Two Cyclic Arrangement Problems In Finite Projective Geometry: Parallelisms And Two-Intersection Sets

Thesis by

Clinton T. White

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2002

(Submitted the 5th of September 2001)

To my parents.

Acknowledgements

I gratefully acknowledge the assistance of my advisor, Richard M. Wilson. In addition to many helpful discussions, I am indebted to him for both his patience and his encouragement as I completed this work.

Part II of this thesis is based on joint work with Bernhard Schmidt. I would like to thank him for granting his permission to include our results.

Abstract

Two arrangement problems in projective geometries over finite fields are studied, each by imposing the condition that solutions be generated by some cyclic automorphism group.

Part I investigates cyclic parallelisms of the lines of $\mathrm{PG}(2n-1,q)$. Properties of a collineation which can act transitively on the spreads of a parallelism are determined, and these are used to show nonexistence of cyclic parallelisms in the cases of $\mathrm{PG}(2n-1,q)$ with $\gcd(2n-1,q-1)>1$ and $\mathrm{PG}(3,q)$ with $q \equiv 0 \pmod 3$. Along with the result first established by Pentilla and Williams that $\mathrm{PG}(3,q)$ admits cyclic (and regular) parallelisms if $q \equiv 2 \pmod 3$, this completes the existence problem in dimension 3. Cyclic regular parallelisms of $\mathrm{PG}(3,q)$ are considered from the point of view of linear transversal mappings, leading to a conjectured classification. Finally, some partial results and open problems relating to cyclic parallelisms in odd dimensions greater than 3 are discussed.

Part II is joint work with B. Schmidt, investigating which subgroups of Singer cycles of $\mathrm{PG}(n-1,q)$ have orbits which are two-intersection sets. This problem is essentially equivalent to investigating which irreducible cyclic codes have at most two non-zero weights. The main results are necessary and sufficient conditions on the parameters for a Singer subgroup orbit to be a two-intersection set. These conditions allow a computer search which revealed two previously known families and eleven sporadic examples, four of which are believed to be new. It is conjectured that there are no further examples.

Contents

List of Tables

Chapter 1 Introduction and Summary

1.1 Overview

The setting for these investigations will be projective geometries over finite fields.

Let $\mathbf{F} = \mathrm{GF}(q)$ be the finite field of order q and let V be an $\mathbf{F}$-vector space of dimension n. The *projective geometry* of V, denoted $\mathrm{PG}(V)$, is the poset whose elements are the proper nontrivial subspaces of V with $U \leq W$ if and only if U is a subspace of W. $\mathrm{PG}(V)$ is ranked poset, where the rank of U is $\dim U - 1$. Sometimes the term dimension will be used in place of rank; every effort will be made to avoid confusion between linear and projective dimensions. Typically, subspaces of rank 0,1,2 are called points, lines, planes, respectively. Hyperplanes are subspaces of rank one less than the rank of A. Given subspaces $U, W \leq V$, $U \vee W$ denotes the subspace of V generated by U and W, while $U \wedge W$ denotes the subspace intersection of U and W.

If $V = W_1 \oplus \cdots \oplus W_k$ then homogeneous coordinates will sometimes be used to specify points of $\mathrm{PG}(V)$. The notation $(x_1 : \cdots : x_k)$ denotes the projective point that is the one-dimensional subspace spanned by the vector $(x_1, \ldots, x_k)$.

The general linear group of V, denoted $\mathrm{GL}(V)$, is the group of nonsingular linear transformations of V. The semilinear group of V, denoted $\Gamma\mathrm{L}(V)$, is the group of invertible semilinear transformations of V. A function $\alpha : V \to V$ is *semilinear* if α is an abelian group homomorphism and there exists $f \in \mathrm{Aut}(\mathbf{F})$ such that $(\lambda\mathbf{x})\alpha = f(\lambda)(\mathbf{x}\alpha)$ for every $\mathbf{x} \in V$ and every $\lambda \in \mathbf{F}$. The projective general linear group and the projective semilinear group, denoted $\mathrm{PGL}(V)$ and $\mathrm{P\Gamma L}(V)$, are the quotients $\mathrm{GL}(V)/Z$ and $\Gamma\mathrm{L}(V)/Z$, where $Z = \{\mathbf{x} \mapsto \lambda\mathbf{x} \mid \lambda \in \mathbf{F}^*\} \cong \mathbf{F}^*$. In geometric terminology, elements of $\mathrm{PGL}(V)$ and $\mathrm{P\Gamma L}(V)$ are called, respectively, *projectivities* and *collineations* of $\mathrm{PG}(V)$. The following result is known as the Fundamental Theorem of Projective Geometry; see [1], [19], for example.

Theorem 1.1. *If* $\dim V \geq 3$, *the automorphism group of the geometry* $\mathrm{PG}(V)$ *is the projective semilinear group* $\mathrm{P\Gamma L}(V)$.

As each of the objects discussed above is determined up to isomorphism by the dimension of the vector space and the order of the field, one may write $X(n,q)$ for $X(V)$, where X is one of $\mathrm{GL}, \Gamma\mathrm{L}, \mathrm{PGL}, \mathrm{P\Gamma L}$; write $\mathrm{PG}(n,q)$ for $\mathrm{PG}(V(n+1,q))$.

Often, $\mathrm{PG}^{(k)}(n,q)$ (or, when there is no ambiguity as to the order of the field, $\Sigma_n^{(k)}$) will be used to denote the set of rank k subspaces of $\mathrm{PG}(n,q)$. The number of k-spaces of $\mathrm{PG}(n,q)$ is given by

$$\frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Two important combinatorial designs obtained from $\mathrm{PG}(n-1,q)$ are the point-line design and the point-hyperplane design. A 2-(v,k,λ) design is a triple $(\mathcal{P},\mathcal{B},\mathcal{I})$, where $\mathcal{P}$ is a set of v points, $\mathcal{B}$ is a set of blocks, and $\mathcal{I}$ is an incident relation on $\mathcal{P}\cup\mathcal{B}$ so that each block is incident with k points and any two points are coincident with exactly λ blocks. A design is called *symmetric* if $|\mathcal{P}| = |\mathcal{B}|$. The points and lines of $\mathrm{PG}(n-1,q)$ form a design with parameters

$$2-\left(\frac{q^n-1}{q-1}, \frac{q^2-1}{q-1}, 1\right).$$

The points and hyperplanes form a symmetric design with parameters

$$2-\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}\right);$$

see [1, 19, 43]. The proof of the following fundamental result on symmetric designs can be found in [43, Theorem 27.1].

Theorem 1.2. *Let* $\mathcal{S}$ *be a symmetric design and let* α *be an automorphism of* $\mathcal{S}$. *Then the type of the cycle decomposition of* α *on the points of* $\mathcal{S}$ *is the same as the type of the cycle decomposition on the blocks of* $\mathcal{S}$.

An important class of automorphisms of $\mathrm{PG}(n,q)$ are the Singer cycles. A gener-

ator of a cyclic group of automorphisms acting regularly on the points of $\mathrm{PG}(n,q)$ is called a *Singer cycle*. By Theorem 1.2, Singer cycles generate groups which also act regularly on the set of hyperplanes. Singer cycles are often useful for combinatorial problems in projective spaces, as will be the case with the problems considered here.

Each of the next two subsections introduces an arrangement problem in finite projective spaces. One may seek solutions to each of these problems by imposing some cyclic automorphism structure on the problem. Section 1.2 summarizes the results of investigations of these problems. A list of some essential notation is included as an appendix at the end of the thesis.

1.1.1 Parallelisms

One of the oldest problems in combinatorial design theory is the famous Kirkman schoolgirl problem: arrange a class of 15 schoolgirls in five rows of three for each of seven days so that any two girls appear in the same row on exactly one day. A solution was known to Kirkman in the mid-nineteenth century. Yet, this problem has given rise to a number of very interesting generalizations. It will appear as a special case of the problem investigated in Part I.

Another scheduling problem to have in mind is that of 1-factorizations of the complete graph K_{2n}. Given a finite set X, the complete graph on X, denoted $K(X)$, consists of a set of *vertices* and *edges*; the vertices of $K(X)$ are the elements of X and the edges are the unordered pairs of elements of X. Incidence is given by inclusion. Write K_n for $K(X)$ if $|X| = n$. Now suppose $|X| = 2n$. A *1-factor* of K_{2n} is a set of n pairwise nonintersecting edges of K_{2n}; that is, a partition of X by 2-subsets. A *1-factorization* of K_{2n} is a partition of the set of edges into 1-factors. K_{2n} consists of $\binom{2n}{2}$ edges; thus, a 1-factorization would contain $(2n-1)$ 1-factors.

It is easy to see that K_{2n} admits 1-factorizations. For a nonzero integer m, $\mathbf{Z}_m$ denotes the cyclic group of integers modulo m. Take $X = \mathbf{Z}_{2n-1} \cup \{\infty\}$. As the edges of a 1-factor F, take the edge $\{0,\infty\}$ and all edges of the form $\{x,-x\}$ for $x \in \mathbf{Z}_{2n-1} \setminus \{0\}$. To obtain the remaining 1-factors of a 1-factorization, take the

translates of F by the elements of $\mathbf{Z}_{2n-1}$, with the convention that ∞ is a fixed point of this action. Below is the example for K_4.

$$\begin{array}{ccc} \{0,\infty\} & \{1,\infty\} & \{2,\infty\} \\ \{1,2\} & \{0,2\} & \{0,1\} \end{array}$$

This construction is actually *cyclic*. The 1-factors of this 1-factorization are permuted in a single cycle by the cyclic automorphism group generated by $x \mapsto x+1$.

It is sometimes interesting to view $\mathrm{PG}(n-1,q)$ as the so-called q-analog of the Boolean lattice on the n-set $\{1,\ldots,n\}$. One is then interested in which combinatorial results for the Boolean lattice have analogs in the projective geometries. From this point of view, edges of K_{2n} would correspond to lines of $\mathrm{PG}(2n-1,q)$. The 1-factorization problem has the following analog.

Two lines of $\mathrm{PG}(n,q)$ are said to be *skew* if there is no point coincident with both lines. A *spread* of $\mathrm{PG}(n,q)$ is a collection S of pairwise skew lines such that each point of $\mathrm{PG}(n,q)$ is incident with a line of S. (In general, one may consider spreads of k-spaces of $\mathrm{PG}(n,q)$, with the obvious definition. However, the only kinds of spreads which will be considered here are spreads consisting of lines, and thus the convention will be that *spread* always refers to spreads of lines. No qualification will be given.) As $\mathrm{PG}(n,q)$ has $(q^{n+1}-1)/(q-1)$ points and each line is incident with $(q^2-1)/(q-1)$ points, it is necessary for the existence of spreads that $(q^2-1)|(q^{n+1}-1)$. This in turn requires that n be odd. It turns out that the condition n odd is sufficient to ensure that spreads exist in $\mathrm{PG}(n,q)$; see [19] for details.

A *parallelism* (also called a *packing*) of $\mathrm{PG}(2n-1,q)$ is a partition of the set of lines into spreads. As $\mathrm{PG}(2n-1,q)$ contains

$$\frac{(q^{2n}-1)(q^{2n-1}-1)}{(q^2-1)(q-1)}$$

lines and spreads consist of $(q^{2n}-1)/(q^2-1)$ lines each, then a parallelism consists of $(q^{2n-1}-1)/(q-1)$ spreads. Note that this number is precisely the number of points on a hyperplane of $\mathrm{PG}(2n-1,q)$.

The existence of parallelisms of $\mathrm{PG}(2n-1,q)$ is a much more difficult problem than was the existence of 1-factorizations of the complete graph. It was not until the early 1970's that $\mathrm{PG}(3,q)$ was shown to admit parallelisms. This result was obtained by Denniston [13] and independently by Beutelspacher [9]. In the same paper, Beutelspacher also proved the existence of parallelisms of $\mathrm{PG}(2^i-1,q)$. However, these results do not answer questions about the existence of parallelisms with certain extra structure.

A parallelism is *cyclic* if there is a collineation acting transitively on its spreads. Considering that the complete graphs K_{2n} admit cyclic 1-factorizations, it would be of interest to determine if the projective spaces $\mathrm{PG}(2n-1,q)$ similarly admit cyclic parallelisms. Secondly, a parallelism of $\mathrm{PG}(3,q)$ is *regular* if it consists entirely of regular spreads. Regular spreads are discussed in some detail in Section 3.2; this use of regular should not be confused with meaning of the term in the context of group actions. Interest in regular spreads stems in part from a construction originally due to M. Walker of a translation plane of order q^4 with kernel $\mathrm{GF}(q)$ from a regular parallelism of $\mathrm{PG}(3,q)$. See [28], [23], and [36] for more on this correspondence.

In [2], Baker constructed a cyclic parallelism of $\mathrm{PG}(2n-1,2)$ for every $n \geq 2$. Denniston [14] claimed that there are no cyclic parallelisms of $\mathrm{PG}(3,3)$ or $\mathrm{PG}(3,4)$. In [15], he finds six inequivalent cyclic parallelisms of $\mathrm{PG}(3,8)$, two of which are regular. In [37], Prince shows that there are no parallelisms of $\mathrm{PG}(3,3)$ such that any two of the constituent spreads are projectively equivalent. In particular, there are no regular parallelisms of $\mathrm{PG}(3,3)$, as any two regular spreads are equivalent. Recently, Prince used a computer search to compile a list of equivalence classes of cyclic parallelisms of $\mathrm{PG}(3,5)$ [38]. There are forty-five of these, two of which are regular. Finally, another recent result was obtained by Pentilla and Williams [36], who construct two inequivalent cyclic regular parallelisms of $\mathrm{PG}(3,q)$ if $q \equiv 2 \pmod 3$.

Currently, almost nothing is known about parallelisms of projective spaces of dimension greater than 3, beyond Baker's and Beutelspacher's results. In particular, there are no known parallelisms of $\mathrm{PG}(5,q)$ with $q > 2$,

1.1.2 Two-intersection sets

An easy counting argument shows that there can be no set of points of $\mathrm{PG}(n-1,q)$ which is met by each hyperplane in the same number of points, except for the set of all points of $\mathrm{PG}(n-1,q)$. A set of points of $\mathrm{PG}(n-1,q)$ is called a *two-intersection set* if each hyperplane meets the set in one of two numbers of points. This is as close as nontrivial point-sets can come to being evenly distributed over the hyperplane sections. Two-intersection sets in the plane have drawn the most interest. There are a number of configurations of points in planes which give two-intersection sections; the following are just a few of the more commonly known.

A *hyperoval* of $\mathrm{PG}(2,q)$, q even, is a set of $q+2$ points met by each line in 0 or 2 points. A *Baer subplane* of $\mathrm{PG}(2,q^2)$ is a set of q^2+q+1 points met by each line in 1 or $(q+1)$ points. These points, together with the lines meeting the set in $q+1$ points, form an embedded $\mathrm{PG}(2,q)$. A *unital* is a set of q^3+1 points of $\mathrm{PG}(2,q^2)$ which, like a Baer subplane, is met by each line in 1 or $(q+1)$ points. Each of these arrangements of points, hyperovals, Baer subplanes, and unitals, have received a great amount of attention from finite geometers.

Consider the example of a hyperoval for a moment. Let $\Sigma = \mathrm{PG}(2,q)$ where $q = 2^e$ and suppose $\mathcal{O}$ is a hyperoval of Σ. Given any point $\mathbf{p} \notin \mathcal{O}$, the nonempty intersections of the lines on $\mathbf{p}$ with the point-set $\mathcal{O}$ give a partition of $\mathcal{O}$ into pairs of points. In this way, each point not in $\mathcal{O}$ determines a 1-factor of the complete graph $K(\mathcal{O})$. Now suppose l is any line of Σ which does not meet $\mathcal{O}$. As each pair of points of $\mathcal{O}$ determines a unique line of Σ, which in turn meets l in a unique point, it follows that every edge of $K(\mathcal{O})$ occurs in a 1-factor determined by a point of l. In this way, each line not meeting $\mathcal{O}$ determines a 1-factorization of $K(\mathcal{O})$. Thus, the plane Σ can be viewed as an extension of the complete graph $K(\mathcal{O})$, for which the additional points and lines correspond to special collections of 1-factors and 1-factorizations of $K(\mathcal{O})$, respectively.

An idea due to Bruck for a possible construction of a projective plane of order $q(q+1)$ is similar to the above, only replacing the complete graph on $q+2$ vertices

with the design of points and lines of $\mathrm{PG}(3,q)$. To extend this design to a projective plane of order $q(q+1)$ requires a very special collection of q^3 parallelisms of $\mathrm{PG}(3,q)$, which will serve as the lines of the new plane which do not meet the points of $\mathrm{PG}(3,q)$. The Bruck-Reyer-Chowla Theorem rules out the possibility of this construction for certain, but not all, values of q. Were it possible, the construction would yield a plane in which $\mathrm{PG}(3,q)$ is embedded as a set of type $(0, q^2+q+1)$; the lines external to the embedded $\mathrm{PG}(3,q)$ would correspond to parallelisms. This idea contains at once both arrangement problems under consideration, parallelisms and two-intersection sets, and for this reason it seems appropriate to mention it here.

Returning to the background discussion of two-intersection sets, one curious fact stands out. Until recently, all known two-intersection sets in planes of odd order, except the trivial examples of a point and a line, occurred in planes whose orders were also squares. Furthermore, the difference of the intersections numbers was the square root of the order of the plane. While it can be shown that the difference of the intersection numbers must divide the order of the plane, it was not clear if it must be the case that the difference was always the square root of the order. Note that in planes of even order, hyperovals provide examples not exhibiting this behavior.

It has long been known that two-intersection sets in $\mathrm{PG}(n-1,q)$ are equivalent to a certain class of codes called projective two-weight codes. A linear code $C \subset \mathrm{GF}(q)^n$ is a *projective code* if its dual $C^{\perp}$, with respect to the usual dot product, has minimum distance at least 3. See the survey of Calderbank and Kantor [12] for a thorough treatment of the correspondence between two-intersection sets, two-weight projective codes, and certain strongly regular graphs.

A coding-theoretic problem that has received a great deal of attention is the problem of determining the weight enumerators of irreducible cyclic codes; see [5, 7, 24, 31], for example. This problem is equivalent to trying to determine the intersection numbers of hyperplanes of $\mathrm{PG}(n-1,q)$ with orbits under a subgroup of a Singer cycle and in general these are very difficult problems. There has been some recent progress, however, in areas relating to two-weight codes and two-intersection sets. Langevin [24] finds several cases of two-weight irreducible cyclic codes (thus giving certain

two-intersection sets as orbits under subgroups of Singer cycles). His proof relies on evaluating certain Gauss sums in this special case. Also, a recent paper of Dover and Batten [4] exhibits, in geometric language, two intersection sets in $\mathrm{PG}(35^3)$ and $\mathrm{PG}(3, 7^3)$ as orbits under subgroups of Singer cycles of index 19 and 37, respectively. These examples are exciting because they occur in planes of odd, nonsquare order.

1.2 Summary of results

In these investigations, the aforementioned arrangement problems, parallelisms and two-intersection sets, are studied by insisting that the solutions arise as orbits of some cyclic group of collineations. Thus, Singer cycles appear in the problems, affording the opportunity to state the problems in terms of some quotient of the multiplicative group of a finite field by a subgroup. Subspaces of projective spaces are linear objects and thus will correspond to certain additive subgroups of finite fields. Each of these problems can thus be restated directly in terms of the interaction between the two group structures, addition and multiplication, of a finite field.

Part I is an investigation of cyclic parallelisms of $\mathrm{PG}(2n-1, q)$. The point of view of Chapter 2 is to study cyclic parallelisms by studying the point and line orbit structure under a collineation which acts transitively on the spreads of a parallelism. It is first shown (Theorem 2.10) that any such collineation must in fact be a projectivity which fixes a point and acts on a hyperplane. Furthermore, all line-orbits under this projectivity have the same length, $(q^{2n-1}-1)/(q-1)$, and any spread of the parallelism is a set of orbit representatives. If $\gcd(2n-1, q-1) > 1$, no element of $\mathrm{PGL}(2n, q)$ has these properties (Lemma 2.9) and thus there are no cyclic parallelisms in this case. This result extends a result of Denniston [14] that $\mathrm{PG}(3, 4)$ admits no cyclic parallelism.

Continuing with the study of the orbit structure of a projectivity with the necessary properties to cyclically permute the spreads of a parallelism leads to a restatement of the cyclic parallelism problem. The problem is cast in terms of a decomposition of the nonzero elements of a finite field in terms of cosets of an additive and a

multiplicative subgroup. In this case it is not difficult to see from this decomposition that there are no cyclic parallelisms of $\mathrm{PG}(3,q)$ if $q \equiv 0 \pmod 3$ (Corollary 2.26 to Theorem 2.25). This extends an earlier result of Denniston [14] which treated only the case $q = 3$. The results of this chapter also complete the existence problem for cyclic parallelisms of $\mathrm{PG}(3,q)$: they exist if and only if $q \equiv 2 \pmod 3$.

Chapter 3 is devoted to the construction and classification of cyclic regular parallelisms of $\mathrm{PG}(3,q)$ if $q \equiv 2 \pmod 3$. The construction is in terms of linear transversal mappings, which are introduced in Section 3.1. A construction of cyclic regular parallelisms was given initially by Pentilla and Williams in [36]. The results of this chapter were discovered independently from their work. The chapter concludes with the conjecture that up to projective equivalence, there are precisely two cyclic regular parallelisms of $\mathrm{PG}(3,q)$ if $q \equiv 2 \pmod 3$. An exhaustive search of linear transversal mappings verifies the conjecture for all such $q \leq 32$.

