous to Kantor's inflation trick, in that it produces a large linear space from a smaller one. We require the following fact, which is part of Theorem 3.35 in [LN97]:

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

We begin with the assumptions laid out at the beginning of Section 3. Suppose that $P(x)$ is an irreducible polynomial satisfying Condition (1) and let e be the order of P. Suppose that t is an integer satisfying:

(i) $t \geqslant 3$;
(ii) t is odd;
(iii) all prime factors of t divide e;
(iv) t is coprime to $(q^m - 1)/e$;
(v) t is coprime to $q + 1$.

Then $P(x^t)$ is an irreducible polynomial satisfying Condition 1.

It is quite straightforward to see this: irreducibility follows from the above lemma. Now suppose that

$$\frac{x^{tm} P(x^{t(q-1)})^{m/d}}{y^{tm} P(y^{t(q-1)})^{m/d}} \in \mathsf{GF}(q).$$

Then since $P(x)$ satisfies condition (1), we have that $x^t/y^t \in \mathsf{GF}(q)$. But since t is coprime to $q + 1$ we have that $x/y \in \mathsf{GF}(q)$.

References

[And54] Johannes André, *Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe*, Math. Z. **60** (1954), 156–186.

[BB64] R. H. Bruck and R. C. Bose, *The construction of translation planes from projective spaces*, J. Algebra **1** (1964), 85–102.

[BDD88] F. Buekenhout, A. Delandtsheer, and J. Doyen, *Finite linear spaces with flag-transitive groups*, J. Combin. Theory Ser. A **49** (1988), no. 2, 268–293.

[BDD+90] 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** (1990), no. 1, 89–94.

[Bue91] F. Buekenhout, *More geometry for Hering's* $3^6 : \mathrm{SL}(2, 13)$, Advances in finite geometries and designs (Chelwood Gate, 1990), Oxford Sci. Publ., Oxford Univ. Press, New York, 1991, pp. 57–68.

[Her85] Christoph Hering, *Two new sporadic doubly transitive linear spaces*, Finite geometries (Winnipeg, Man., 1984), Lecture Notes in Pure and Appl. Math., vol. 103, Dekker, New York, 1985, pp. 127–129.

[HM61] D. G. Higman and J. E. McLaughlin, *Geometric ABA-groups*, Illinois J. Math. **5** (1961), 382–397.

[Kan93] William M. Kantor, 2-*transitive and flag-transitive designs*, Coding theory, design theory, group theory (Burlington, VT, 1990), Wiley-Intersci. Publ., Wiley, New York, 1993, pp. 13–30.

[Lie98] Martin W. Liebeck, *The classification of finite linear spaces with flag-transitive automorphism groups of affine type*, J. Combin. Theory Ser. A **84** (1998), no. 2, 196–235.

[LN97] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn.

[Mun99] Akihiro Munemasa, *Flag-transitive* 2-*designs arising from line-spreads in* $\mathrm{PG}(2n-1,2)$, Geom. Dedicata **77** (1999), no. 2, 209–213.

[Pin96] Ivano Pinneri, *Flocks, generalised quadrangles and hyperovals*, Ph.D. thesis, The University of Western Australia, 1996.

[Roi97] Moshe Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. **125** (1997), no. 7, 1913–1919.

[Sax02] Jan Saxl, *On finite linear spaces with almost simple flag-transitive automorphism groups*, J. Combin. Theory Ser. A **100** (2002), no. 2, 322–348.