Part I concludes with a discussion of the cyclic parallelism problem in odd dimensions greater than 3. Two partial solutions are presented, which, however, cannot be merged into a full solution. Some open problems relating to cyclic parallelisms in higher dimensions are discussed, with emphasis on the case of $\mathrm{PG}(5,q)$.

Part II is the result of joint work with B. Schmidt and will appear in slightly different form in [40]. Here, the problem is to understand which subgroups of Singer cycles of $\mathrm{PG}(n-1,q)$ have orbits which are two-intersection sets. The paper [40] is written from the point of view of irreducible cyclic codes; it is an essentially equivalent problem to determine when these codes have at most two weights. Investigations of the weight distribution of irreducible cyclic codes is not a new problem; it has been understood for some time how these weight enumerators are related to certain Gauss sums. The new result offered here is that in order to determine when at most two weights (or hyperplane intersection numbers, in the geometric language) arise, one need not evaluate the relevant Gauss sums. Enough information can be obtained from Stickelberger's result on their prime ideal factorization, together with Parseval's identity.

The main result (Theorem 6.1) is a set of three conditions on the parameters

of a Singer subgroup orbit which are necessary and sufficient for that orbit to be a two intersection set. There are two known families of two-intersection sets arising in this way and a computer search reveals 11 sporadic examples. It is believed that four of these were previously unknown. It is conjectured that there are no further examples and this conjecture is proved in a special case (Theorem 6.12), subject to the generalized Riemann hypothesis.

Part I

Cyclic Parallelisms

Chapter 2 Some Nonexistence Results

A parallelism of $\mathrm{PG}(2n-1,q)$ is called *cyclic* if its stabilizer in $\mathrm{P\Gamma L}(2n,q)$ contains an element α acting transitively on its spreads. The main results of this chapter are the nonexistences of cyclic parallelisms in the following cases:

- $\mathrm{PG}(2n-1,q)$, if $n \geq 2$ and $\gcd(2n-1, q-1) > 1$;
- $\mathrm{PG}(3,q)$, if $q \equiv 0 \pmod 3$.

These results are obtained by analyzing the necessary orbit structure of a collineation α which acts transitively on the spreads of a parallelism. The chapter begins with some basic and most likely well-known facts about Singer cycles, which are then used in the later sections to more carefully describe the orbit structure of α.

2.1 Singer cycles

This section is primarily concerned with collineations of $\mathrm{PG}(n-1,q)$ having large order and, more specifically, with a particular kind of collineation called a Singer cycle. The main result characterizes Singer cycles as projectivities. This result is put to use in the next section to characterize collineations which cyclically permute the spreads of a parallelism.

Lemma 2.1. *Let* $\mathbf{F}$ *be a finite field and let* $\mathbf{K}$ *be a subfield of* $\mathbf{F}$. *If* $A \in \mathrm{GL}(n,\mathbf{F})$ *and its minimal polynomial has degree* d *and coefficients in* $\mathbf{K}$, *then the order of* A *in* $\mathrm{PGL}(n,\mathbf{F})$ *is at most* $(|\mathbf{K}|^d - 1)/(|\mathbf{K}| - 1)$.

Proof. Every power of A is a $\mathbf{K}$-linear combination of $I, A, \ldots, A^{d-1}$. There are at most $(|\mathbf{K}|^d - 1)/(|\mathbf{K}| - 1)$ d-tuples from $\mathbf{K}$, no two of which are $\mathbf{K}^*$ multiples of each other. □

Definition 2.2. For $n \geq 3$, a *Singer cycle* of $\mathrm{PG}(n-1,q)$ is a generator of a cyclic group of collineations which acts regularly on the set of points.

Remark 2.3. As

$$|\mathrm{PG}^{(0)}(n-1,q)| = \frac{q^n-1}{q-1},$$

a Singer cycle has order $(q^n-1)/(q-1)$ in the group $\mathrm{P\Gamma L}(n,q)$. As the points and hyperplanes of $\mathrm{PG}(n-1,q)$ form a symmetric design, then Theorem 1.2 implies that a collineation α is a Singer cycle if and only if $\langle\alpha\rangle$ acts regularly on the set of hyperplanes of $\mathrm{PG}(n-1,q)$.

Example 2.4. Let $\mathbf{L} = \mathrm{GF}(q^n)$ and let $\mathbf{F}$ be the subfield of $\mathbf{L}$ of order q. View $\mathbf{L}$ as an $\mathbf{F}$-vector space. For a primitive element ω of $\mathbf{L}$, let $\sigma \in \mathrm{PGL}(\mathbf{L})$ be determined by the linear map $x \mapsto \omega x$ on $\mathbf{L}$. For $x \in \mathbf{L}^*$, $\omega^i x \in \mathbf{F}x$ if and only if $\omega^i \in \mathbf{F}$. Any such i must be a multiple of $(q^n-1)/(q-1)$ as $\omega^{(q^n-1)/(q-1)}$ generates $\mathbf{F}^*$. Thus, σ permutes the points of $\mathrm{PG}(\mathbf{L})$ in a cycle of length $(q^n-1)/(q-1)$.

It is next shown that, like the above example, all Singer cycles are projectivities. Thus, Singer cycles are represented by linear transformations of the underlying vector space.

Theorem 2.5. *For $n \geq 3$ and q a prime power, Singer cycles of $\mathrm{PG}(n-1,q)$ are projectivities.*

Proof. Let $q = p^m$ with $m \geq 1$ and let $\mathbf{F} = \mathrm{GF}(q)$. $\mathrm{P\Gamma L}(n,q)$ is isomorphic to a semidirect product of $\mathrm{PGL}(n,q)$ by $\mathbf{Z}_m$; $\mathrm{PGL}(n,q)$ is a normal subgroup of $\mathrm{P\Gamma L}(n,q)$ and a complement is $\{\phi^i \mid 0 \leq i < m\}$, where $(x_0,\ldots,x_{n-1})\phi = (x_0^p,\ldots,x_{n-1}^p)$. Given $\alpha \in \mathrm{P\Gamma L}(n,q)$ there exist $A \in \mathrm{GL}(n,q)$ and $0 \leq k < m$ such that α is represented in $\Gamma\mathrm{L}(n,q)$ by $\phi^k A$.

Assume $\alpha \notin \mathrm{PGL}(n,q)$; that is, assume $k > 0$. Note that $A\phi^k = \phi^k A^{(p^k)}$, where $A^{(p)} = (a_{ij}^p)$. In general for $t \geq 1$,

$$\alpha^t = \phi^{kt} A^{(p^{(t-1)k})} \cdots A^{(p^k)} A.$$

Let $d = \gcd(k, m)$ and choose $t = m/d$. Let $\beta = \alpha^t$. As $\phi^{kt} = 1$, then $\beta \in \mathrm{PGL}(n, q)$ and is represented in $\mathrm{GL}(n, q)$ by the matrix $B = A^{(p^{(t-1)k})} \cdots A^{(p^k)} A$. Using the fact that the map $^{(p)}$ is an endomorphism of the ring of square matrices over a field of characteristic p, it follows that

$$B^{(p^k)} = A^{(p^{tk})} A^{(p^{(t-1)k})} \cdots A^{(p^k)} = ABA^{-1}. \tag{2.1}$$

Suppose $f(x) = \sum_i a_i x^i \in \mathbf{F}[x]$. Now $f(B) = \mathbf{0}$ if and only if $f(B)^{(p^k)} = \mathbf{0}$. Furthermore,

$$f(B)^{(p^k)} = \sum_i (a_i B^i)^{(p^k)} = \sum_i a_i^{p^k} \left(B^{(p^k)}\right)^i.$$

Letting $\mu_M(x)$ denote the minimal polynomial of a square matrix M, it follows that $\mu_B(x) = \sum_i a_i x^i$ if and only if $\mu_{B^{(p^k)}}(x) = \sum_i a_i^{p^k} x^i$. That is, a coefficient of $\mu_{B^{(p^k)}}(x)$ is obtained by raising the coefficient of $\mu_B(x)$ of the same degree to the power p^k.

On the other hand, $B^{(p^k)}$ and B have the same minimal polynomials since they are conjugate by equation (2.1). Hence, the coefficients of $\chi_B(x)$ are fixed by the field automorphism $x \mapsto x^{p^k}$. Let $\mathbf{E}$ denote the subfield of $\mathbf{F}$ fixed by this automorphism. Note that $|\mathbf{E}| = p^d$, where $d = (k, m)$. By Lemma 2.1, the order of β in $\mathrm{PGL}(n, \mathbf{F})$ is at most $(p^{nd} - 1)/(p^d - 1)$. Therefore, the order of α in $\mathrm{P\Gamma L}(n, q)$ is at most

$$\frac{m(p^{nd} - 1)}{d(p^d - 1)},$$

which can be shown to be less than $(p^{nm} - 1)/(p^m - 1)$. Therefore, no element of $\mathrm{P\Gamma L}(n, q) \setminus \mathrm{PGL}(n, q)$ is a Singer cycle of $\mathrm{PG}(n - 1, q)$. □

Lemma 2.6. *(i) If $A_1, A_2 \in \mathrm{GL}(n, q)$ have the same order in $\mathrm{GL}(n, q)$ and each represent Singer cycles of $\mathrm{PG}(n - 1, q)$, then A_1 and A_2 generate conjugate subgroups of $\mathrm{GL}(n, q)$.*

(ii) If there exists $A \in \mathrm{GL}(n, q)$ of order $(q^n - 1)/(q - 1)$ in $\mathrm{GL}(n, q)$ which represents a Singer cycle of $\mathrm{PG}(n - 1, q)$, then $(n, q - 1) = 1$.

Proof. By Lemma 2.1, matrices representing Singer cycles of $\mathrm{PG}(n - 1, q)$ have min-

imal polynomials of degree n and hence have irreducible characteristic polynomials. As A_i is conjugate to the companion matrix of its minimal polynomial, it may be assumed without loss of generality that A_i is a companion matrix. Let $\mathbf{L} = \mathrm{GF}(q^n)$ and let $\mathbf{F}$ be the subfield of $\mathbf{L}$ of order q. For $i = 1, 2$, let $\lambda_i \in \mathbf{L}$ be an eigenvalue of A_i. Regarding $\mathbf{L}$ as an $\mathbf{F}$-vector space of dimension n, define $\mu_i \in \mathrm{GL}(\mathbf{L})$ by $x\mu_i = \lambda_i x$. Let $\mathcal{B}_i$ denote the ordered basis $(\lambda_i^j \mid 0 \leq j < n)$ of $\mathbf{L}$. Using the notation $M_X(\alpha)$ to denote the matrix of a linear transformation α with respect to the ordered basis X, one has $M_{\mathcal{B}_i}(\mu_i) = A_i$.

As A_i is conjugate to the diagonal matrix $\Lambda_i = \mathrm{diag}[\lambda_i, \lambda_i^q, \ldots, \lambda_i^{q^{n-1}}]$, it follows that the order of A_i in $\mathrm{GL}(n, q)$ is equal to the order of λ_i in the group $\mathbf{L}^*$. If A_1 and A_2 have the same order, then λ_1 and λ_2 have the same order in $\mathbf{L}^*$. Since $\mathbf{L}^*$ is a cyclic group, it has at most one subgroup of any given order. Thus $\langle \lambda_1 \rangle = \langle \lambda_2 \rangle$ in $\mathbf{L}^*$ and λ_2 is a power of λ_1, so $\langle \mu_1 \rangle = \langle \mu_2 \rangle$. Let C be the matrix representing the change of basis from $\mathcal{B}_1$ to $\mathcal{B}_2$. Then,

$$\langle A_1 \rangle = M_{\mathcal{B}_1}(\langle \mu_1 \rangle) = M_{\mathcal{B}_1}(\langle \mu_2 \rangle) = C^{-1} M_{\mathcal{B}_2}(\langle \mu_2 \rangle) C = C^{-1} \langle A_2 \rangle C.$$

In part *(ii)*, as in part *(i)*, the characteristic polynomial of A is irreducible and A is conjugate to the diagonal matrix $\Lambda = \mathrm{diag}[\lambda, \lambda^q, \ldots, \lambda^{n-1}]$, where λ is an eigenvalue of A in $\mathbf{L}$. Write $\mathrm{ord}(\lambda)$ to denote the order of $\lambda \in \mathbf{F}^*$. As A is conjugate to Λ, the order of A in $\mathrm{GL}(n, q)$ is equal to $\mathrm{ord}(\lambda)$. Also, the order of A in $\mathrm{PGL}(n, q)$ is equal to

$$\min\{k \geq 1 \mid \lambda^k \in \mathbf{F}^*\} = \frac{\mathrm{lcm}(\mathrm{ord}(\lambda), q-1)}{q-1}.$$

Under the assumption that each order is equal to $(q^n - 1)/(q - 1)$, one has

$$\mathrm{lcm}\left(\frac{q^n - 1}{q-1}, q - 1\right) = q^n - 1.$$

Note that

$$\frac{q^n - 1}{q-1} = \sum_{i=0}^{n-1} q^i = n + (q-1)\sum_{i=0}^{n-2}(n-i-1)q^i.$$

Hence,

$$\gcd\left(\frac{q^n-1}{q-1}, q-1\right) = \gcd(n, q-1).$$

Thus, if A has order $(q^n-1)/(q-1)$ in $\mathrm{GL}(n,q)$ and represents a Singer cycle of $\mathrm{PG}(n-1,q)$, then

$$q^n - 1 = \mathrm{lcm}\left(\frac{q^n-1}{q-1}, q-1\right) = \frac{q^n-1}{\gcd(n, q-1)}. \tag{2.2}$$

Equation (2.2) implies that $\gcd(n, q-1) = 1$, which gives statement *(ii)* of the Lemma. □

2.2 Characterization of the automorphism

The topic of this section is the characterization of collineations which act transitively on the spreads of a parallelism of $\mathrm{PG}(2n-1,q)$. It is of course assumed throughout that n is at least 2, and this assumption will not always be repeated in each result.

Recall the adopted convention that the term *parallelism* will always refer to a parallelism of lines. Also recall the notation $\Sigma_n^{(k)}$ used to denote the set of k-dimensional subspaces of the n-dimensional projective space. Finally, let

$$\theta(n,q) = \frac{q^{n+1}-1}{q-1},$$

the number of points of the geometry $\mathrm{PG}(n,q)$. Simply write $\theta(n)$ where there is no ambiguity as to the order of the field.

Definition 2.7. A parallelism P of $\mathrm{PG}(2n-1,q)$ is said to be *cyclic* if there is a collineation acting transitively on the spreads of P.

Lemma 2.8. *If a collineation $\alpha \in \mathrm{P\Gamma L}(2n,q)$ permutes the spreads of a parallelism of $\mathrm{PG}(2n-1,q)$ in a single cycle, then α stabilizes a unique hyperplane and a unique point of $\mathrm{PG}(2n-1,q)$. This point and this hyperplane are not incident. Furthermore, each orbit of lines under α and each orbit of points, aside from the fixed point, has length $\theta(2n-2)$. In particular, α has order $\theta(2n-2)$.*

Proof. Let P be a parallelism whose spreads are cyclically permuted by α; let $S \in P$. As $P = \{S\alpha^i \mid 0 \leq i < \theta(2n-2)\}$ is a partition of $\Sigma^{(1)}_{2n-1}$ and $S\alpha^{\theta(2n-2)} = S$, then S contains a set of orbit representatives of the lines of Σ_{2n-1} under the action of $\langle\alpha\rangle$. Let $l \in S$. As $l\alpha^t \in S$ if and only if $\theta(2n-2)$ divides t, it follows that the length of the orbit of l is divisible by $\theta(2n-2)$. The line l was chosen arbitrarily from S and S contains a set of orbit representatives; therefore, the length of each orbit of lines under α is a multiple of $\theta(2n-2)$.

Now suppose a point $\mathbf{x}$ is not a fixed point of α. Let l be the line determined by $\mathbf{x}$ and $\mathbf{x}\alpha$. Let t_0 denote the length of the orbit of $\mathbf{x}$ under α; similarly, let t_1 denote the length of the orbit of l under α. By definition, the stabilizer of l in the group $\langle\alpha\rangle$ is generated by α^{t_1}. On the other hand, $\mathbf{x}\alpha^{t_0} = \mathbf{x}$ and $(\mathbf{x}\alpha)\alpha^{t_0} = \mathbf{x}\alpha$; hence, $l\alpha^{t_0} = l$. Thus, $\alpha^{t_0} \in \langle\alpha^{t_1}\rangle$ so t_1 divides t_0.

Combining this result with the above fact that $\theta(2n-2)$ divides t_1, it follows that the length of an orbit of points under α is either 1 or else is divisible by $\theta(2n-2)$. As $|\Sigma^{(0)}_{2n-1}| = \theta(2n-1) = 1 + q\theta(2n-2)$, then α must have a fixed point. Then the automorphism α stabilizes some hyperplane by Theorem 1.2. Necessarily this hyperplane is not incident with the fixed point, for else α acts on the pencil of lines incident with both the fixed point and the invariant hyperplane. There are only $\theta(2n-3)$ such lines, contradicting the result that all orbits have length at least $\theta(2n-2)$.

Now let $\mathbf{p}$ and Π denote a fixed point and an invariant hyperplane of $\mathrm{PG}(2n-1,q)$ under the action of α. Since two points determine a line, if there were a second point $\mathbf{p}' \neq \mathbf{p}$ fixed by α then the line $\mathbf{p} \vee \mathbf{p}'$ is fixed by α, a contradiction. So $\mathbf{p}$ is unique. Therefore, Π is unique by Theorem 1.2.

The $\theta(2n-2)$ lines incident with $\mathbf{p}$ are permuted by α; therefore, they form a single orbit. As each line incident with $\mathbf{p}$ meets Π in a unique point, and each point of Π is incident with some line on $\mathbf{p}$, it follows that α has a single orbit of length $\theta(2n-2)$ on the points of Π. That is, α acts as a Singer cycle on Π. Therefore, $\alpha^{\theta(2n-2)}$ fixes every point of Π and hence every line of Π. Combining this with the earlier result that all orbits of lines have length at least $\theta(2n-2)$, it follows that each

orbit of lines in Π has length exactly $\theta(2n-2)$.

Now suppose l is any line of $\mathrm{PG}(2n-1,q)$ which is neither a line of Π nor incident with $\mathbf{p}$. Let $\mathbf{x}$ denote the point of Π which is incident with l. Notice that $l\alpha^{\theta(2n-2)}$ meets Π in the point $\mathbf{x}$, as $\mathbf{x}\alpha^{\theta(2n-2)} = \mathbf{x}$. Furthermore, $l\alpha^{\theta(2n-1)}$ and l are either the same line or else are skew lines, as they belong to the same spread of the parallelism P. Since they have a common point, then it must be that $l\alpha^{\theta(2n-2)} = l$. Hence, every orbit of lines under α has length $\theta(2n-2)$.

It remains to show that orbits of points, other than the fixed point, have length $\theta(2n-2)$. It has already been shown that α has a single orbit of length $\theta(2n-2)$ on the points of Π. Let $\mathbf{x} \neq \mathbf{p}$ be any point not incident with Π. As $\mathbf{x} \neq \mathbf{p}$, it was shown earlier in the proof that the length of the orbit of $\mathbf{x}$ under α is a multiple of $\theta(2n-2)$. Pick any two distinct lines l and m which are incident with $\mathbf{x}$. As $\mathbf{x} = l \wedge m$ it follows that

$$\mathbf{x}\alpha^{\theta(2n-2)} = (l\alpha^{\theta(2n-2)}) \wedge (m\alpha^{\theta(2n-2)}) = l \wedge m = \mathbf{x}.$$

Thus, the orbit of $\mathbf{x}$ has length equal to $\theta(2n-2)$.

Finally, as $\alpha^{\theta(2n-2)}$ fixes each point, α must have order $\theta(2n-2)$. □

Lemma 2.9. *Suppose α is a collineation of $\mathrm{PG}(2n-1,q)$ each of whose orbits of lines has length $\theta(2n-2)$. It then follows that $\gcd(2n-1, q-1) = 1$ and α is a projectivity. Furthermore, if β is another projectivity each of whose orbits of lines has length $\theta(2n-2)$, then $\langle\alpha\rangle$ and $\langle\beta\rangle$ are conjugate in $\mathrm{PGL}(2n,q)$.*

Proof. Let $V = V(2n,q)$ and suppose that the action of $\alpha \in \mathrm{P\Gamma L}(2n,q)$ partitions the set of lines of $\mathrm{PG}(2n,q)$ into orbits of length $\theta(2n-2)$. Arguing as in the proof of Lemma 2.8, it can be shown that α stabilizes a point and a hyperplane of $\mathrm{PG}(2n-1,q)$ and that these subspaces are not incident. Thus, there exist subspaces $U, W \leq V$ with $U \cap W = \{0\}$, $\dim_{\mathbf{F}} U = 1$, $\dim_{\mathbf{F}} W = 2n-1$, $U\alpha = U$, and $W\alpha = W$. That is, α stabilizes the direct sum decomposition $V = U \oplus W$. Again arguing as in the proof of Lemma 2.8, it can be shown that the orbit of α on any point of $\mathrm{PG}(V)$ other than U has length $\theta(2n-2)$. In particular, $\alpha|_W$ is a Singer cycle on the projective plane $\mathrm{PG}(W)$. Thus $\alpha|_W \in \mathrm{PGL}(W)$ by Theorem 2.5. It follows that $\alpha \in \mathrm{PGL}(V)$.

Now choose a representative $\hat{\alpha} \in \mathrm{GL}(V)$ of α such that $\hat{\alpha}|_U$ is the identity map on U. Pick an ordered basis $\mathcal{B}$ of V consisting of a union of bases of U and W. Recall that $M_{\mathcal{B}}(\hat{\alpha})$ denotes the matrix of α with respect to $\mathcal{B}$. Then

$$M_{\mathcal{B}}(\hat{\alpha}) = \left(\begin{array}{c|c} 1 & \\ \hline & \\ & A \end{array}\right),$$

where $A \in \mathrm{GL}(2n-1, q)$. For any vector of the form $\mathbf{x} = (1, x_1, \ldots, x_{2n-1}) \in V(2n, q)$ with some $x_i \neq 0$, note that $\mathbf{x}M_{\mathcal{B}}(\hat{\alpha})^k \in \mathbf{x}\mathbf{F}$ if and only if $(x_1, \ldots, x_{2n-1})A^k = (x_1, \ldots, x_{2n-1})$. It was argued in the previous paragraph that the orbits under $M_{\mathcal{B}}(\hat{\alpha})$ of projective points of the form $(1 : x_1 : \cdots : x_{2n-1})$, with some $x_i \neq 0$, have length $\theta(2n-2)$. Thus, for nonzero vectors $\mathbf{x}' = (x_1, \ldots, x_{2n-1})$, $\mathbf{x}'A^k = \mathbf{x}'$ if and only k is a multiple of $\theta(2n-2)$. Therefore, the matrix A has order $\theta(2n-2)$. Then $(2n-1, q-1) = 1$ by part *(ii)* of Lemma 2.6.

Finally, suppose β is another projectivity of $\mathrm{PG}(V)$ each of whose line-orbits has length $\theta(2n-2)$. As with α, there exists subspaces U', W' of V of dimensions 1 and $2n-1$, respectively, such that β stabilizes the decomposition $V = U' \oplus W'$ and $\beta|_{W'}$ is a Singer cycle of $\mathrm{PG}(W')$. As above, choose a representative $\hat{\beta} \in \mathrm{GL}(V)$ of β such that $\hat{\beta}|_U$ is the identity and choose a basis $\mathcal{B}'$ of V consisting of a union of bases of U' and W'. Then

$$M_{\mathcal{B}'}(\hat{\beta}) = \left(\begin{array}{c|c} 1 & \\ \hline & \\ & B \end{array}\right),$$

where $B \in \mathrm{GL}(2n-1, q)$ has order $\theta(2n-2)$. Now A and B each represent Singer cycles of $\mathrm{PG}(n-1, q)$ and each have order $\theta(n-1)$. By part *(i)* of Lemma 2.6, there exists $C \in \mathrm{GL}(2n-1, q)$ such that $C^{-1}\langle B\rangle C = \langle A\rangle$. Extending C linearly to $V(2n, q)$ by setting $(1, 0, \ldots, 0)C = (1, 0, \ldots, 0)$ results in $C^{-1}\langle M_{\mathcal{B}'}(\hat{\beta})\rangle C = \langle M_{\mathcal{B}}(\hat{\alpha})\rangle$. Note that $M_{\mathcal{B}}(\hat{\beta})$ and $M_{\mathcal{B}'}(\hat{\beta})$ are conjugate via the matrix representing the change of basis from $\mathcal{B}$ to $\mathcal{B}'$. It then follows that $M_{\mathcal{B}}(\hat{\alpha})$ and $M_{\mathcal{B}}(\hat{\alpha})$ generate conjugate subgroups of

$\mathrm{GL}(V)$; hence, $\hat{\alpha}$ and $\hat{\beta}$ generate conjugate subgroups of $\mathrm{GL}(V)$ and α and β generate conjugate subgroups of $\mathrm{PGL}(V)$. □

Theorem 2.10. *There exists a cyclic parallelism P of $\mathrm{PG}(2n-1,q)$ only if there exists a projectivity $\alpha \in \mathrm{PGL}(2n,q)$ each of whose line-orbits has length $\theta(2n-2)$. If P is a cyclic parallelism and α is such a projectivity, then P is projectively equivalent to a parallelism whose spreads are cyclically permuted by α.*

Proof. Suppose $\beta \in \mathrm{P\Gamma L}(2n,q)$ cyclically permutes the spreads of some parallelism $P = \{S\beta^i \mid 0 \leq i < \theta(2n-2)\}$. By Lemma 2.9, each orbit of the lines of $\mathrm{PG}(2n-1,q)$ under β has length $\theta(2n-2)$, giving the first statement of the Theorem.

Suppose α is any collineation of $\mathrm{PG}(2n-1,q)$ each of whose orbits of lines has length $\theta(2n-2)$. By Lemma 2.9, α and β are projectivities and generate conjugate subgroups of $\mathrm{PGL}(2n-1,q)$. Hence, α is conjugate to a generator of $\langle\beta\rangle$, which in turn also cyclically permutes the spreads of P. Without loss of generality, there exists $\gamma \in \mathrm{PGL}(2n-1,q)$ such that $\alpha = \gamma^{-1}\beta\gamma$. Let $P' = P\gamma$, by definition projectively equivalent to P. Note that $P' = \{S\beta^i\gamma \mid 0 \leq i < \theta(2n-2)\}$ and $S\beta^i\gamma = S\gamma\gamma^{-1}\beta^i\gamma = (S\gamma)(\gamma^{-1}\beta\gamma)^i = (S\gamma)\alpha^i$. So $P' = \{S'\alpha^i \mid 0 \leq i < \theta(2n-2)\}$, where $S' = S\gamma$. Hence, P is projectively equivalent to a parallelism, P', whose spreads are cyclically permuted by α. □

Theorem 2.10 generalizes an observation of Denniston that there are no cyclic parallelisms of $\mathrm{PG}(3,4)$. He writes, "There is no cyclic packing of $\mathrm{PG}(3,4)$ because any collineation of period 21 has some line-orbits of length less than 21; and I should expect the same difficulty to arise whenever q^2+q+1 is not a prime," [13]. His observation concerning the orbits of lines under collineations of $\mathrm{PG}(3,4)$ is accurate; however, its accuracy rests not on the fact that 21 is not prime but instead on the more specific fact that 21 is divisible by 3.

Corollary 2.11. *If $\gcd(2n-1,q-1) > 1$ then $\mathrm{PG}(2n-1,q)$ admits no cyclic parallelism.*

2.3 Line orbits vs. point orbits

The rest of this chapter specializes to the problem in three dimensions. The results of the previous section have established that the primary components of a cyclic parallelism of PG$(3,q)$ are a projectivity σ, which partitions the lines into q^2+1 orbits of size q^2+q+1, and a spread consisting of one line representing each of the orbits of σ. Furthermore, given any such projectivity σ, every projective equivalence class of cyclic parallelisms has at least one representative each of whose spreads represent the orbits of σ. This section begins with a presentation of such a projectivity if $q \not\equiv 1 \pmod 3$. The question arises as to whether the existence of this automorphism, which is necessary for the existence of a cyclic parallelism, is also sufficient. It is to be emphasized that this question is equivalent to asking whether there exists a set of pairwise skew representatives of the line-orbits of *this particular* projectivity σ. The approach to this question will be through a more careful study of the interaction between lines and the point-orbits of σ.

With the case $q \equiv 1 \pmod 3$ out of the way, assume for the rest of this chapter that q is a prime power which is not congruent to 1 modulo 3. It was seen in the last section that an automorphism of Σ whose line-orbits all have length q^2+q+1 must have a unique fixed point and a unique invariant plane. The choice of the following coordinates is motivated by the earlier analysis of such automorphisms; these coordinates provide the framework for much of the subsequent discussion of cyclic parallelisms.

Let $\mathbf{F} = \mathrm{GF}(q)$ and let $\mathbf{L}$ be the extension of $\mathbf{F}$ of degree 3. The ambient four-dimensional $\mathbf{F}$-vector space for the three-dimensional projective geometry will be $V = \mathbf{F} \oplus \mathbf{L}$. Let $\omega \in \mathbf{L}$ be a primitive (q^2+q+1)st root of unity and define $\sigma : V \to V$ to be the linear transformation $\sigma : (t,x) \mapsto (t,\omega x)$ for $t \in \mathbf{F}$ and $x \in \mathbf{L}$. Let Π_∞ denote the subspace $\{0\} \oplus \mathbf{L}$. Note that σ fixes the projective point $(1:0)$ and acts on the plane Π_∞.

As a matter of convenience, write N and Tr, without the usual subscripts, to denote the norm and trace functions, respectively, of the extension $\mathbf{L}/\mathbf{F}$. Let $G = \ker \mathrm{N}$. Note

that G is generated by ω. It is straightforward to check that $\mathbf{L}^*$ is the internal direct sum of $\mathbf{F}^*$ and G since $q \not\equiv 1 \pmod 3$. Now pick an element $\xi \in \mathbf{L}$ such that $\mathrm{Tr}(\xi) = 1$ and set $H = \{x \in \mathbf{L} \mid \mathrm{Tr}(\xi x) = 0\}$. That is, $H = \xi^\perp$ with respect to the symmetric bilinear form $(x, y) \mapsto \mathrm{Tr}(xy)$. It is also straightforward to check that the additive group of the field $\mathbf{L}$ is the internal direct sum of $\mathbf{F}$ and H. Note that if $(q, 3) = 1$, then one may choose $\xi = \frac{1}{3}$, in which case $H = \ker \mathrm{Tr}$.

It will be good to give names to the following few lines and point-sets of $\mathrm{PG}(V)$.

$$\begin{aligned} \text{For } x \in H,\ L_x &= (0:1) \vee (1:x); \\ L_\infty &= \{0\} \oplus \ker \mathrm{Tr}; \\ \text{for } \lambda \in \mathbf{F}^*,\ \mathcal{O}_\lambda &= \{(1:y) \mid y \in \lambda G\}; \\ \mathcal{O}_\infty &= \{(0:g) \mid g \in G\}. \end{aligned}$$

Note that $y \in \lambda G$ if and only if $\mathrm{N}(y) = \lambda^3$. Since $(q-1, 3) = 1$ then the map $\lambda \mapsto \lambda^3$ is a permutation of $\mathbf{F}^*$ and the sets $\mathcal{O}_\lambda$ partition the points of the form $(1:y)$, $y \in \mathbf{F}^*$, according to the value of $\mathrm{N}(y)$.

Proposition 2.12. *The q^2+1 lines $\{L_x \mid x \in H\} \cup \{L_\infty\}$ comprise a complete system of representatives for the orbits of σ on the lines of* $\mathrm{PG}(V)$*; each orbit has length q^2+q+1. The singleton $\{(1:0)\}$ together with the sets of points $\mathcal{O}_\lambda$, for $\lambda \in \mathbf{F}^* \cup \{\infty\}$, are the orbits of σ on the points of* $\mathrm{PG}(V)$.

Proof. Since $\sigma^{q^2+q+1} = 1$, then all orbits have length at most q^2+q+1. Recall that $\mathbf{L}^* = \mathbf{F}G$. It follows that the set $\mathcal{O}_\infty$ consists of all the points of Π_∞; σ is transitive on $\mathcal{O}_\infty$ because ω is a generator of G. Therefore, σ is a Singer cycle on Π_∞ and is transitive on its q^2+q+1 lines. The line L_∞ may be taken as a representative of this orbit.

Note that $\mathbf{F} \oplus H$ is a projective plane of $\mathrm{PG}(V)$ which is not incident with the point $(0:1)$. Thus, each of the q^2 lines on $(0:1)$ which are not contained in Π_∞ meets exactly one point of the form $(1:y)$ for $y \in H$. Thus, the lines $\{L_x \mid x \in H\}$ are distinct. They belong to different σ-orbits, and these orbits have length q^2+q+1,

by the previous remark that σ is a Singer cycle on Π_∞.

Finally, the sets $\mathcal{O}_\infty$ are clearly σ-invariant. Again, as ω generates G, σ is transitive on each such set. □

Remark 2.13. The orbit $\mathcal{O}_\infty$ is the point-set of a plane, so lines meet it in 1 or $q+1$ points. In how many points do various lines meet the other nontrivial point-orbits? The answer is simple if $q = 2$. In this case, there are precisely three point orbits: the fixed point $(1:0)$; $\mathcal{O}_\infty$, consisting of the points of the plane Π_∞; and $\mathcal{O}_1$, consisting of the remaining points. The lines meet $\mathcal{O}_1$ in 0, 1, or 2 points: the lines of Π_∞ meet $\mathcal{O}_1$ in zero points; the lines incident with the fixed point meet $\mathcal{O}_1$ in exactly one point; and the remaining lines meet $\mathcal{O}_1$ in exactly two points.

Suppose now that $q > 2$. A set of points of $\mathrm{PG}(3, q)$ with no three collinear is called a *cap*. It is well-known that the maximum size of a cap in $\mathrm{PG}(3, q)$, with $q > 2$, is $q^2 + 1$; such sets are called *ovoids*. Since the orbits $\mathcal{O}_\lambda$ contain $q^2 + q + 1$ points, then they cannot be caps and some line must meet each set in at least three points. What is the maximum number of points of an orbit $\mathcal{O}_\lambda$ which are collinear? This question will be answered shortly.

The data concerning the intersections of lines with point-orbits can be recorded in an array which gives a decomposition of the elements of the field $\mathbf{L}$ with respect to a subgroup of its additive group and a subgroup of its multiplicative group. Define $\Delta : H \times \mathbf{F}^* \to 2^{\mathbf{L}^*}$ by

$$\Delta(x, \lambda) = (x + \mathbf{F}) \cap \lambda G.$$

The set-valued array Δ is somewhat like a double coset decomposition of $\mathbf{L}^*$. However, instead of describing the intersection of the cosets of two subgroups of $\mathbf{L}^*$, Δ describes the intersection of the additive cosets of $\mathbf{F} < \mathbf{L}$ and the multiplicative cosets of $G < \mathbf{L}^*$. Note that $\mathbf{L}/\mathbf{F} \cong H$ and $\mathbf{L}^*/G \cong \mathbf{F}^*$. The relevance of Δ is explained by the following simple observation.

Claim 2.14. *Let $x \in H$, $\lambda \in \mathbf{F}^*$, and $k \in \mathbf{Z}$. The line $L_x\sigma^k$ meets the orbit $\mathcal{O}_\lambda$ in the points $\{(1:y) \mid y \in \omega^k \Delta(x, \lambda)\}$.*

Proof. As $\mathcal{O}_\lambda$ is a σ-orbit, then $L_x\sigma^k \cap \mathcal{O}_\lambda = (L_x \cap \mathcal{O}_\lambda)\sigma^k$ and it suffices to show that the claim holds for $k = 0$. The set of points incident with L_x is

$$\{(1 : x + s) \mid s \in \mathbf{F}\} \cup \{(0 : 1)\}.$$

The result is now immediate from the definition of $\mathcal{O}_\lambda$. □

To complete the correspondence between Δ and the interaction of the line-orbits and point-orbits of σ, the array should be extended by adding another row and column, each indexed by the symbol ∞, say, so that

$$\begin{aligned}\Delta(\infty, \lambda) &= \emptyset \text{ for } \lambda \in \mathbf{F}^*,\\ \Delta(x, \infty) &= \{1\} \text{ for } x \in H,\\ \Delta(\infty, \infty) &= G \cap \ker \mathrm{Tr}.\end{aligned}$$

Now, $L_x\sigma^k$ meets $\mathcal{O}_\infty$ in the single point $(0 : \omega^k)$, for $x \in H$. $L_\infty\sigma^k$ meets $\mathcal{O}_\infty$ in the set $G \cap \big((\ker \mathrm{Tr})\omega^k\big)$.

Let $\pi : \mathbf{L}^* \to G$ be the homomorphism

$$x \mapsto \frac{x}{\mathrm{N}(x)^{\frac{1}{3}}}.$$

Note that $\ker\pi = \mathbf{F}^*$ and $x\pi = x$ for every $x \in G$. Let $\rho : G \to \mathbf{Z}_{q^2+q+1}$ be the isomorphism determined by $\omega \mapsto 1$. Finally, define $\tilde{\Delta}(x, \lambda) := \Delta(x, \lambda)\pi$ and $\bar{\Delta}(x, \lambda) = \Delta(x, \lambda)\pi\rho$.

Remark 2.15. By Claim 2.14, $L_x\sigma^k \cap \mathcal{O}_\lambda = \{(1 : y) \mid y \in \omega^k\Delta(x, \lambda)\}$. Note that

$$\big(\omega^k\Delta(x, \lambda)\big)\pi = \omega^k\big(\Delta(x, \lambda)\pi\big) = \omega^k\tilde{\Delta}(x, \lambda).$$

Therefore, $L_x\sigma^k$ meets the orbit $\mathcal{O}_\lambda$ in the points $\{(1 : y) \mid y \in \lambda\omega^k\tilde{\Delta}(x, \lambda)\}$. The upshot is that the G-translates of a row $\tilde{\Delta}(x, \cdot)$ completely describe the intersections of the $\langle\sigma\rangle$-translates of the line L_x with the point-orbits. The arrays $\tilde{\Delta}$ and $\bar{\Delta}$ completely

describe the incidence of points and lines of PG(V) and the orbit structure of the collineation σ on these sets.

It should be said that moving the cyclic parallelism problem in a sense out of the geometric language and into this table $\bar{\Delta}$ doesn't necessarily make it any easier. However, the table contains all of the necessary data for the problem in a compact form. In fact, it will soon be seen that $\bar{\Delta}$ contains certain redundancies and can be completely specified by an even smaller set of data. This compact description of the problem in terms of special subsets of, and arithmetic in, $\mathbf{Z}_{q^2+q+1}$ is a computer-friendly presentation. Probabilistic searches for solutions, using a method such as simulated annealing, are particularly appropriate with this presentation.

The following examples concern the arrays $\bar{\Delta}$ for $q = 2, 3, 5$. The indices for the rows and columns are not shown, but the last row and last column are those pertaining to L_∞ and $\mathcal{O}_\infty$, respectively. Braces have been omitted from the subsets in the cells of the array. In each case, $\omega = \alpha^{q-1}$, where α is a primitive element of the field $\mathbf{L} = \mathrm{GF}(q^3)$ satisfying the given primitive polynomial. For $q = 2$ and $q = 5$, $\xi = \frac{1}{3}$ and $H = \ker \mathrm{Tr}$. The entries of the tables are subsets of the indicated group G.

Example 2.16. $q = 2$, $\alpha^3 + \alpha + 1 = 0$, $G = \mathbf{Z}_7$. The first column of Table 2.1

0	0
1,3	0
2,6	0
4,5	0
	1,2,4

Table 2.1: $\bar{\Delta}$ for $q = 2$

represents the 7 points of $\mathcal{O}_1$; the second column represents the 7 points of the plane $\mathcal{O}_\infty$. Together they account for 14 of the 15 points of PG$(3, 2)$; the table does not represent the fixed point $(1 : 0)$. The $\mathbf{Z}_7$-translates of the five rows together give the 35 lines of PG$(3, 2)$.

Example 2.17. $q = 3$, $\alpha^3 + \alpha^2 - 1 = 0$, $\xi = \alpha^2$, $G = \mathbf{Z}_{13}$.

0	0	0
1	8,10	0
4,11	3	0
2,5,6		0
9	7,12	0
8,10	1	0
3	4,11	0
	2,5,6	0
7,12	9	0
		0,2,5,6

Table 2.2: $\bar{\Delta}$ for $q = 3$

Example 2.18. $q = 5$, $\alpha^3 + 2\alpha^2 + 1 = 0$, $G = \mathbf{Z}_{31}$. Notice that each column of Table 2.3 contains a subset of size at least 3, as was explained in Remark 2.13. Also note that aside from the orbit $\mathcal{O}_\infty$, no point-orbit is met by any line in more than three points.

Definition 2.19. A collection of subsets $\{S_i \subset \mathcal{G} \mid i \in I\}$ of an abelian group $\mathcal{G}$ is called a *hyperstarter* for $\mathcal{G}$ if, as multisets,

$$(i) \bigcup_{i \in I} S_i = \mathcal{G},$$

$$(ii) \bigcup_{i \in I} \{x - y \mid x \neq y \in S_i\} = \mathcal{G} \setminus \{0\}.$$

The following is a list of some of the properties of the tables Δ and $\tilde{\Delta}$. Analogous statements for $\bar{\Delta}$ are easily obtained by applying the automorphism ρ.

Proposition 2.20. *(i)* $|\Delta(x, \lambda)| \leq 3$ *for all* $(x, \lambda) \in H \times \mathbf{F}^*$.

(ii) The row $\Delta(0, \cdot)$ *contains a total of* q *elements; every other row contains a total of* $q + 1$ *elements.*

(iii) For $\lambda \in \mathbf{F}^*$, *the column* $\tilde{\Delta}(\cdot, \lambda)$ *is a hyperstarter for* G. *Furthermore, for any*

0	0	0	0	0
8, 15		17	21, 20	0
5, 24, 2	16	6		0
	25, 27, 10	18	30	0
26		11, 1, 19	28	0
14, 3		22	29, 4	0
9, 13		23	12, 7	0
	17	21, 20	15, 8	0
16	6		24, 5, 2	0
25, 27, 10	18	30		0
	1, 11, 19	28	26	0
	22	29, 4	3, 14	0
	23	12, 7	13, 9	0
17	21, 20	8, 15		0
6		24, 5, 2	16	0
18	30		27, 25, 10	0
1, 11, 19	28	26		0
22	29, 4	14, 3		0
23	12, 7	9, 13		0
20, 21	8, 15		17	0
	5, 24, 2	16	6	0
30		27, 25, 10	18	0
28	26		11, 1, 19	0
4, 29	14, 3		22	0
7, 12	9, 13		23	0
				2,10,17,19,22,23

Table 2.3: $\bar{\Delta}$ for $q = 5$

$\lambda \neq \mu \in \mathbf{F}^* \cup \{\infty\}$, *it holds that*

$$\bigcup_{x \in H \cup \{\infty\}} \tilde{\Delta}(x, \lambda)\tilde{\Delta}(x, \mu)^{-1} = G,$$

as multisets.

(iv) For $\lambda \in \mathbf{F}^*$, *the column* $\tilde{\Delta}(\cdot, \lambda)$ *is a permutation of the column* $\tilde{\Delta}(\cdot, 1)$. *For* $s \in \mathbf{F}^*$ *and* $x \in G \cap H$, *the row* $\tilde{\Delta}(sx, \cdot)$ *is a permutation of the row* $\tilde{\Delta}(x, \cdot)$.

(v) The image of any row of Δ *under the map* $y \mapsto y^q$ *is again a row of* Δ.

Proof. *(i)* $\Delta(x, \lambda) = \{x + s \mid s \in \mathbf{F},\ x + s \in \lambda G\} = \{x + s \mid s \in \mathbf{F},\ \mathrm{N}(x + s) = \lambda^3\}$.

Note that

$$\begin{aligned} \mathrm{N}(x+s) &= (x+s)(x^q+s)(x^{q^2}+s) \\ &= s^3 + \mathrm{Tr}(x)s^2 + \mathrm{Tr}(x^{q+1})s + \mathrm{N}(x). \end{aligned}$$

So $\mathrm{N}(x+s) = \lambda^3$ if and only if $s \in \mathbf{F}$ is a root of the cubic polynomial

$$t^3 + \mathrm{Tr}(x)t^2 + \mathrm{Tr}(x^{q+1})t + \mathrm{N}(x) - \lambda^3 \in \mathbf{F}[t].$$

(ii) This statement follows from the fact that lines are incident with $q+1$ points. The "missing point" from the row $\Delta(0,\cdot)$ is the fixed point $(1:0)$, the only point of the geometry which is not in one of the orbits $\mathcal{O}_\lambda$, $\lambda \in \mathbf{F}^* \cup \{\infty\}$.

(iii) These statements follow from the fact that the points and lines of $\mathrm{PG}(V)$ form a $2-(\frac{q^4-1}{q-1}, \frac{q^2-1}{q-1}, 1)$ design, together with the fact that the lines of the geometry arise from taking G-translates of the rows of the table Δ.

(iv) For $\lambda \in \mathbf{F}^*$,

$$\Delta(x,\lambda) = (x+\mathbf{F}) \cap (\lambda G) = \lambda\big((\frac{x}{\lambda}+\mathbf{F}) \cap G\big) = \lambda\Delta\big(\frac{x}{\lambda}, 1\big).$$

As $\mathbf{F}^* = \ker\pi$ and $\pi|_G = 1$, it follows that $\tilde{\Delta}(x,\lambda) = \tilde{\Delta}\big(\frac{x}{\lambda}, 1\big)$ for every $x \in H \cup \{\infty\}$.

(v) The Frobenius automorphism of the extension $\mathbf{L}/\mathbf{F}$ acts on the subgroups $\mathbf{F} < \mathbf{L}$ and $G < \mathbf{L}^*$. Thus

$$\Delta(x^q,\lambda) = (x^q+\mathbf{F}) \cap (\lambda G) = \big((x+\mathbf{F}) \cap (\lambda G)\big)^q = \Delta(x,\lambda)^q.$$

Note that $(x\pi)^q = x^q\pi$ to obtain the analogous result for $\tilde{\Delta}$. □

Remark 2.21. The proof of Proposition 2.20 *(iv)* shows that the column $\tilde{\Delta}(\cdot,\lambda)$ is a reordering of the column $\tilde{\Delta}(\cdot,1)$induced by the permutation $x \mapsto \frac{x}{\lambda}$ of $H \cup \{\infty\}$. If λ is a primitive element of $\mathbf{F}$, then this permutation has two fixed points, 0 and ∞, and $q+1$ orbits of length $q-1$. Accordingly, a column with $\lambda \in \mathbf{F}^*$ is a shift of the column with $\lambda = 1$, where the shift is some cyclic shift of the rows with $x \neq 0, \infty$.

That is to say, in some ordering of the elements of H and $\mathbf{F}^*$, the subarray of $\tilde{\Delta}$ on just the rows and columns of $H \setminus \{0\} \times \mathbf{F}^*$ is a $(q-1) \times (q-1)$ block array with blocks of size $(q+1) \times 1$. Furthermore, it can be arranged that the columns (rows) are cyclic shifts of the first column (row). The full array $\tilde{\Delta}$ is obtained by bordering this subarray with the $x = 0$ and $x = \infty$ rows and the $\lambda = \infty$ column.

Take for example the specific case $q = 5$. The array $\bar{\Delta}$ which was presented in Example 2.3 already appears with this cyclic block structure. Indeed, notice that the subarray obtained by deleting the first and last rows and the last column of $\bar{\Delta}$ has the following structure,

A	B	C	D
B	C	D	A
C	D	A	B
D	A	B	C

where A, B, C, and D are 6×1 arrays.

2.4 A line-orbit correspondence

The notation of the previous section is continued. By Theorem 2.10, there exists a cyclic parallelism of PG(V) if and only if there exists a spread of PG(V) which contains one line from each orbit of σ. It has been shown that the array $\tilde{\Delta}$ gives a representation of the points and lines of PG(V) in a format which conveniently describes the orbits under σ as well as the incidence in the geometry. Choosing a collection of line-orbit representatives corresponds to choosing a G-translate of each row of $\tilde{\Delta}$; two such lines are skew in PG(V) if and only if the entries in each column of the corresponding shifted rows of $\tilde{\Delta}$ are disjoint subsets of G. The notion of choosing shifts of the rows of $\tilde{\Delta}$ leads to the following notation.

Given a function $\psi : H \to G$, write $\psi\tilde{\Delta}$ to denote the array which arises by

translating the elements of the row $\tilde{\Delta}(x,\cdot)$ of $\tilde{\Delta}$ by $\psi(x)$; that is,

$$(\psi\tilde{\Delta})(x,\lambda) = \psi(x)\tilde{\Delta}(x,\lambda) \text{ for } x \in H,\ \lambda \in \mathbf{F}^* \cup \{\infty\},$$
$$(\psi\tilde{\Delta})(\infty,\lambda) = \tilde{\Delta}(\infty,\lambda).$$

Similarly, for $\psi : H \to \mathbf{Z}_{q^2+q+1}$, $\psi\bar{\Delta}$ will be used to denote the array arising from additive shifts of the rows of $\bar{\Delta}$ by the elements $\psi(x)$ in the group $\mathbf{Z}_{q^2+q+1}$.

Lemma 2.22. *There exists a cyclic parallelism of* PG(V) *if and only if there exists a function $\psi : H \to G$ such that each column of the array $\psi\tilde{\Delta}$ is a partition of G. An equivalent condition is obtained by replacing G with $\mathbf{Z}_{q^2+q+1}$ and $\tilde{\Delta}$ with $\bar{\Delta}$.*

Proof. Combine Theorem 2.10, Proposition 2.12, and Remark 2.15. □

Example 2.23. $q = 2$. The table $\bar{\Delta}$ appears as Example 2.1. It is not hard in this small case to find ways to shift the rows of the table by elements of $\mathbf{Z}_7$ so that the columns of the resulting array are partitions of $\mathbf{Z}_7$. In fact, Table 2.4 presents the only solutions to this problem which leave the last row of $\bar{\Delta}$ unshifted. It is worth noting

0	0
4,6	3
1,5	6
2,3	5
	1,2,4

0	0
1,6	5
2,5	3
3,4	6
	1,2,4

Table 2.4: Cyclic parallelisms of PG$(3,2)$

that these examples furnish solutions to the original problem of Kirkman. Identify the 15 schoolgirls with the 15 points of PG$(3,2)$. An arrangement of the 15 girls into five rows of three girls each corresponds to a spread of PG$(3,2)$. As any two points of PG$(3,2)$ are incident with a unique line (which is incident with a total of three points), the final condition of the Kirkman problem corresponds to a set of 7 spreads which partition the lines; ie, a parallelism.

It is worth noting that both arrays in Table 2.4 contain the same first and last rows. An examination of Prince's [38] exhaustive list of forty equivalence classes of

cyclic parallelisms of PG(3, 5) reveals that the base spreads of all those examples contain the same pair of lines from the orbit of lines incident with the fixed point and the orbit of lines in the invariant plane. The same can been seen in the six inequivalent examples found by Denniston [15] for PG(3, 8). Theorem 2.25 offers an explanation for this phenomenon.

For convenience, introduce the notation $\check{H} = H \cup \{\infty\}$ and $\check{\mathbf{F}} = \mathbf{F}^* \cup \{\infty\}$. In the following results, all arithmetic takes place in the group $\mathbf{Z}_{q^2+q+1}$.

Lemma 2.24. *For every* $\lambda \in \mathbf{F}^* \cup \{\infty\}$,

$$\sum_{x \in \check{H}} \sum_{u \in \bar{\Delta}(x,\lambda)} u = 0.$$

Proof. By Proposition 2.20 *(iii)*, each column of $\bar{\Delta}$ with $\lambda \in \mathbf{F}^*$ is a partition of $\mathbf{Z}_{q^2+q+1}$. Therefore, summing the elements of such a column amounts to summing the elements of $\mathbf{Z}_{q^2+q+1}$. Since $q^2 + q + 1$ is odd, then

$$\sum_{k=0}^{q^2+q} k \equiv 0 \pmod{q^2+q+1}.$$

Now suppose $\lambda = \infty$. Note that

$$\sum_{x \in \check{H}} \sum_{u \in \bar{\Delta}(x,\infty)} u = \sum_{u \in \bar{\Delta}(\infty,\infty)} u = \sum_{v \in G \cap \ker \mathrm{Tr}} v\rho = \Big(\prod_{v \in G \cap \ker \mathrm{Tr}} v \Big) \rho.$$

Now $v \in G \cap \ker \mathrm{Tr}$ if and only if $\{v, v^q, v^{q^2}\} \subset G \cap \ker \mathrm{Tr}$. Also, $v = v^q$ if and only if $v \in \mathbf{F}$. As $\mathbf{F} \cap G = \{1\}$, it follows that

$$\prod_{v \in G \cap \ker \mathrm{Tr}} v = \prod_{\{v, v^q, v^{q^2}\} \subset G \cap \ker \mathrm{Tr}} v^{1+q+q^2} = 1.$$

The claim follows as $1\rho = 0$. □

Theorem 2.25. *Let* $\psi : H \to \mathbf{Z}_{q^2+q+1}$. *If each column of* $\psi\bar{\Delta}$ *is a partition of* $\mathbf{Z}_{q^2+q+1}$ *then* $\psi(0) = 0$.

Proof. For simplicity, set $\psi(\infty) = 0$; recall that $(\psi\bar{\Delta})(x,\lambda) = \psi(x) + \bar{\Delta}(x,\lambda)$. Assuming that each column of $\psi\bar{\Delta}$ is a partition of $\mathbf{Z}_{q^2+q+1}$, it follows from Lemma 2.24 that

$$0 = \sum_{x\in\check{H}} \sum_{u\in\bar{\Delta}(x,\lambda)} \big(\psi(x) + u\big) \tag{2.3a}$$

$$= \sum_{x\in\check{H}} \psi(x)|\Delta(x,\lambda)| + \sum_{x\in\check{H}} \sum_{u\in\bar{\Delta}(x,\lambda)} u \tag{2.3b}$$

$$= \sum_{x\in\check{H}} \psi(x)|\Delta(x,\lambda)|. \tag{2.3c}$$

Therefore,

$$0 = \sum_{\lambda\in\check{\mathbf{F}}} \sum_{x\in\check{H}} \psi(x)|\Delta(x,\lambda)| \tag{2.4a}$$

$$= \sum_{x\in\check{H}} \psi(x) \sum_{\lambda\in\check{\mathbf{F}}} |\Delta(x,\lambda)|. \tag{2.4b}$$

By Proposition 2.20 *(ii)*,

$$\sum_{\lambda\in\check{\mathbf{F}}} |\Delta(x,\lambda)| = \begin{cases} q & \text{if } x = 0, \\ q+1 & \text{otherwise.} \end{cases} \tag{2.5}$$

Furthermore, substituting $\lambda = \infty$ into equation (2.3) implies

$$\sum_{x\in\check{H}} \psi(x) = 0. \tag{2.6}$$

Therefore,

$$\begin{aligned} 0 &= \sum_{x\in\check{H}}\sum_{\lambda\in\check{\mathbf{F}}}\psi(x)|\Delta(x,\lambda)| && \text{by equation (2.4)},\\ &= q\psi(0) + (q+1)\sum_{x\neq 0}\psi(x) && \text{by equation (2.5)},\\ &= q\psi(0) - (q+1)\psi(0) && \text{by equation (2.6)},\\ &= -\psi(0). \end{aligned}$$

□

Corollary 2.26. *If* $q \equiv 0 \pmod 3$ *then* $\mathrm{PG}(3,q)$ *does not admit a cyclic parallelism.*

Proof. If $q \equiv 0 \pmod 3$ then $\mathbf{F} \subset \ker \mathrm{Tr}$. In particular, $1 \in G \cap \ker \mathrm{Tr}$; hence $0 \in \bar{\Delta}(\infty,\infty)$. Suppose that there exists a cyclic parallelism of $\mathrm{PG}(3,q)$. By Lemma 2.22, there exists $\psi : H \to \mathbf{Z}_{q^2+q+1}$ such that each column of $\psi\bar{\Delta}$ is a partition of $\mathbf{Z}_{q^2+q+1}$. Theorem 2.25 implies that $\psi(0) = 0$. Therefore,

$$(\psi\bar{\Delta})(0,\infty) = \psi(0) + \bar{\Delta}(0,\infty) = \{0\} \subset \bar{\Delta}(\infty,\infty),$$

contradicting the deduction that the column $\bar{\Delta}(\cdot,\infty)$ is a partition of $\mathbf{Z}_{q^2+q+1}$. □

Remark 2.27. In [13], Denniston claimed that an exhaustive search revealed that there are no cyclic parallelisms of $\mathrm{PG}(3,3)$, although he does not give any details of his search. He then makes the interesting remark that there is a design with the parameters of the points and lines of $\mathrm{PG}(3,3)$, that is, an $S(2,4,40)$, which admits a cyclic resolution. He finds reference to this design in a paper of E. H. Moore [33] from the late nineteenth century. Moore specifies the following as the blocks of a spread on the point-set $\mathbf{Z}_{39} \cup \{\infty\}$:

$$\begin{array}{llll} \{0,13,26,\infty\} & \{1,5,8,25\} & \{2,10,11,16\} & \{4,20,22,32\}\\ & \{14,18,21,38\} & \{15,23,24,29\} & \{17,33,35,6\}\\ & \{27,31,34,12\} & \{28,36,37,3\} & \{30,7,9,19\} \end{array}$$

Developed by the group $\mathbf{Z}_{39}$, this spread generates a resolution of an $S(2,4,40)$. Notice that the design automorphism $x \mapsto x+13$ stabilizes the above base spread, fixing one of its blocks and permuting the other nine blocks in three orbits of length 3. Thus, the automorphism $x \mapsto x+1$ cyclically permutes the 13 spreads of a resolution of the design. This automorphism has order 39, fixes one point, is transitive on the remaining 39 points, has one line-orbit of length 13 and three line-orbits of length 39. Contrast this behavior with that found in the geometries. By Lemma 2.8, an automorphism cyclically permuting the spreads of a parallelism of PG$(3,q)$ has order q^2+q+1.

The automorphism $x \mapsto x+3$ has order 13 and also cyclically permutes the spreads of the above resolution. It has a fixed point, three point-orbits of length 13, and ten line-orbits of length 13. Table 2.5 is the decomposition of Moore's design into point-orbits and line-orbits under this automorphism. The three nontrivial point-orbits are $\mathcal{O}_i = 13i + 3\mathbf{Z}_{39}$, $i = 0,1,2$. Each point-orbit is projected onto $3\mathbf{Z}_{39}$ by $x \mapsto 27x$. Under the isomorphism $\mathbf{Z}_{13} \cong 3\mathbf{Z}_{39}$ given by $1 \mapsto 3$, the decomposition is as follows.

$\mathcal{O}_0$	$\mathcal{O}_1$	$\mathcal{O}_2$
0	0	0
	4,9	6,7
	1,12	5,8
	3,10	2,11
6,7		4,9
5,8		1,12
2,11		3,10
4,9	6,7	
1,12	5,8	
3,10	2,11	

Table 2.5: $S(2,4,40)$

Chapter 3 Cyclic Regular Parallelisms

This chapter begins with an overview of a connection between spreads of projective spaces of dimension three and a special class of functions on affine spaces of dimension two, called transversal mappings. The idea to study spreads through these functions is originally due to Ostrom [35]. His interest in spreads stemmed from an interest in studying the associated translation planes and their duals; the transversal mappings provided a means to study the spreads. Here, the use of transversal mappings provides a method for representing spreads which will turn out to be very convenient for purposes searching for cyclic regular parallelisms, as regular spreads correspond to linear transversal mappings.

Using these linear transversal mappings, it is shown that there exists a cyclic regular parallelism of $\mathrm{PG}(3,q)$ if $q \equiv 2 \pmod 3$. A second example is obtained from the first by the application of a polarity of the geometry, and these examples are shown to be inequivalent under $\mathrm{P\Gamma L}(4,q)$. A similar result had been obtained by Pentilla and Williams in [36]. Finally, a computer search for linear transversal mappings which generate cyclic regular parallelisms of $\mathrm{PG}(3,q)$, $q \equiv 2 \pmod 3$, reveals no further inequivalent examples for several small values of q. It is conjectured that the same holds for all $q \equiv 2 \pmod 3$.

3.1 Spreads and transversal mappings

The following definition is a generalization of Ostrom's definition of transversal mappings to vector spaces of arbitrary dimension.

Definition 3.1. Let V be a vector space of dimension n over the field $\mathbf{F}$. A function $f : V \to V$ is called a *transversal mapping* or *transversal function* if for each $\lambda \in \mathbf{F}$ the map $\mathbf{v} \mapsto f(\mathbf{v}) + \lambda\mathbf{v}$ is a permutation of V. Denote the set of transversal mappings of V by $\mathrm{TM}(V)$.

Remark 3.2. Vector space isomorphisms induce bijections of the corresponding sets of transversal mappings. Suppose $\alpha : W \to V$ is an isomorphism of GF(q) vector spaces. Then α induces a bijection $\mathrm{TM}(W) \to \mathrm{TM}(V)$ by $f \mapsto \alpha f \alpha^{-1}$. Indeed, using the linearity of α, one has $\alpha f \alpha^{-1}\mathbf{v} + \lambda\mathbf{v} = \alpha(f(\alpha^{-1}\mathbf{v}) + \lambda\alpha^{-1}\mathbf{v})$. Since α is a bijection, then the latter is a permutation of V if and only if $\mathbf{w} \mapsto f\mathbf{w} + \lambda\mathbf{w}$ is a permutation of W. It is straightforward to check that the map $f \mapsto \alpha f \alpha^{-1}$ is a bijection. Thus, one may refer to $\mathrm{TM}(n, q)$ when $\dim W = n$.

The term *transversal mapping*, due to Ostrom, is derived from the notion of transversals in partial geometries. The particular partial geometry here is the net $\mathcal{N}$ defined to have as points the elements of $V \times V$, where $V = V(n, q)$, and to have as lines the sets $\{(\mathbf{b}, \mathbf{x}) \mid \mathbf{x} \in V\}$, $\{(\mathbf{x}, \lambda\mathbf{x} + \mathbf{b}) \mid \mathbf{x} \in V\}$, for $\lambda \in \mathbf{F}$ and $\mathbf{b} \in V$. Given $f : V \mapsto V$, define the graph of f to be the set of points $\Gamma(f) = \{(\mathbf{x}, f(\mathbf{x})) \mid \mathbf{x} \in V\}$. One can check that $f \in \mathrm{TM}(V)$ if and only if $\Gamma(f)$ meets every line of $\mathcal{N}$ in exactly one point; that is, if and only if $\Gamma(f)$ is a transversal of $\mathcal{N}$. It can also be shown that any transversal of $\mathcal{N}$ is the graph of a transversal mapping of V.

It is worth noting that the definition of transversal mapping is similar to those of orthomorphism and complete mapping. Given a group G, a permutation $f : G \to G$ is called an *orthomorphism* of G if the function $x \mapsto x^{-1}f(x)$ is also a permutation (where the group operation is written multiplicatively). A permutation f is called a *complete mapping* if the function $x \mapsto xf(x)$ is a permutation. Let $G = V(n, q)$ and $f : V \to V$ such that $x \mapsto f(x) + \lambda x$ is a permutation of V for every $\lambda \in \Omega \subset \mathbf{F}$. Then f is an orthomorphism if $\{0, -1\} \subseteq \Omega$ and f is a complete mapping if $\{0, 1\} \subseteq \Omega$. Notice that all three concepts coincide if $q = 2$. In general, transversal mappings are orthomorphisms as well as complete mappings, but not conversely. Orthomorphisms arise in the constructions of, among others, triple systems, Mendelsohn designs, Room squares, and group sequencings. See [16] for some background and a survey of many results on orthomorphisms and complete mappings.

Example 3.3. *Transversal mappings with* $q = n = 2$. In this case, transversal mappings, orthomorphisms, and complete mappings are the same. It is simple to

check that there are precisely two transversal mappings of GF(4) sending 0 to 0; they are listed in the following table. The elements of GF(4) are denoted by $0, 1, \omega, \omega^2$ where $\omega^2 + \omega + 1 = 0$.

x	0	1	ω	ω^2
$f_1(x)$	0	ω	ω^2	1
$f_2(x)$	0	ω^2	1	ω

Example 3.4. Let $\mathbf{L}$ be a field extension of $\mathbf{F} = \mathrm{GF}(q)$. For any $\tau \in \mathbf{L} \setminus \mathbf{F}$, the function $f(x) = \tau x$ is a transversal mapping of $\mathbf{L}$ as a vector space over $\mathbf{F}$. Notice that the functions in the previous example are both of this form. Indeed, $f_1(x) = \omega x$ and $f_2(x) = \omega^2 x$.

Of greatest interest in this chapter will be transversal mappings of two-dimensional vector spaces, as these are closely connected to spreads of three-dimensional projective spaces. In order to make this clear, recall some notation introduced in the previous chapter. Let q be a prime power. Let $\mathbf{F} = \mathrm{GF}(q)$ and let $\mathbf{L}$ be the extension of $\mathbf{F}$ of degree 3. The ambient vector space is $V = \mathbf{F} \oplus \mathbf{L}$; let Σ denote the geometry $\mathrm{PG}(V)$. Pick an element $\xi \in \mathbf{L}$ such that $\mathrm{Tr}(\xi) = 1$ and set $H = \{x \in \mathbf{L} \mid \mathrm{Tr}(\xi x) = 0\}$.

It will be particularly useful to distinguish a certain collection of planes of Σ. Let

$$\Pi_\infty = \{(0, x) \mid x \in L\};$$
$$\Pi_\lambda = \{(t, x) \mid \mathrm{Tr}(\xi x) = \lambda t\}, \text{ for } \lambda \in \mathbf{F}.$$

Note that these $q+1$ planes are incident with a common line $\{(0, x) \mid x \in H\}$, which will be denoted by l_∞. Furthermore, each point of Π_∞ is represented by a unique vector of the form $(0, x+1)$, with $x \in H$. Indeed, given $y \in \mathbf{L} \setminus H$, let

$$x = \frac{y}{\mathrm{Tr}(\xi y)} - 1.$$

Then $x \in H$ and $(0 : x+1) = (0 : \frac{y}{\mathrm{Tr}(\xi y)}) = (0 : y)$, so at least one such representation always exists. On the other hand, if $(0 : x+1) = (0 : x'+1)$ with $x, x' \in H$, then $x = sx'$ for some $s \in \mathbf{F}^*$. Apply $\mathrm{Tr}(\xi \cdot)$ to the latter equation to obtain $1 = s$, hence

$x = x'$. In a similar manner, it may be shown that each point of $\Pi_0 \setminus l_\infty$ is represented by a unique vector of the form $(1, x)$ with $x \in H$.

The first lemma of this section establishes the equivalence between spreads which contain the line l_∞ and transversal mappings of H. The result is due to Ostrom, [35]. For the convenience of the reader, a short proof is included here in the notation of this work.

Proposition 3.5. *There is a one-to-one correspondence between the set of spreads of* Σ *which contain the line* l_∞ *and the set* $\mathrm{TM}(H)$.

Proof. Given $f : H \to H$, define $\mathcal{S}(f) = \{l_f(x) \mid x \in H\} \cup \{l_\infty\}$ where $l_f(x)$ is the projective line $(0 : x + 1) \vee (1 : f(x))$. As $(0 : x + 1) \neq (0 : y)$ for any $x, y \in H$, then $l_f(x)$ and l_∞ are skew for every $x \in H$. Now suppose $x, y \in H$ and $x \neq y$. As every point of $\Pi_\infty \setminus l_\infty$ is represented by a unique vector of the form $(0, z + 1)$ with $z \in H$, then $l_f(x)$ and $l_f(y)$ do not intersect in a point of Π_∞. Furthermore, the set of planes $\{\Pi_\lambda \mid \lambda \in \mathbf{F}\}$ partitions the complement of Π_∞ in Σ. Thus, $l_f(x)$ and $l_f(y)$ intersect only if they intersect in some point on a plane Π_λ. The line $l_f(x)$ meets the plane Π_λ in the point $(1 : f(x) + \lambda x + \lambda)$. If $l_f(x)$ intersects $l_f(y)$ at the plane Π_λ, it follows that $f(x) + \lambda x = f(y) + \lambda y$. Thus, if $f \in \mathrm{TM}(H)$, then $l_f(x)$ and $l_f(y)$ are skew. Therefore, $\mathcal{S}(f)$ is a set of $q^2 + 1$ pairwise skew lines and hence is a spread of Σ containing l_∞.

It is straightforward to see that the map $f \mapsto \mathcal{S}(f)$ is injective. To check surjectivity, let S be any spread of Σ and suppose $l_\infty \in S$. Recall that each point of $\Pi_\infty \setminus l_\infty$ is represented by a unique vector of the form $(0, x + 1)$, $x \in H$, and each point of $\Pi_0 \setminus l_\infty$ is represented by a unique vector of the form $(1, y)$, $y \in H$. Furthermore, each point of $\Sigma \setminus l_\infty$ is incident with a unique line of $S \setminus \{l_\infty\}$. Now define a map $f : H \to H$ by $f(x) = y$ if there is a line of S which is incident with the points $(0 : x + 1)$ and $(1 : y)$. That f is well defined follows from the comments immediately above. Since S is a spread, it follows as in the previous paragraph that $f \in \mathrm{TM}(H)$ and it is straightforward to check that $S = \mathcal{S}(f)$. Therefore, $\mathcal{S}$ is a bijection. □

It would be very desirable to count the number of spreads of $\mathrm{PG}(3, q)$. This is

currently an open problem and believed to be quite difficult. A corollary of Proposition 3.5 is that counting spreads is equivalent to counting transversal mappings. Let $\eta(q)$ denote the number of spreads of $\mathrm{PG}(3,q)$. As $\mathrm{P\Gamma L}(4,q)$ is transitive on $\Sigma_3^{(1)}$ and maps spreads to spreads, it follows that the number of spreads containing a specific line does not depend on the choice of this line. Denote by $\eta'(q)$ the number of spreads containing a certain distinguished line.

Corollary 3.6. $\eta(q) = (q^2+q+1)|TM(2,q)|$.

Proof. In two ways, count the number of ordered pairs (l,S), where S is a spread containing the line l. One obtains

$$\eta(q)(q^2+1) = |\Sigma_3^{(1)}|\eta'(q).$$

Note that $|\Sigma_3^{(1)}| = (q^2+1)(q^2+q+1)$, and $\eta'(q) = |TM(2,q)|$ by Proposition 3.5. The desired result now follows by substitution. □

The next lemma concerns some groups acting on $\mathrm{TM}(n,q)$; the simple proof is omitted.

Lemma 3.7. *The set* $\mathrm{TM}(n,q)$ *is invariant under the following transformations:*

(i) $f \mapsto f + \mu\mathbf{1}$, *where* $\mu \in \mathbf{F}$ *and* $\mathbf{1}$ *is the identity on* $V(n,q)$;

(ii) $f \mapsto \lambda f + \mathbf{c}$, *where* $\lambda \in \mathbf{F}^*$ *and* $\mathbf{c} \in V(n,q)$;

(iii) $f \mapsto \alpha^{-1} f \alpha$, *where* α *is a permutation of* $V(n,q)$.

Remark 3.8. For the purposes of counting transversal maps, it suffices, in light of Lemma 3.7 *(ii)*, to count the number of $f \in \mathrm{TM}(n,q)$ for which $f(0) = 0$. In Example 3.3 it is remarked that there are exactly two transversal maps of $V(2,2)$ fixing 0. Thus, there are a total of 8 transversal maps of $V(2,2)$, leading to the well known result that there are 56 spreads of $\mathrm{PG}(3,2)$.

To close this section, some further basic results on transversal mappings are presented. While the number of transversal mappings of $V(2,q)$ is unknown and probably very difficult to determine, the same cannot be said for the number of *linear* transversal mappings, which is given by the first of these results.

Proposition 3.9. *There are* $\frac{1}{2}q^2(q-1)^2$ *linear transversal mappings of* $V(2,q)$.

Proof. A linear transversal mapping is an endomorphism of $V = V(2,q)$ having no eigenvalues in GF(q). Thus, it suffices to count the number of linear transformations $\alpha : V \to V$ which do have eigenvalues in GF(q). There are three mutually exclusive and exhaustive cases: (i) α has two distinct eigenvalues in GF(q); (ii) α has one eigenvalue in GF(q) of algebraic and geometric multiplicity 2; (iii) α has one eigenvalue in GF(q) of algebraic multiplicity 2 and geometric multiplicity 1. One can check that the number of invertible α in each of these cases is as follows: (i) $\frac{1}{2}q(q^2-1)(q-2)$; (ii) $q-1$; (iii) $(q^2-1)(q-1)$. The result follows by subtracting these totals from $q(q^2-1)(q-1) = |\mathrm{GL}(2,q)|$. □

The final result concerns the representation of transversal maps as polynomials. Let $\mathbf{F} = \mathrm{GF}(q)$. For any function $\phi : \mathbf{F} \to \mathbf{F}$ there is a polynomial $f(X) \in \mathbf{F}[X]$ of degree at most $q-1$ for which $f(x) = \phi(x)$ for every $x \in \mathbf{F}$. If f is in fact a permutation polynomial, then $\deg f \leq q-2$ by Hermite's Criterion [25]. It was shown by Niederreiter and Robinson [34] that orthomorphisms of $\mathbf{F}$ have degree at most $q-3$ in the case q is odd. The proof is also based on Hermite's Criterion. The same result for q even is due to Wan [44]. Proofs of each case may also be found in [16]. Wan's proof is easily modified to prove the following more general result.

Proposition 3.10. *Let* $\mathbf{F} = \mathrm{GF}(q)$. *Let* $f(x) \in \mathbf{F}[x]$ *have degree less than* q *and suppose that* $f(x)+\theta x$ *is a permutation polynomial for every* θ *in some subset* $\Theta \subseteq \mathbf{F}$. *Then* $\deg f < q - |\Theta|$.

Proof. Let $q = p^d$ where p is prime. Let $1 \leq m \leq |\Theta|$ and suppose $p^e || m$, where $0 \leq e \leq d$. It will be shown that the coefficient of the term of $f(x)$ of degree $q-m$ is zero.

Let $\mathcal{O}$ be the ring of algebraic integers of some number field such that $\mathcal{O}/p\mathcal{O} \cong \mathbf{F}$. Let $\pi : \mathcal{O} \to \mathbf{F}$ be the canonical surjective homomorphism and extend π to a homomorphism of polynomial rings $\mathcal{O}[x] \to \mathbf{F}[x]$ by $\pi(x) = x$. Let ω be a primitive element of $\mathbf{F}$ and choose $\alpha \in \mathcal{O}$ such that $\pi(\alpha) = \omega$. Note that $\alpha^{q-1} \equiv 1 \mod p\mathcal{O}$. If $\alpha^{q-1} = 1 + \mu p^i$ for some $\mu \in \mathcal{O}$ and some $1 \leq i \leq e$, then

$$(\alpha^q)^{q-1} = (1+\mu p^i)^q = 1 + \sum_{j=1}^{q} \binom{q}{j} \mu^j p^{ij} \equiv 1 \mod p^{2i}\mathcal{O},$$

as $q \geq p^i$. Since $\pi(\alpha^q) = \omega^q = \omega$, then without loss of generality it may be assumed that $\alpha^{q-1} \equiv 1 \mod p^{e+1}\mathcal{O}$.

Let $S = \{\alpha^i \mid i = 1, \ldots, q-1\} \cup \{0\}$. Suppose $\psi : \mathbf{F} \to \mathbf{F}$ is a permutation polynomial and $\Psi : \mathcal{O} \to \mathcal{O}$ is any polynomial with coefficients in $\mathcal{O}$ such that $\pi(\Psi(x)) = \psi(x)$. Note that $\{\pi(s) \mid s \in S\} = \{\pi(\Psi(s)) \mid s \in S\}$. Thus,

$$\sum_{s \in S} \Psi(s)^m = \sum_{s \in S} (s + p\mu(s))^m,$$

for some $\mu : S \to \mathcal{O}$. Furthermore, $(s + p\mu(s))^m \equiv s^m \mod p^{e+1}\mathcal{O}$. Thus,

$$\begin{aligned}
\sum_{s \in S} \Psi(s)^m &\equiv \sum_{s \in S} s^m && \text{(3.1a)} \\
&\equiv \sum_{i=1}^{q-1} \alpha^{im} && \text{(3.1b)} \\
&\equiv \frac{\alpha^m(\alpha^{(q-1)m} - 1)}{\alpha^m - 1} && \text{(3.1c)} \\
&\equiv 0 \mod p^{e+1}\mathcal{O}. && \text{(3.1d)}
\end{aligned}$$

Now suppose $f \in \mathbf{F}[x]$ is a polynomial of degree less than q such that $f(x) + \theta x$ is a permutation polynomial for every $\theta \in \Theta \subseteq \mathbf{F}$. Without loss of generality, assume $0 \in \Theta$. Let $F(x) \in \mathcal{O}[x]$ such that $\pi(F(x)) = f(x)$ and let $T = \{t \in S \mid \pi(t) \in \Theta\}$.

It follows from equation (3.1) that

$$\sum_{s\in S}(F(s)+ts)^m \equiv 0 \mod p^{e+1}\mathcal{O}$$

for every $t \in T$. Note that

$$(F(s)+ts)^m = t^m s^m + F(s)^m + \sum_{i=1}^{m-1}\binom{m}{i}t^i s^i F(s)^{m-i}.$$

Since

$$\sum_{s\in S} s^m \equiv \sum_{s\in S} F(s)^m \equiv 0 \mod p^{e+1}\mathcal{O}$$

and p^e divides $\binom{m}{i}$ in $\mathbf{Z}$ for $1 \leq i \leq m-1$, then

$$\sum_{s\in S}\sum_{i=1}^{m-1} p^{-e}\binom{m}{i}t^i s^i F(s)^{m-i} \equiv 0 \mod p\mathcal{O}.$$

As $s^q \equiv s \mod p\mathcal{O}$ for all $s \in S$, then there exist $c_j^{(i)} \in \mathcal{O}$ such that

$$s^i F(s)^{m-i} \equiv \sum_{j=0}^{q-1} c_j^{(i)} s^j \mod p\mathcal{O}.$$

Furthermore,

$$\sum_{s\in S} s^j \equiv 0 \mod p\mathcal{O},$$

for $1 \leq j \leq q-2$, and

$$\sum_{s\in S} s^{q-1} \equiv -1 \mod p\mathcal{O}.$$

Therefore,

$$\begin{aligned}
0 &\equiv \sum_{s\in S}\sum_{i=1}^{m-1} p^{-e}\binom{m}{i} t^i s^i F(s)^{m-i} \\
&\equiv \sum_{s\in S}\sum_{i=1}^{m-1} p^{-e}\binom{m}{i} t^i \sum_{j=0}^{q-1} c_j^{(i)} s^j \\
&\equiv \sum_{i=1}^{m-1} p^{-e}\binom{m}{i} t^i \sum_{j=0}^{q-1} c_j^{(i)} \sum_{s\in S} s^j \\
&\equiv -\sum_{i=1}^{m-1} p^{-e}\binom{m}{i} t^i c_{q-1}^{(i)} \mod p\mathcal{O},
\end{aligned}$$

for every $t \in T$. Thus, the polynomial

$$\sum_{i=1}^{m-1} p^{-e}\binom{m}{i} c_{q-1}^{(i)} x^i$$

has degree $m-1$ and has $|T| = |\Omega| > m-1$ roots in $\mathcal{O}/p\mathcal{O} \cong \mathbf{F}$. Thus, it must be the case that for every $i \in \{1, \ldots, m-1\}$,

$$p^{-e}\binom{m}{i} c_{q-1}^{(i)} \equiv 0 \mod p\mathcal{O}.$$

In particular, noting that $p^e || m$, it follows that $c_{q-1}^{(m-1)} \equiv 0 \mod p\mathcal{O}$.

From the definition of the $c_j^{(i)}$'s, one has

$$s^{m-1}F(s) \equiv c_j^{(m-1)} s^j \mod p\mathcal{O}.$$

Let

$$f(x) = \sum_{i=0}^{q-1} a_i x^i, \quad F(x) = \sum_{i=0}^{q-1} b_i x^i.$$

Then $b_{q-m} \equiv c_{q-1}^{(m-1)} \equiv 0 \mod p\mathcal{O}$, as $m \leq q$. Finally, $a_{q-m} = \pi(b_{q-m}) = 0$ as claimed. □

The following corollary is immediate from the definition of transversal mapping.

Corollary 3.11. *Let* $\mathbf{L}$ *be a finite extension of a finite field* $\mathbf{F}$. *If* $f \in \mathbf{L}[x]$ *is a transversal mapping polynomial of* $\mathbf{L}$ *as a vector space over* $\mathbf{F}$ *and* $\deg f < |\mathbf{L}|$, *then* $\deg f < |\mathbf{L}| - |\mathbf{F}|$.

Example 3.12. The above result says that all transversal mapping polynomials of GF(9) over GF(3) have degree at most $9 - 3 - 1 = 5$. The result here is sharp as indeed there are transversal mapping polynomials of degree 5. An example is $f(x) = \omega^2 x^5 + x^4 + \omega^6 x^3 + x^2 + \omega^6 x$, where $\omega^2 + \omega + 2 = 0$.

3.2 Regular spreads

Definition 3.13. A *regulus* $\mathcal{R}$ of Σ is a set of $q + 1$ pairwise skew lines with the property that any line meeting three lines of $\mathcal{R}$ meets every line of $\mathcal{R}$. Such a line is called a *transversal* of $\mathcal{R}$.

A line of $\mathrm{PG}(3, q)$ meeting a nondegenerate hyperbolic quadric in three points must be contained in the quadric. Each hyperbolic quadric admits two ruling families of $q + 1$ pairwise skew lines each. As the lines of such a family partition the points of the quadric, any line on the surface is either a member of the family or meets each member in a point. These families thus form regulii. In fact, any regulus arises as the ruling family of lines of a hyperbolic quadric. The following Lemma lists some more basic facts about regulii. See [11] for proofs of these and other facts concerning regulii.

Lemma 3.14. *Any three mutually skew lines* l, m, n *determine a unique regulus which will be denoted* $\mathcal{R}(l, m, n)$. *There are* $q + 1$ *transversals to a regulus* $\mathcal{R}$, *they are pairwise skew and themselves form another regulus which will be denoted* $\mathcal{R}^{opp}$. *Furthermore,* $(\mathcal{R}^{opp})^{opp} = \mathcal{R}$.

Definition 3.15. A spread is called *regular* if it contains the regulus determined by any three of its lines.

The proof of the following proposition can be found in [11].

Proposition 3.16. *If a line l is skew to each line of a regulus $\mathcal{R}$ then there is a unique regular spread containing l and $\mathcal{R}$.*

It turns out that if a spread is not regular, then it must be missing quite a few regulii. As the next lemma shows, a spread which contains every possible regulus on a given line must already contain too many regulii to avoid being regular.

Lemma 3.17. *Let $q > 2$ and let S be a spread of* $\mathrm{PG}(3, q)$. *If there exists some line l_0 of S such that the regulus $\mathcal{R}(l_0, l_1, l_2)$ is contained in S for every pair of distinct lines $l_1, l_2 \in \mathcal{S} \setminus \{l_0\}$, then S is regular.*

Proof. Let $\mathcal{R}$ be any regulus of S which contains l_0 and let $m \in S \setminus \mathcal{R}$. By Lemma 3.16 there exists a unique regular spread T containing $\mathcal{R}$ and m. For each $l \in \mathcal{R} \setminus \{l_0\}$, the regulus $\mathcal{R}(l_0, l, m)$ is contained in $S \cap T$ by hypotheses on S and T. Note that $\mathcal{R} \cap \mathcal{R}(l_0, l, m) = \{l_0, l\}$ and $\mathcal{R}(l_0, l_1, m) \cap \mathcal{R}(l_0, l_2, m) = \{l_0, m\}$ for distinct $l_i \in \mathcal{R} \setminus \{l_0\}$. Thus, for each of the q lines of $\mathcal{R} \setminus \{l_0\}$ we find $q - 2$ distinct lines of $(S \cap T) \setminus (\mathcal{R} \cup \{m\})$. Together with m this accounts for $(q-1)^2$ lines of $(S \cap T) \setminus \mathcal{R}$.

Suppose $S \neq T$. Let $m' \in S \setminus T$ and let T' be the unique regular spread containing $\mathcal{R}$ and m'. As above, $|(S \cap T') \setminus \mathcal{R}| \geq (q-1)^2$. Furthermore, by Proposition 3.16, $T \cap T' = \mathcal{R}$. Therefore

$$q(q-1) = |S \setminus \mathcal{R}| \geq |(S \cap T) \setminus \mathcal{R}| + |(S \cap T') \setminus \mathcal{R}| \geq 2(q-1)^2,$$

a contradiction if $q > 2$. Hence $S = T$ and S is regular. □

In the notation of the previous section, the next result characterizes regular spreads in terms of their associated transversal mappings. Recall $\mathbf{L} = \mathrm{GF}(q^3)$, $\mathbf{F} = \mathrm{GF}(q)$, $\xi \in \mathbf{L}$ such that $\mathrm{Tr}(\xi) = 1$ and $H = \{x \in L \mid \mathrm{Tr}(\xi x) = 0\}$. Furthermore, $V = \mathbf{F} \oplus \mathbf{L}$, $\Pi_\infty = \{0\} \oplus \mathbf{L}$, $\Pi_0 = \mathbf{F} \oplus H$, and $l_\infty = \{0\} \oplus H$.

Proposition 3.18. *Given $f \in \mathrm{TM}(H)$, the spread $\mathcal{S}(f)$ is a regular spread if and only if f is an affine map over $\mathbf{F}$.*

Proof. By Lemma 3.17, it is enough to show that $\mathcal{S}(f)$ contains each regulus of the form $\mathcal{R}(l_\infty, l_f(x), l_f(y))$ if and only if f is affine. Let $x, y \in H$ with $x \neq y$. Let $\mathcal{R} = \mathcal{R}(l_\infty, l_f(x), l_f(y))$. For $\lambda \in \mathbf{F}$ let

$$m_\lambda = (1, f(x) + \lambda x + \lambda) \vee (1, f(y) + \lambda y + \lambda)$$

and let

$$m_\infty = (1 : x + 1) \vee (1 : y + 1).$$

It is simple to check that $\mathcal{R}^{\text{opp}} = \{m_\lambda \mid \lambda \in \mathbf{F}^\circ\}$.

The points of m_∞ have as representatives the vectors $(0, rx + (1-r)y + 1)$, where $r \in \mathbf{F}^\circ$ and the usual conventions regarding ∞ are adopted. The points of m_λ have as representatives the vectors

$$\big(1, r(f(x) + \lambda x) + (1-r)(f(y) + \lambda y) + \lambda\big).$$

For each fixed r, there exist unique $s, t \in \mathbf{F}$ such that the following three projective points are collinear:

$$\begin{aligned}
&\big(0 : rx + (1-r)y + 1 \big), \\
&\big(1 : sf(x) + (1-s)f(y) \big), \\
&\big(1 : t(f(x) + x) + (1-t)(f(y) + y) + 1 \big).
\end{aligned}$$

Furthermore, this line is an element of $\mathcal{R}$, as it is a transversal of $\mathcal{R}^{\text{opp}}$. Note that with $r = s = t$, the sum of the first two of these vectors equals the third and hence these projective points are collinear. This line meets Π_∞ in the point $(0, rx + (1-r)y + 1)$ and meets Π_0 in the point $(1, rf(x) + (1-r)f(y))$. Hence, it is an element of $\mathcal{S}(f)$ if and only if $f(rx + (1-r)y) = rf(x) + (1-r)f(y)$. □

Remark 3.19. Together, Lemma 3.7, Proposition 3.9, and Proposition 3.18 count the number of regular spreads of Σ which contain the line l_∞. Indeed, by Proposition 3.9 there are $\frac{1}{2}q^2(q-1)^2$ linear transversal mappings of H. Thus, there are $\frac{1}{2}q^4(q-1)^2$

affine transversal mappings by applying Lemma 3.7 part (ii). By Proposition 3.18, there are the same number of regular spreads containing l_∞. This gives the well known result that there are $\frac{1}{2}q^4(q-1)^2(q^2+q+1)$ regular spreads of Σ, arguing as in Corollary 3.6.

One great benefit of the representation of spreads by their transversal mappings is that it is extremely easy to restrict one's attention solely to regular spreads. This feature allows a convenient computer search for regular spreads which would generate cyclic parallelisms under the application of a certain automorphism. Indeed, choosing a basis for H, one need only run through the 2×2 matrices over GF(q), omitting those with eigenvalues in GF(q), and allowing arbitrary affine translations. This search revealed a family of cyclic regular parallelisms when $q \equiv 2 \pmod 3$ which is the subject of the remaining sections of this chapter.

3.3 The construction

It was shown in Chapter 2 that if $q \equiv 0, 1 \pmod 3$ then PG$(3, q)$ admits no cyclic parallelisms. Thus, a standing assumption for the rest of this chapter is that $q \equiv 2 \pmod 3$. In [36], Pentilla and Williams give a construction of two inequivalent cyclic regular parallelisms of PG$(3, q)$ when $q \equiv 2 \pmod 3$. Their construction is given in terms of the hyperbolic polar space $O^+(6, q)$ via the Klein correspondence between the lines of PG$(3, q)$ and the singular points of this quadric. This section presents a construction of a cyclic regular parallelism of PG$(3, q)$ which was discovered independently of the result of Pentilla and Williams. The question of the equivalence of this construction with those of [36] is not addressed here. However, in Section 3.5 it is conjectured that there are exactly two equivalence classes of cyclic regular parallelisms of PG$(3, q)$ when $q \equiv 2 \pmod 3$. This conjecture of course implies the equivalence of the example here with one of those of [36].

The construction presented here is given in terms of a linear transversal mapping with the notation introduced in Chapter 2. Since $q \not\equiv 0 \pmod 3$, one may take $\xi = \frac{1}{3}$ and thus it will be the case that $H = \ker \mathrm{Tr}$. As before, let ω be a primitive

(q^2+q+1)st root of unity in $\mathbf{L}$. Note that ω generates G. Let $\sigma : V \to V$ be the linear transformation $\sigma : (t,x) \mapsto (t,\omega x)$. Recall Proposition 2.12, which shows that σ partitions the set of lines of $\mathrm{PG}(V)$ into q^2+1 orbits of length q^2+q+1.

Lemma 3.20. *As a projectivity of Σ, the map σ has a unique fixed point and a unique invariant plane. Furthermore, all orbits of σ on the lines of Σ have length q^2+q+1.*

Proof. It is straightforward to see that σ fixes the projective point $(1:0)$ and acts on the projective plane $\Pi_\infty = \{0\} \oplus \mathbf{L}$. As ω has order q^2+q+1 in $\mathbf{L}^*$, it follows that σ has order q^2+q+1 in $\mathrm{PGL}(V)$. Thus, the orbits of lines have length at most q^2+q+1. Next, note that $\sigma|_{\Pi_\infty}$ is a Singer cycle of $\mathrm{PG}(\Pi_\infty)$, since $G \cap \mathbf{F}^* = \{1\}$. Therefore, all line orbits of σ must have length exactly q^2+q+1. It is now trivial that there are no further fixed points or invariant planes. □

Given $f \in \mathrm{TM}(H)$, it is natural to ask whether the spread $\mathcal{S}(f)$ consists of a full set of orbit representatives under $\langle\sigma\rangle$ and thus generates a cyclic parallelism under the action of $\langle\sigma\rangle$. Let $\mathcal{P}(f) = \{\mathcal{S}(f)\sigma^i \mid i = 0,\ldots,q^2+q\}$ be the set of spreads generated by $\mathcal{S}(f)$ and σ.

Proposition 3.21. *$\mathcal{P}(f)$ is a parallelism of Σ if and only if*

$$f\left(\frac{3(x+1)y}{\mathrm{Tr}((x+1)y)} - 1\right) = f(x)y - \frac{\mathrm{Tr}(f(x)y)}{\mathrm{Tr}((x+1)y)}(x+1)y \tag{3.2}$$

has no solutions $(x,y) \in H \times G \setminus \{1\}$ with $\mathrm{Tr}((x+1)y) \neq 0$.

Proof. Since σ acts as a Singer cycle on the plane Π_∞, the orbit of the line l_∞ is precisely the set of lines of Π_∞. A parallelism results from the action of σ on $\mathcal{S}(f)$ if and only if the orbits of the lines $l_f(x)$, $x \in H$, are disjoint. It suffices to check whether or not the orbit of each $l_f(x)$ meets $\mathcal{S}(f)$. Suppose $l_f(x)\sigma^i = l_f(x')$ for some pair $x, x' \in H$ and $0 < i < q^2+q+1$. With $y = \omega^i$ it then follows that $\mathrm{Tr}((x+1)y) \neq 0$ and

$$x' + 1 = \frac{3(x+1)y}{\mathrm{Tr}((x+1)y)}.$$

Furthermore,

$$f\left(\frac{3(x+1)y}{\mathrm{Tr}((x+1)y)}-1\right)=f(x)y+\lambda(x+1)y$$

for some $\lambda \in \mathbf{F}$. Take the trace of each side of the above equation to see that

$$\lambda=-\frac{\mathrm{Tr}(f(x)y)}{\mathrm{Tr}((x+1)y)},$$

yielding the desired result. □

The following will be used as the base spread to generate a cyclic regular parallelism. Define $\theta : H \to H$ by $\theta(x) = x^q - x$.

Lemma 3.22. *$\mathcal{S}(\theta)$ is a regular spread of Σ.*

Proof. Note that

$$\frac{\theta(x)-\theta(y)}{x-y}=(x-y)^{q-1}.$$

If $x, y \in H$ and $x \neq y$, then the above expression cannot lie in $\mathbf{F}$. Indeed, $z^{q-1} \in \mathbf{F}$ implies $z \in \mathbf{F}$ as $(q-1, q^2+q+1) = 1$ when $q \not\equiv 1 \pmod 3$. Further, $x - y \in \mathbf{F}$ implies $x = y$ as $H \cap \mathbf{F} = \{0\}$. Now the above condition on the slopes of secants to the graph of θ is easily seen to be equivalent to the condition that θ is a transversal mapping of H. Therefore, $\mathcal{S}(\theta)$ is a spread of Σ by Proposition 3.5. Regularity follows from Proposition 3.18 and the fact that θ is a linear map. □

Substituting $f(x) = x^q - x$ into equation (3.2) and collecting the resulting terms in powers of y, it follows that $\mathcal{P}(\theta)$ is a parallelism if and only if the equation

$$\Big((x+1)^{q^2+q}-(x+1)^2\Big)y^{q^2+1}-\Big((x+1)^{q^2+1}-(x+1)^{2q}\Big)y^{q+1}-3(x+1)^q y^q+3(x+1)y=0$$

has no solutions $(x, y) \in H \times G \setminus \{1\}$ with $\mathrm{Tr}\big((x+1)y\big) \neq 0$. Applying the Frobenius automorphism of the extension $\mathbf{L}/\mathbf{F}$ to the above equation results in the equation $\Psi(x, y) = 0$, where $\Psi(x, y) = \phi(x, y) - \phi(x, y)^q$ and

$$\phi(x,y)=\Big((x+1)^{q^2+1}-(x+1)^{2q}\Big)y^{q+1}+3(x+1)^q y^q.$$

Thus, $\mathcal{P}(\theta)$ is a parallelism if and only if the bivariate polynomial $\Psi(x,y)$ has no zeros with $(x,y) \in H \times G \setminus \{1\}$ and $\mathrm{Tr}\big((x+1)y\big) \neq 0$. The following characterization of the zeros of Ψ will be more than sufficient to establish that $\mathcal{P}(\theta)$ is a parallelism of Σ. Its proof will occupy the next section of this chapter.

Theorem 3.23. *For each $x \in \mathbf{L} \setminus \{-1\}$, if $\Psi(x,y_1) = \Psi(x,y_2) = 0$ and $y_1 \neq y_2$, then $\mathrm{N}(y_1) \neq \mathrm{N}(y_2)$.*

Corollary 3.24. *$\mathcal{P}(\theta)$ is a parallelism of Σ.*

Proof. Suppose $x \in H$. Expand the polynomial $\Psi(x,1)$ in powers of x and reduce modulo $x^{q^2} + x^q + x$ to obtain

$$\begin{aligned}
\Psi(x,1) &= (x+1)^{q^2+1} - (x+1)^{2q} - (x+1)^{q+1} + (x+1)^{2q^2} - 3(x+1)^{q^2} + 3(x+1)^q \\
&= x^{q^2+1} + x^{q^2} + x + 1 - x^{2q} - 2x^q - 1 - x^{q+1} - x^q - x - 1 \\
&\qquad + x^{2q^2} + 2x^{q^2} + 1 - 3x^{q^2} - 3 + 3x^q + 3 \\
&= x^{q^2+1} - x^{2q} - x^{q+1} + x^{2q^2} \\
&= -x(x^q + x) - x^{2q} - x^{q+1} + (x^q + x)^2 \\
&= 0.
\end{aligned}$$

Thus, $\Psi(x,1) = 0$ whenever $x \in H$, so Theorem 3.23 implies that $\Psi(x,y) \neq 0$ for $(x,y) \in H \times G \setminus \{1\}$. Therefore, $\mathcal{P}(\theta)$ is a cyclic parallelism. Regularity was shown in Lemma 3.22. □

3.4 The proof of Theorem 3.23

This section contains two technical lemmas needed to prove Theorem 3.23.

Lemma 3.25. *If $a \in \mathbf{L} \setminus \{1\}$ then the polynomial $z^{q+1} + z^q + a$ has at most two roots in $\mathbf{L}$. Moreover, these roots are of the form*

$$z = \frac{\mu + a^{q^2}}{(a-1)^q},$$

where $\mu \in \mathbf{F}$ *and* $\mu^2 - (1 - \mathrm{Tr}(a))\mu + \mathrm{N}(a) = 0$.

Proof. If $a = 0$ then the roots of the polynomial are $0, 1$ and the given formula holds. So assume $a \in \mathbf{L} \setminus \{0, 1\}$. Note that $(q+1)(q^2 - q + 1) = 2 + (q^3 - 1)$. Thus,

$$\begin{aligned} z^2 &= (z^{q+1})^{q^2-q+1} \\ &= z^{q+1}\left((z^{q+1})^q\right)^{q-1} \\ &= z^{q+1}(z^{q^2} + a^q)^{q-1} \\ &= z^{q+1}(-1 - \frac{a^{q^2}}{z} + a^q)^{q-1} \\ &= z^2\left((a-1)^q z - a^{q^2}\right)^{q-1}. \end{aligned}$$

Since z cannot equal 0, it must be that $(a-1)^q z - a^{q^2} = \mu$ for some $\mu \in \mathbf{F}^*$. Thus, $z = \frac{\mu + a^{q^2}}{(a-1)^q}$. Now substitute this expression for z into the original equation $z^{q+1} + z^q + a = 0$ to obtain the desired quadratic satisfied by μ. □

Recall that $\Psi(x, y) = \phi(x, y) - \phi(x, y)^q$. Let

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

so that $\phi(x, y) = \alpha(x)y^{q+1} + \beta(x)y^q$.

The first case for the proof of Theorem 3.23 is to assume $x \in \mathbf{F} \setminus \{-1\}$. In this case, $\alpha(x) = 0$ and $\beta(x) \in \mathbf{F}^*$. Thus, $\Psi(x, y) = \beta(x)(y^q - y^{q^2}) = 0$ if and only if $y \in \mathbf{F}$. Distinct elements of $\mathbf{F}$ have distinct norms relative to the extension $\mathbf{L}/\mathbf{F}$, as $(q-1, 3) = 1$. Thus, the claimed characterization of the zeros of Ψ holds if $x \in \mathbf{F} \setminus \{-1\}$.

For the remainder of this section assume $x \in \mathbf{L} \setminus \mathbf{F}$. Note that $\alpha(x) \neq 0$ in this case. Indeed, $\alpha(x) = 0$ if and only if $(x+1)^{(q-1)^2} = 1$. Using the fact that $u^{q-1} \in \mathbf{F}^*$ if and only if $u^{q-1} = 1$, it follows that $\alpha(x) = 0$ if and only if $x \in \mathbf{F}$.

Thus, it is the case that $\alpha(x), \beta(x) \neq 0$. For the sake of notational simplicity, the arguments to α and β will, where reasonable, be omitted. As $\Psi(x,y) = \phi(x,y) - \phi(x,y)^q$, it follows that $\Psi(x,y) = 0$ if and only if $\phi(x,y) \in F$. Suppose that

$$\alpha y^{q+1} + \beta y^q + \lambda = 0, \tag{3.3}$$

for some $\lambda \in \mathbf{F}$.

Let $z = \frac{\alpha y}{\beta}$. Multiplying equation (3.3) by $\frac{\alpha^q}{\beta^{q+1}}$ results in

$$z^{q+1} + z^q + \gamma = 0, \tag{3.4}$$

where

$$\gamma = \gamma(x,\lambda) = \frac{\lambda\alpha(x)^q}{\beta(x)^{q+1}} \tag{3.5a}$$

$$= \frac{\lambda}{3}\Big((x+1)^{q(q-1)} - (x+1)^{q-1}\Big). \tag{3.5b}$$

Note that expression (3.5b) implies that $\mathrm{Tr}(\gamma) = 0$; in particular, $\gamma \neq -1$. Therefore, Lemma 3.25 applies to equation (3.4), yielding

$$z = \frac{\mu + \gamma^{q^2}}{(\gamma - 1)^q} \tag{3.6}$$

where $\mu \in \mathbf{F}$ and

$$\mu^2 - \mu + \mathrm{N}(\gamma) = 0. \tag{3.7}$$

Lemma 3.26. *With z and μ as in equations (3.6) and (3.7), $\mathrm{N}(z) = -\mu$.*

Proof. Note that

$$\mathrm{N}(z) = \frac{\mathrm{N}(\mu + \gamma)}{\mathrm{N}(\gamma - 1)}.$$

Furthermore, as $\mathrm{Tr}(\gamma) = 0$ and $\mu^2 - \mu + \mathrm{N}(\gamma) = 0$, one has

$$\begin{aligned}\mathrm{N}(\mu+\gamma) &= (\mu+\gamma)(\mu+\gamma^q)(\mu+\gamma^{q^2}) \\ &= \mu^3 + \mu^2\mathrm{Tr}(\gamma) + \mu\mathrm{Tr}(\gamma^{q+1}) + \mathrm{N}(\gamma) \\ &= \Big(1 + \mathrm{Tr}(\gamma^{q+1}) - \mathrm{N}(\gamma)\Big)\mu \\ &= -\mathrm{N}(\gamma-1)\mu.\end{aligned}$$

The result is now immediate. □

To complete the proof of Theorem 3.23, suppose $x \in \mathbf{L} \setminus \mathbf{F}$ and $\Psi(x, y_1) = \Psi(x, y_2) = 0$. It has been shown that then there exist $\lambda_1, \lambda_2 \in \mathbf{F}$ such that

$$\alpha(x)y_i^{q+1} + \beta(x)y_i^q + \lambda_i = 0,$$

for $i = 1, 2$. Let $z_i = \frac{\alpha(x)y_i}{\beta(x)}$ and $\gamma_i = \gamma(x, \lambda_i) = \frac{\lambda_i\alpha(x)^q}{\beta(x)^{q+1}}$. Then there also exist $\mu_1, \mu_2 \in \mathbf{F}$ such that

$$z_i = \frac{\mu_i + \gamma_i^{q^2}}{(\gamma_i - 1)^q}$$

and $\mu_i^2 - \mu_i + \mathrm{N}(\gamma_i) = 0$.

Suppose $\mathrm{N}(y_1) = \mathrm{N}(y_2)$. By definition of z_i, one has $\mathrm{N}(z_1) = \mathrm{N}(z_2)$. By Lemma 3.26, one has $\mathrm{N}(z_i) = -\mu_i$. Thus, $\mu_1 = \mu_2$. Therefore,

$$\mathrm{N}(\gamma_1) = \mu_1 - \mu_1^2 = \mu_2 - \mu_2^2 = \mathrm{N}(\gamma_2).$$

Furthermore, by definition of γ_i, one has

$$\mathrm{N}(\gamma_i) = \frac{\lambda_i^3\mathrm{N}(\alpha)}{\mathrm{N}(\beta)^2}.$$

Hence, $\mathrm{N}(y_1) = \mathrm{N}(y_2)$ implies that $\lambda_1^3 = \lambda_2^3$ from which it follows, since $(3, q-1) = 1$, that $\lambda_1 = \lambda_2$. But then $\gamma_1 = \gamma_2$ and hence $\mu_1 = \mu_2$. Now it follows that $z_1 = z_2$, hence $y_1 = y_2$.

In summary, if $\Psi(x, y_1) = \Psi(x, y_2) = 0$ and $\mathrm{N}(y_1) = \mathrm{N}(y_2)$, then $y_1 = y_2$ and the proof is complete. □

3.5 Other examples

This section concerns the investigation of further examples of cyclic regular parallelisms. Of course, it is easy to see that there are at least $q - 1$ additional cyclic regular parallelisms, given by $\mathbf{F}^*$ multiples of the transversal mapping θ. However, these examples are equivalent under the group of projectivities $\mathrm{PGL}(V)$ of Σ. An inequivalent example is produced by applying a polarity of Σ to the original example. This idea for producing a new example was also used in [36]. It is conjectured that there are no further examples of cyclic regular parallelisms, up to projective equivalence. Some reductions are offered which slightly simplify the scope of work remaining to prove such a classification.

To obtain some additional cyclic regular parallelisms, note that $f : H \to H$ is a transversal mapping if and only if λf is a transversal mapping for every $\lambda \in \mathbf{F}^*$. Furthermore, combining Proposition 3.21 with the fact that the trace function of the extension $\mathbf{L}/\mathbf{F}$ is $\mathbf{F}$-linear, it follows that $\mathcal{P}(f)$ is a parallelism if and only if $\mathcal{P}(\lambda f)$ is a parallelism for every $\lambda \in \mathbf{F}^*$. Thus, one obtains a family of cyclic regular parallelisms $\mathcal{P}(\lambda\theta)$, $\lambda \in \mathbf{F}^*$, from the single example constructed in the previous sections.

However, as mentioned above, these new parallelisms are essentially the same as the original example, in that they are equivalent under the group of projectivities of the geometry. Indeed, for $\lambda \in \mathbf{F}^*$ define $\tau_\lambda : V \to V$ by $(t, x)\tau_\lambda = (t, \lambda x)$. Note that $(0 : u) = (0 : \lambda u) = (0 : u)\tau_\lambda$ for every $u \in \mathbf{L}^*$. That is, τ_λ fixes each point of Π_∞. Therefore, for $f \in \mathrm{TM}(H)$,

$$l_{\lambda f}(x) = (0 : x + 1) \vee (1 : \lambda f(x)) = l_f(x)\tau_\lambda.$$

Since $l_\infty \tau_\lambda = l_\infty$ then $\mathcal{S}(\lambda f) = \mathcal{S}(f)\tau_\lambda$ for every $\lambda \in \mathbf{F}^*$ and every $f \in \mathrm{TM}(H)$.

Finally, the projectivities σ and τ_λ commute. Therefore, for $f \in \mathrm{TM}(H)$,

$$\begin{aligned}\mathcal{P}(\lambda f) &= \{\mathcal{S}(\lambda f)\sigma^i \mid 0 \le i \le q^2+q\} \\ &= \{\mathcal{S}(f)\tau_\lambda\sigma^i \mid 0 \le i \le q^2+q\} \\ &= \{\mathcal{S}(f)\sigma^i\tau_\lambda \mid 0 \le i \le q^2+q\} \\ &= \mathcal{P}(f)\tau_\lambda.\end{aligned}$$

Thus, $\mathcal{P}(f)$ and $\mathcal{P}(\lambda f)$ are projectively equivalent. One is a parallelism if and only if the other is. Hence, the members of the family $\{\mathcal{P}(\lambda\theta) \mid \lambda \in \mathbf{F}^*\}$ of cyclic regular parallelisms mentioned above belong to the same equivalence class under the action of $\mathrm{PGL}(V)$.

An inequivalent example can be obtained by considering the following polarity of Σ. Let $\langle\cdot,\cdot\rangle : V \times V \to \mathbf{F}$ be the symmetric bilinear form

$$\langle (t_1, x_1), (t_2, x_2)\rangle = t_1t_2 - \frac{1}{3}\mathrm{Tr}(x_1x_2).$$

That this is indeed a symmetric bilinear form is straightforward to check and merely makes uses of the $\mathbf{F}$-linearity of the trace map Tr. It is also straightforward to see that this inner product is nondegenerate. Define the polarity $\perp$: $V \to \mathbf{F}$ by $\mathbf{v}^\perp = \langle \mathbf{v}, \mathbf{v}\rangle$. An important property of this particular polarity is that it interchanges the point, $(1:0)$, and the plane, Π_∞, which are stabilized under the action of σ. Furthermore, $l_\infty^\perp = (0:1) \vee (1:0)$. Since polarities send the points, lines, and planes of Σ to the planes, lines, and points, respectively, and preserve incidence in Σ, it follows that the dual of any spread which contains the lines l_∞ and $l_\infty^\perp$ is itself another spread containing these two lines. Thus, if f is a transversal mapping of H and $f(0) = 0$ then there exists a unique transversal mapping of H, call it $f^\perp$, such that $\mathcal{S}(f)^\perp = \mathcal{S}(f^\perp)$.

Proposition 3.27. *Let $f \in \mathrm{TM}(H)$ and suppose $f(0) = 0$. Then $\mathcal{P}(f)$ is a parallelism if and only if $\mathcal{P}(f^\perp)$ is a parallelism.*

Proof. It is straightforward to check that $(\mathbf{v}\sigma)^\perp = \mathbf{v}^\perp\sigma^{-1}$ for every $\mathbf{v} \in V$. Thus

$(\mathcal{S}(f)\sigma^i)^\perp = \mathcal{S}(f)^\perp\sigma^{-i} = \mathcal{S}(f^\perp)\sigma^{-i}$. Hence,

$$\begin{aligned}\mathcal{P}(f)^\perp &= \{(\mathcal{S}(f)\sigma^i)^\perp \mid 0 \le i \le q^2+q\} \\ &= \{\mathcal{S}(f^\perp)\sigma^{-i} \mid 0 \le i \le q^2+q\} \\ &= \{\mathcal{S}(f^\perp)\sigma^{i} \mid 0 \le i \le q^2+q\} \\ &= \mathcal{P}(f^\perp).\end{aligned}$$

As the notation suggests, it happens that $\mathcal{P}(f)$ and $\mathcal{P}(f^\perp)$ are duals of each other under the polarity $\perp$. Therefore, one of them is a parallelism if and only if both of them are parallelisms. □

Thus, $\mathcal{P}(\theta)^\perp = \mathcal{P}(\theta^\perp)$ is a cyclic regular parallelism. It turns out that it is not equivalent to $\mathcal{P}(\theta)$; establishing this fact is the subject of the next proposition. The proof will use the fact that $\theta^\perp(x) = -\frac{1}{3}(x^q + 2x)$. The details of the calculation of $f^\perp$ from a transversal mapping f with $f(0) = 0$ will be given in an appendix following this section.

Proposition 3.28. *$\mathcal{P}(\theta)$ and $\mathcal{P}(\theta^\perp)$ are not projectively equivalent.*

Proof. For notational simplicity, let $\mathcal{P}$ denote the parallelism $\mathcal{P}(\theta)$. Suppose to the contrary that $\mathcal{P}^\perp\tau = \mathcal{P}$ for some $\tau \in \mathrm{P\Gamma L}(V)$. Let $\mathrm{Stab}(\mathcal{P})$ denote the group of collineations of Σ which act on the set of spreads of $\mathcal{P}$. It follows that $\langle\sigma\rangle$ and $\tau^{-1}\langle\sigma\rangle\tau$ are subgroups of $\mathrm{Stab}(\mathcal{P}) \cap \mathrm{PGL}(V)$. Note that q^2+q+1 is relatively prime to $|\mathrm{PGL}(V)|/(q^2+q+1) = q^6(q^2+1)(q+1)(q-1)^2$, since $(q-1,3) = 1$. It follows that any two subgroups of $\mathrm{Stab}(\mathcal{P}) \cap \mathrm{PGL}(V)$ with the same maximal prime-power order dividing q^2+q+1 are Sylow subgroups and hence are conjugate. Therefore, for some $1 \le r < q^2+q+1$, there exists $h \in \mathrm{Stab}(\mathcal{P}) \cap \mathrm{PGL}(V)$ such that $\langle\sigma^r\rangle = h^{-1}\tau^{-1}\langle\sigma^r\rangle\tau h$. Note that $\tau h \in N_{\mathrm{P\Gamma L}(V)}(\langle\sigma^r\rangle)$ and $\mathcal{P}^\perp\tau h = \mathcal{P}h = \mathcal{P}$. Furthermore, $\tau h\sigma^i$ shares these two properties. Without loss of generality it thus may be assumed that $\tau \in N_{\mathrm{P\Gamma L}(V)}(\langle\sigma^r\rangle)$ and $\mathcal{S}(\theta^\perp)\tau = \mathcal{S}(\theta)$.

Note that σ^r has a unique fixed point $(1:0)$ and a unique invariant plane, Π_∞. Since τ normalizes $\langle\sigma^r\rangle$ it follows that τ fixes the point $(1:0)$ and acts on the plane

Π_∞. Define $f \in \mathrm{P\Gamma L}(\mathbf{L})$ so that $(0 : x)\tau = (0 : f(x))$ for $x \in \mathbf{L}^*$. Note that $(0 : x)\sigma^r = (0 : \alpha x)$ where $\alpha = \omega^{r(q-1)}$. Since τ normalizes $\langle \sigma^r \rangle$, it follows that there exists $k > 0$ such that

$$f(\alpha x) = \alpha^k f(x) \text{ for all } x \in \mathbf{L}. \tag{3.8}$$

Let $q = p^n$. All functions from $\mathbf{L}$ to $\mathbf{L}$ are polynomials and the $\mathbf{F}$-linear polynomials are those of the form $g(x) = \xi_0 x + \xi_1 x^q + \xi_2 x^{q^2}$, with coefficients $\xi_i \in \mathbf{L}$. The semilinear polynomials all have the form $g(x^{p^m})$ for some linear polynomial $g(x)$ and $0 \leq m < n$. From equation (3.8), it can be seen that at most one coefficient of $f(x)$ is nonzero; hence,

$$f(x) = \xi x^{p^{m+in}} \text{ for some } i \in \{0, 1, 2\}. \tag{3.9}$$

Recall that $\mathcal{S}(\theta^\perp)\tau = \mathcal{S}(\theta)$. Since τ fixes the projective point $(1 : 0)$ and stabilizes the plane Π_∞, it must be the case that τ fixes the lines l_∞ and $l_{\theta^\perp}(0) = l_\theta(0)$. Hence, $\xi = f(1) \in \mathbf{F}^*$ and $f(H) = H$. Furthermore, for $x \in H$,

$$\begin{aligned} l_{\theta^\perp}(x)\tau &= \big(0 : f(x+1)\big) \vee \big(1 : f(\theta^\perp(x))\big) \\ &= \big(0 : f(x) + \xi\big) \vee \left(1 : \frac{-1}{3} f(x^q) - \frac{2}{3} f(x)\right). \end{aligned}$$

This line meets Π_∞ in the point $(0 : \frac{f(x)}{\xi} + 1)$. Therefore $l_{\theta^\perp}(x)\tau = l_\theta(\frac{f(x)}{\xi})$ for each $x \in H$, from which it follows that

$$\frac{f(x^q) + 2f(x)}{3} = \frac{f(x) - f(x)^q}{\xi} \quad \forall x \in H. \tag{3.10}$$

Since f is a permutation of H, introduce the new variable $y = f(x)$. Note that $f(x^q) = f(x)^q = y^q$, as $\xi \in \mathbf{F}$. Substituting equation (3.9) into equation (3.10) and changing variables yields

$$(\xi + 3)y^q + (2\xi - 3)y = 0 \quad \forall y \in H. \tag{3.11}$$

Since $q \equiv 2 \pmod 3$, it cannot be that both coefficients of the above polynomial are zero. Thus, equation (3.11) gives a nonzero polynomial of degree less than q^2 vanishing everywhere on H, a contradiction as $|H| = q^2$. Therefore no such τ exists. □

For $q \equiv 2 \pmod 3$, there are thus at least two projective equivalence classes of cyclic regular parallelisms of $\mathrm{PG}(3, q)$. The question arises whether there are any more. The characterization of regular spreads by affine transversal mappings gives an efficient way to answer this question by computer search for sufficiently small values of q. This section concludes with some remarks about this search and its results.

The search for cyclic regular parallelisms is based on Propositions 3.18 and 3.21. Recall that Proposition 3.18 says that regular spreads are of the form $\mathcal{S}(f)$ for some affine $f \in \mathrm{TM}(H)$. Proposition 3.21 gives a necessary and sufficient condition for the set of spreads $\mathcal{P}(f)$ to be a parallelism. The problem is thus to determine which affine transversal mappings satisfy the condition of Proposition 3.21. The place to start is to give a description of affine transversal mappings in terms of polynomials.

Proposition 3.29. *Every affine transversal mapping of H is uniquely of the form $(ax)^q + bx + c$, for $a, b, c \in \mathbf{L}$, where*

(i) $a + b \in \mathbf{F}$,

(ii) $c \in H$, and

(iii) the polynomial $\lambda^2 + \mathrm{Tr}(a)\lambda + \mathrm{Tr}(a^{q+1})$ has no roots in $\mathbf{F}$.

Proof. $\mathrm{Hom}_{\mathbf{F}}(H, \mathbf{L})$ is an $\mathbf{L}$-vector space of dimension 2 spanned by $\{x, x^q\}$. Given an affine map $f : H \to L$, there exist unique $a, b, c \in L$ such that $f(x) = (ax)^q + bx + c$ for all $x \in H$. Conditions *(i)* and *(ii)* of the Proposition arise from requiring that $f(H) \subseteq H$. As $f(0) = c$, it follows that $c \in H$. In general,

$$\begin{aligned} \mathrm{Tr}(f(x)) &= \mathrm{Tr}((ax)^q) + \mathrm{Tr}(bx) + \mathrm{Tr}(c) \\ &= \mathrm{Tr}(ax) + \mathrm{Tr}(bx) + 0 \\ &= \mathrm{Tr}\big((a+b)x\big). \end{aligned}$$

The condition $\mathrm{Tr}(f(x)) = 0$ for all $x \in H$ implies that $a + b \in H^{\perp} = \mathbf{F}$ under the trace inner product. Thus, $f : H \to H$ if and only if conditions *(i)* and *(ii)* are met.

Finally, condition *(iii)* arises from the requirement that f be a transversal mapping of H. As

$$\frac{f(x) - f(y)}{x - y} = a^q(x - y)^{q-1} + b$$

and $a + b \in \mathbf{F}$, then $f \in \mathrm{TM}(H)$ if and only if

$$a^q x^{q-1} - a \notin \mathbf{F} \ \forall \ x \in H \setminus \{0\}.$$

Furthermore, for any $x \in L^*$,

$$a^q x^{q-1} - a = \lambda \in \mathbf{F}$$

if and only if

$$\begin{aligned}
\mathrm{Tr}(x) &= x + x^q + x^{q^2} \\
&= x + x \cdot x^{q-1} + x \cdot x^{q-1} \cdot (x^{q-1})^q \\
&= x + x\left(\frac{\lambda + a}{a^q}\right) + x\left(\frac{\lambda + a}{a^q}\right)\left(\frac{\lambda + a^q}{a^{q^2}}\right) \\
&= \frac{ax}{\mathrm{N}(a)}\left(a^{q^2+q} + a^{q^2}(\lambda + a) + (\lambda + a)(\lambda + a^q)\right) \\
&= \frac{ax}{\mathrm{N}(a)}\left(\lambda^2 + \mathrm{Tr}(a)\lambda + \mathrm{Tr}(a^{q+1})\right).
\end{aligned}$$

Therefore, there exists $x \in H \setminus \{0\}$ such that $a^q x^{q-1} - a \in \mathbf{F}$ if and only if there exists $\lambda \in \mathbf{F}$ such that $\lambda^2 + \mathrm{Tr}(a)\lambda + \mathrm{Tr}(a^{q+1}) = 0$. Thus, $f \in \mathrm{TM}(H)$ if and only if the quadratic polynomial $X^2 + \mathrm{Tr}(a)X + \mathrm{Tr}(a^{q+1}) \in \mathbf{F}[X]$ has no roots in $\mathbf{F}$. □

Theorem 2.25 limits the search for transversal mappings f generating a cyclic parallelism $\mathcal{P}(f)$. With the choice $l_\infty = \{0\} \oplus \ker \mathrm{Tr}$, Theorem 2.25 implies that a necessary condition for $\mathcal{P}(f)$ to be a parallelism is that $f(0) = 0$. That is, one need only consider linear transversal mappings when searching for cyclic regular parallelisms. An exhaustive computer search over all linear transversal mappings, using

the characterization of Proposition 3.29, for those which generate cyclic parallelisms revealed only the two examples $\theta(x)$ and $\theta^{\perp}(x)$, along with their $\mathbf{F}^*$-multiples, for $q \in \{2, 5, 8, 11, 17, 23, 29, 32\}$. Thus, the following conjecture has been verified for all prime powers $q \leq 32$.

Conjecture 3.30. *If* $q \equiv 2 \pmod 3$, *there are exactly two projective equivalence classes of cyclic regular parallelisms of* $\mathrm{PG}(3, q)$.

3.6 Appendix: calculating $f^{\perp}$

Recall from the previous section the inner product $\langle \cdot, \cdot \rangle : V \times V \to \mathbf{F}$ given by

$$\langle (t_1, x_1), (t_2, x_2) \rangle = t_1 t_2 - \frac{1}{3}\mathrm{Tr}(x_1 x_2)$$

and the polarity $\perp$: $V \to \mathbf{F}$ given by $\mathbf{v}^{\perp} = \langle \mathbf{v}, \mathbf{v} \rangle$. Since $\perp$ maps lines of $\mathrm{PG}(V)$ to lines of $\mathrm{PG}(V)$, interchanges the lines $l_\infty = \{0\} \oplus H$ and $\mathbf{F} \oplus \mathbf{F}$, and preserves incidence, it follows that $\perp$ acts on the set of spreads containing $\mathbf{F} \oplus \mathbf{F}$ and l_∞. By extension, one can define an action of $\perp$ on the set of transversal mappings of H which fix 0; namely, set $f^{\perp}$ to be the transversal mapping such that $\mathcal{S}(f^{\perp}) = \mathcal{S}(f)^{\perp}$. This section contains the details for calculating $f^{\perp}$.

Let $f \in \mathrm{TM}(H)$ with $f(0) = 0$. Since $l_\infty^{\perp} = (0:1) \vee (1:0)$ then $f^{\perp}(0) = 0$. Let $x \in H$ and $x \neq 0$. Note that $l_f(x)^{\perp}$ is skew to $l_f(0) = l_\infty^{\perp}$; therefore, $l_f(x)^{\perp}$ is skew to l_∞. So $l_f(x)^{\perp}$ meets the plane Π_∞ in a unique point, and this point is not incident with the line l_∞.

Let $u = u(x) = 2f(x)^q + f(x)$. Note that $u \in H$ and

$$\mathrm{Tr}(uf(x)) = \mathrm{Tr}\big(2f(x)^{q+1} + f(x)^2\big) = \mathrm{Tr}\big(f(x)\big)^2 = 0.$$

Therefore,

$$\langle (0, cu + 1), \big(1, f(x)\big) \rangle = 0 \text{ for every } c \in \mathbf{F}.$$

Suppose $\mathrm{Tr}(ux) = 0$. Then

$$\langle (0, x+1), (0, u) \rangle = -\frac{1}{3}\mathrm{Tr}(ux) = 0.$$

Since

$$\langle (1, f(x)), (0, u) \rangle = -\frac{1}{3}\mathrm{Tr}(uf(x)) = 0,$$

this assumption implies that the point $(0 : u)$ is incident with the line $l_f(x)^\perp$. However, this is impossible as $(0 : u)$ is a point of l_∞. Therefore, $\mathrm{Tr}(ux) \neq 0$ and

$$l_f(x)^\perp \cap \Pi_\infty = \left(0 : \frac{-3u}{\mathrm{Tr}(ux)} + 1\right).$$

Now let $y = y(x) = 2x^q + x$. Arguing as above, it can be shown that $\mathrm{Tr}(yf(x)) \neq 0$ and

$$l_f(x)^\perp \cap \Pi_0 = \left(1 : \frac{3y}{\mathrm{Tr}\big(yf(x)\big)}\right).$$

Thus, for every $x \in H \setminus \{0\}$,

$$f^\perp\left(\frac{-3\big(2f(x)^q + f(x)\big)}{\mathrm{Tr}\big(2xf(x)^q + xf(x)\big)}\right) = \frac{3(2x^q + x)}{\mathrm{Tr}\big(2x^q f(x) + xf(x)\big)}.$$

If it is further assumed that f is linear, then a more explicit expression for $f^\perp$ may be given. Indeed, if f is linear then $\mathcal{S}(f)$ is a regular spread. Hence, $\mathcal{S}(f^\perp) = \mathcal{S}(f)^\perp$ is a regular spread, as it is easily seen that polarities preserve the regularity property of spreads. Thus, $f^\perp$ is an affine transversal mapping. But $f^\perp(0) = 0$, so $f^\perp$ is also linear. Therefore,

$$f^\perp\big(2f(x)^q + f(x)\big) = -\frac{\mathrm{Tr}\big(2xf(x)^q + xf(x)\big)}{\mathrm{Tr}\big(2x^q f(x) + xf(x)\big)}(2x^q + x) \quad \forall x \in H \setminus \{0\}.$$

Note that for each $x \in H$,

$$\begin{aligned}
&\mathrm{Tr}\big(2xf(x)^q + xf(x)\big) + \mathrm{Tr}\big(2x^q f(x) + xf(x)\big) \\
&\qquad = 2\mathrm{Tr}\big(xf(x) + xf(x)^q + x^q f(x)\big) \\
&\qquad = 2\mathrm{Tr}\big(xf(x) + xf(x)^q + xf(x)^{q^2}\big) \\
&\qquad = 2\mathrm{Tr}\big(x\mathrm{Tr}(f(x))\big) \\
&\qquad = 2\mathrm{Tr}(x)\mathrm{Tr}\big(f(x)\big) \\
&\qquad = 0.
\end{aligned}$$

Therefore,

$$\frac{\mathrm{Tr}\big(2xf(x)^q + xf(x)\big)}{\mathrm{Tr}\big(2x^q f(x) + xf(x)\big)} = -1 \text{ for every } x \in H \setminus \{0\}.$$

Let $\delta(x) = 2x^q + x$. Then

$$f^{\perp}\big(\delta\big(f(x)\big)\big) = \delta(x) \quad \forall x \in H. \tag{3.12}$$

Since f and δ are permutations of H, equation (3.12) can be rewritten as

$$f^{\perp}(x) = \delta \circ f^{-1} \circ \delta^{-1}(x) \quad \forall x \in H. \tag{3.13}$$

It remains to calculate the inverse of linear transversal mappings of H.

By Proposition 3.29 a linear transversal mapping of H has the form $f(x) = (ax)^q + (\lambda - a)x$, where $\lambda \in \mathbf{F}$ and the polynomial $X^2 + \mathrm{Tr}(a)X + \mathrm{Tr}(a^{q+1})$ has no roots in $\mathbf{F}$. Write $f^{-1}(x) = (bx)^q + (\mu - b)x$ for some $b \in \mathbf{L}$ and $\lambda \in \mathbf{F}$. The equations $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x$ yield

$$b = \frac{-a}{\lambda^2 - \mathrm{Tr}(a)\lambda + \mathrm{Tr}(a^{q+1})} \tag{3.14}$$

$$\mu = \frac{\lambda - \mathrm{Tr}(a)}{\lambda^2 - \mathrm{Tr}(a)\lambda + \mathrm{Tr}(a^{q+1})}. \tag{3.15}$$

Note that $\lambda^2 - \mathrm{Tr}(a)\lambda + \mathrm{Tr}(a^{q+1}) \neq 0$ by Proposition 3.29 *(iii)*. In particular, $\delta^{-1}(x) =$

$-\frac{1}{3}\delta(x)$. Finally, one obtains $f^{\perp}(x) = -\frac{1}{3}\delta \circ f^{-1} \circ \delta(x) = (cx)^q + (\mu - c)x$ where μ is given by equation (3.14b) and

$$c = \frac{3a - 2\mathrm{Tr}(a)}{3(\lambda^2 - \mathrm{Tr}(a)\lambda + \mathrm{Tr}(a^{q+1}))}.$$

Note that for $\theta(x) = x^q - x$, one has $a = 1$ and $\lambda = 0$. Thus, $\theta^{\perp}(x) = -\frac{1}{3}(x^q + 2x)$ as claimed in the previous section.

Chapter 4 Beyond Dimension Three

As always, *parallelism* refers to a parallelism of the lines of $\mathrm{PG}(2n+1,q)$. Projective spaces of dimensions greater than three may admit spreads of subspaces of dimensions greater than 1; one may wish to consider parallelisms consisting of these subspaces. However, the concern here will be confined to parallelisms of lines and thus the term parallelism will remain unqualified.

Surprisingly little is known about parallelisms of projective spaces of odd dimension greater than 3. Despite being among the most well-known designs, and possessing the basic numerical parameters necessary to admit resolutions, the design of points and lines of $\mathrm{PG}(2n+1,q)$ is only known to be resolvable in the following cases:

- $\mathrm{PG}(2n-1,2)$ is resolvable for all $n \geq 2$, due to Baker [2];
- $\mathrm{PG}(2^i-1,q)$ is resolvable for all $i \geq 2$ and any prime power q, due to Beutelspacher [9].

There is no instance for which it is known that $\mathrm{PG}(2n-1,q)$ fails to admit parallelisms. In particular, the question of resolvability for $\mathrm{PG}(5,q)$ is open for every prime power $q > 2$.

Beutelspacher's construction [9] does not result in cyclic parallelisms. On the other hand, Baker's constructions of parallelisms of $\mathrm{PG}(2n-1,2)$ are cyclic. In fact, in [3], a variant of his construction of [2] yields a pair of orthogonal cyclic parallelisms of $\mathrm{PG}(2n-1,2)$ if $n \not\equiv 2 \pmod 3$. Two parallelisms P and P' are said to be *orthogonal* if $|S \cap S'| \leq 1$ for any pair of spreads $S \in P$ and $S' \in P'$. These examples of Baker appear to be the only examples of cyclic parallelisms in dimensions greater than 3.

Section 4.1 contains a construction of a set of skew line-orbit representatives under the action of a Singer cycle on projective spaces of even dimension. A second construction, this time in $\mathrm{PG}(2n-1,2)$, gives a partial spread consisting of representatives of all line-orbits not contained in the invariant hyperplane of an automorphism

of order $\theta(2n-2,2)$. Section 4.2 concludes the chapter with a discussion of some open problems relating to parallelisms in dimensions greater than three.

4.1 Partial solutions

Suppose $\alpha \in \mathrm{P\Gamma L}(2n,q)$ acts transitively on the spreads of a parallelism of $\mathrm{PG}(2n-1,q)$. By Lemma 2.8 and Theorem 2.10, $q \not\equiv 1 \pmod{2n-1}$, α is a projectivity, and all line-orbits under α have length $\theta(2n-2,q) = \frac{q^{2n-1}-1}{q-1}$. Furthermore, α fixes a point and acts as a Singer cycle on some hyperplane Π. As there are

$$\frac{(q^{2n}-1)(q^{2n-1}-1)}{(q^2-1)(q-1)}$$

lines of $\mathrm{PG}(2n-1,q)$, then there are

$$\frac{q^{2n}-1}{q^2-1} = \theta(n-1,q^2)$$

orbits of lines under α. The number of orbits of lines which are not lines of Π is

$$\theta(2n-2,q) - \theta(2n-3,q) = q^{2n-2}.$$

The number of orbits of lines of Π is then

$$\frac{q^{2n-2}-1}{q^2-1} = \theta(n-2,q^2).$$

Constructing a parallelism of $\mathrm{PG}(2n-1,q)$ with $n \geq 3$ involves a new problem which did not arise in the construction of parallelisms of $\mathrm{PG}(3,q)$. Essentially, there are two kinds of line-orbits under α: orbits of lines of Π and orbits of lines which are not lines of Π. In dimension 3, there is only one of the former. It is thus trivial to select a collection of pairwise skew representatives of the orbits in the invariant plane; any line of the plane will do. However, in the case $n \geq 2$, the automorphism now has a plurality of line-orbits in the invariant hyperplane and the selection of pairwise

skew representatives is no longer trivial. What follows are two partial solutions, one for each of the two types of line-orbits. Unfortunately, the two solutions together do not form a spread and hence do not furnish a construction of a cyclic parallelism.

Let $\mathbf{F} = \mathrm{GF}(q)$ and let $\mathbf{L}$ be the extension of $\mathbf{F}$ of degree $2n-1$. Regarding $\mathbf{L}$ as an $\mathbf{F}$-vector space, the geometry $\Sigma = \mathrm{PG}(\mathbf{L})$ will serve as the model of $\mathrm{PG}(2n-1,q)$. The elements of $\mathbf{L}$ represent the points of the geometry, with $x, y \in \mathbf{L}^*$ representing the same point if and only if $\frac{y}{x} \in \mathbf{F}^*$. As usual, let N and Tr denote the norm and trace functions of the extension $\mathbf{L}/\mathbf{F}$. Let $G = \ker \mathrm{N}$ and note that $|G| = \theta(2n-1,q)$. Let ω be a primitive element of $\mathbf{L}$ and define $\sigma \in \mathrm{PGL}(\mathbf{L})$ to be determined by the linear map $x \mapsto \omega x$. Note that σ is a Singer cycle of Σ.

Lemma 4.1. *The automorphism σ partitions the lines of Σ into $\frac{q^{2n}-1}{q^2-1}$ orbits each of length $\frac{q^{2n-1}-1}{q-1}$.*

Proof. As the order of σ is $\theta(2n-1,q) = \frac{q^{2n-1}-1}{q-1}$, it suffices to show that there are no short orbits of lines. Suppose $x, y \in \mathbf{L}^*$ represent distinct projective points; that is, $\frac{y}{x} \notin \mathbf{F}$. Suppose further that σ^k fixes the line $x \vee y$ of Σ. With $\alpha = \omega^k$, it follows that for some $a, b, c, d \in \mathbf{F}$, one has

$$\alpha x = ax + by \tag{4.1a}$$

$$\alpha y = cx + dy. \tag{4.1b}$$

As $x \neq 0$, dividing by x results in $\alpha = a + b\frac{y}{x}$. Substituting this expression into equation (4.1b) and again dividing by x results in the equation

$$b\left(\frac{y}{x}\right)^2 + (a-d)\frac{y}{x} - c = 0. \tag{4.2}$$

Since $\frac{y}{x}$ is a root of this quadratic polynomial, $\frac{y}{x} \notin \mathbf{F}$, and $\mathbf{L}$ is an extension of $\mathbf{F}$ of odd degree, it must be that each of the coefficients of the polynomial in equation (4.2) is 0. Therefore, $b = c = 0$ and $\alpha = a = d \in \mathbf{F}$. The result follows as $\alpha \in \mathbf{F}$ if and only if $\theta(2n-2,q) | k$. □

Remark 4.2. If it is further assumed that $(2n-1, q-1) = 1$, then it is the case that the automorphism σ^{q-1} also partitions the set of lines of Σ into $\frac{q^{2n}-1}{q^2-1}$ orbits each of length $\frac{q^{2n}-1}{q-1}$. All that is used to show this fact is that $\langle \omega^{q-1} \rangle \cap \mathbf{F}^* = \{1\}$ under this assumption.

The following construction reduces, upon restriction to the case $q = 2$, to that given by Baker for a partial spread of $\mathrm{PG}(2n-2, 2)$ representing each orbit under the action of a Singer cycle [2]. Define $\nu : \mathbf{L} \times \mathbf{L} \to \mathbf{L}$ by

$$\nu(x, y) = x^q y - x y^q.$$

Let $\mathcal{S} = \{x \vee y \mid \nu(x, y) \in \mathbf{F}^*\}$.

Proposition 4.3. *$\mathcal{S}$ is a partial spread of $\mathrm{PG}(\mathbf{L})$ containing exactly one line from each orbit under σ.*

Proof. Let $x, y \in \mathbf{L}^*$ such that $\frac{y}{x} \notin \mathbf{F}$. It holds that $\nu(x, y) = t \in \mathbf{F}$ if and only if

$$\frac{y}{x} - \left(\frac{y}{x}\right)^q = t x^{-(q+1)}. \tag{4.3}$$

The equation $z - z^q = u$ has solutions in $\mathbf{L}$ if and only if $\mathrm{Tr}(u) = 0$, in which case the solutions are given by

$$z = s + \sum_{k=0}^{2n-3} \xi^{q^k} \sum_{i=0}^{k} u^{q^i}, \quad \text{for } s \in \mathbf{F}, \tag{4.4}$$

where ξ is an element of $\mathbf{L}$ such that $\mathrm{Tr}(\xi) = 1$; see [21, Theorem V 7.6]. Hence, $\nu(x, y) \in \mathbf{F}^*$ if and only if $\mathrm{Tr}(x^{-(q+1)}) = 0$ and $y = sx + tf(x)$ for some $s, t \in \mathbf{F}$, where

$$f(x) = \sum_{k=0}^{2n-3} \xi^{q^k} \sum_{i=0}^{k} x^{1-q^i(q+1)}.$$

That is to say, $\nu(x, y) \in \mathbf{F}^*$ if and only if $\mathrm{Tr}(x^{-(q+1)}) = 0$ and $y \in \mathrm{span}_{\mathbf{F}}\{x, f(x)\}$. Now suppose $\mathcal{S}$ contains two lines, l_1 and l_2, with a common point x. Choose a point

y_i on l_i so that $l_i = \mathrm{span}_{\mathbf{F}}\{x, y_i\}$. By the above, $y_i \in \mathrm{span}_{\mathbf{F}}\{x, f(x)\}$, for $i = 1, 2$. But then $l_1 = l_2$, proving that $\mathcal{S}$ is indeed a partial spread.

It remains to show that for each line PG($\mathbf{L}$) there is some power of σ which maps that line to a line of $\mathcal{S}$. Note that $(x \vee y)\sigma^k = (\omega^k x) \vee (\omega^k y)$. Thus, given any $x, y \in \mathbf{L}^*$ with $\frac{y}{x} \notin \mathbf{F}$, it suffices to show that there exists $\alpha \in \mathbf{L}^*$ such that $\nu(\alpha x, \alpha y) \in \mathbf{F}^*$. But $\nu(\alpha x, \alpha y) = \alpha^{q+1}\nu(x, y)$. Also, $\nu(x, y) \neq 0$ as $x, y \neq 0$ and $\frac{y}{x} \notin \mathbf{F}$. Setting $\alpha = \nu(x, y)^{q\theta(n-2,q^2)}$, one checks that

$$\alpha^{q+1}\nu(x, y) = \nu(x, y)^{1+q\theta(2n-3,q)} = \mathrm{N}\big(\nu(x, y)\big) \in \mathbf{F}^*,$$

as desired. □

Remark 4.4. If $\nu(x, y) \in \mathbf{F}^*$, then the points of the line $x \vee y$ are represented by $\{x + \lambda y \mid \lambda \in \mathbf{F}^\circ\}$. Thus

$$\prod_{\lambda \in \mathbf{F}^\circ} (x + \lambda y) = xy \prod_{\lambda \in \mathbf{F}^*} (x + \lambda y) = x^q y - x y^q \in \mathbf{F}^*.$$

Under the isomorphism $\mathbf{L}^*/\mathbf{F}^* \cong \mathbf{Z}_{\theta(2n-2)}$ determined by $\omega\mathbf{F}^* \mapsto 1$, the lines of Theorem 4.3 are thus the so-called zero-sum base blocks of the associated cyclic difference family in $\mathbf{Z}_{\theta(2n-2)}$.

For the next construction, one must return to odd dimensional projective spaces. The construction applies only to PG($2n - 1, 2$), however. Again, let $\mathbf{F} = \mathrm{GF}(2)$, $\mathbf{L} = \mathrm{GF}(2^{2n-1})$, and let ω be a primitive element of $\mathbf{L}$. As in the previous chapters, set $V = \mathbf{F} \oplus \mathbf{L}$ and define $\sigma : V \to V$ by $(t, x) \mapsto (t, \omega x)$. Let $H = \ker \mathrm{Tr}_{\mathbf{L}/\mathbf{F}}$ and let $\Pi = \{0\} \oplus \mathbf{L}$.

Given a transversal mapping f of H, let $\mathcal{S}(f) = \{l_f(x) \mid x \in \mathbf{F}\}$ where

$$l_f(x) = (0 : x + 1) \vee (1 : f(x)),$$

as in Chapter 3.

Proposition 4.5. *Let $f(x) = x^2 + x$. Then $f \in \mathrm{TM}(H)$ and $\mathcal{S}(f)$ is a set of orbit representatives under $\langle\sigma\rangle$ of the lines of* $\mathrm{PG}(V)$ *which are not contained in* Π.

Proof. It is straightforward to check that f is a transversal mapping of H. Note that $[\mathbf{L} : \mathbf{F}]$ odd implies that $1 \notin H$; this is needed in order that $f(x)$ itself is a permutation.

To see that lines of $\mathcal{S}$ are from different orbits of $\langle\sigma\rangle$, note that

$$\{(0:1) \vee (1:x) \mid x \in H\}$$

is a set of representatives of the orbits under σ which are not contained in Π. Finally, if $x + 1 = \omega^k$, then

$$l_f(x)\sigma^{-k} = (0:1) \vee (1:x),$$

completing the proof. □

It was shown in the proof of Theorem 4.3 that a point of $\Sigma = \mathrm{PG}(\mathbf{L})$ represented by $x \in \mathbf{L}^*$ is on a line of $\mathcal{S}$ if and only if $\mathrm{Tr}(x^{-(q+1)}) = 0$. Note that

$$\mathrm{Tr}(x^{-(q+1)}) = \frac{\mathrm{Tr}(x^{q^2+q^3+\cdots+q^{2n}})}{\mathrm{N}(x)} = \frac{\mathrm{Tr}(x^{1+q+\cdots+q^{2n-2}})}{\mathrm{N}(x)}.$$

Thus, the set of points of $\mathbf{L}^*$ covered by lines of $\mathcal{S}$ is $H\tau^{-1}$, where τ is the automorphism of $\mathbf{L}^*$ given by $x \mapsto x^{1+q+\cdots+q^{2n-4}}$. Note that $H\tau \neq H$. In particular, it is not possible to combine the constructions in Proposition 4.3 and Proposition 4.5 to obtain a spread of $V = \mathbf{F} \oplus \mathbf{L}$ generating a cyclic parallelism of $\mathrm{PG}(V)$.

4.2 Open problems

The following example can be combined with the construction in Proposition 4.3 to obtain a cyclic parallelism of $\mathrm{PG}(5, 2)$.

Example 4.6. Let $\mathbf{L} = \mathrm{GF}(32)$, $\mathbf{F} = \mathrm{GF}(2)$ and let ω be a primitive element of $\mathbf{L}$ satisfying $\omega^5 + \omega^3 + 1 = 0$. Work in $\mathbf{Z}_{31}$ rather than $\mathbf{L}^*$, under the isomorphism

$\rho : \omega \mapsto 1$. Then

$$(\ker \mathrm{Tr})\rho = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}.$$

The following sets are obtained from a spread of $\ker \mathrm{Tr}$ containing one line from each of the five orbits of lines under the Singer cycle $x \mapsto \omega x$:

$$\{1, 3, 29\}, \{2, 6, 27\}, \{4, 12, 23\}, \{8, 24, 15\}, \{16, 17, 30\}.$$

This motivates the following interesting question, which was raised by Fuji-Hara, Jimbo, and Vanstone in [18].

Problem 4.7. Is it possible to partition the lines of $\mathrm{PG}(2n, q)$ into sets each of which is a spread of some hyperplane and so that each hyperplane is partitioned by one of these sets?

Example 4.6 gives a cyclic solution of this problem in $\mathrm{PG}(4, 2)$ and is among those presented in [18]. These authors, with the help of a computer search, find solutions to this problem for $\mathrm{PG}(2n, q)$ with

- $q = 2$ and $n \in \{1, 2, 3, 4, 5\}$,
- $q = 3$ and $n \in \{1, 2, 3\}$.

The examples with $q = 2$ can be combined with the construction in Proposition 4.5 to obtain cyclic parallelisms of $\mathrm{PG}(2n, 2)$, $1 \leq n \leq 5$, which are not equivalent to those constructed by Baker.

Trying to complete the other partial solution of Section 4.1 to a cyclic parallelism raises the next question.

Problem 4.8. Can the construction given in Proposition 4.3 be extended to a cyclic parallelism of $\mathrm{PG}(2n - 1, q)$ for any values of $q > 2$ and $n > 2$?

The smallest case for Problem 4.8 is $\mathrm{PG}(5, 3)$. In this case, one might also try to extend the example of [18] for $\mathrm{PG}(4, 3)$ to a parallelism of $\mathrm{PG}(5, 3)$ by finding an

appropriate transversal mapping of $\ker \mathrm{Tr}_{GF(3^5)/GF(3)}$. As there are 81 orbits of lines which are not contained in the invariant hyperplane of an automorphism with line-orbits of length 121, an exhaustive search is not feasible. A random search based on the method of simulated annealing produced no examples extending either of these sets of lines.

Part II

Singer Subgroup Orbits As Two-Intersection Sets

Chapter 5 Background

The material in this part is based on a joint paper with B. Schmidt, [40]. That paper presents most of these results from the point of view of irreducible cyclic codes; here the presentation is in terms of two-intersection sets. While the problems are essentially equivalent, the geometric language seems more appropriate in light of Part I.

A *two-intersection set* of $\mathrm{PG}(n-1,q)$ is a set of points which is met by every hyperplane in one of two numbers of points. The aim of these investigations is the classification of subgroups of Singer cycles whose point-orbits are two-intersection sets. A basic identity due to McEliece relates the sizes of the hyperplane intersections with Singer subgroup orbits to certain linear combinations of Gauss sums via the Fourier transform. Parseval's identity for Fourier transforms and Stickelberger's Theorem on the prime ideal factorization of Gauss sums suffice to establish "simple" numerical conditions on the parameters of these orbits which are necessary and sufficient for the orbits to be two-intersection sets. Finally, a classification of two-intersection sets which are orbits of subgroups of Singer cycles is conjectured; the classification is based upon classifying the corresponding solutions to the necessary numerical conditions.

5.1 Definitions and equivalent problems

Definition 5.1. A subset X consisting of h points of $\mathrm{PG}(m-1,q)$ such that every hyperplane meets X in h_1 or h_2 points is called a *projective* (h,m,h_1,h_2) *set.* Other common terms for X are a *set of type* (h_1,h_2) or *projective two-intersection set.*

Here are several common examples of two-intersection sets in projective planes.

Example 5.2. Any subspace of $\mathrm{PG}(m-1,q)$ is a two-intersection set. Indeed, a dimension k subspace is either contained in a hyperplane, or else is met by a hyperplane

in a dimension $k-1$ subspace. Thus, a dimension k subspace is a set of type

$$\left(\frac{q^k-1}{q-1}, \frac{q^{k-1}-1}{q-1}\right).$$

Example 5.3. A *Baer subplane* of $\mathrm{PG}(2,q^2)$ is a set of q^2+q+1 points met by each line in 1 or $q+1$ points. This set of points, together with the lines incident with $q+1$ of its points, forms a projective plane of order q. One obtains an example of such a set by considering the $\mathrm{GF}(q)$-subspace of $V(3,q^2)$ consisting of vectors whose coordinates each live in $\mathrm{GF}(q)$.

Example 5.4. The singular points of a nondegenerate Hermitian form on $\mathrm{PG}(2,q^2)$ is an example of a set of q^3+1 points met by each line in either 1 or $q+1$ points. Such sets are called *unitals*; those arising in this manner from a Hermitian form are called *Hermitian*, or *classical, unitals.*

Example 5.5. An *oval* of $\mathrm{PG}(2,q)$ is a set of $q+1$ points, no three of which are collinear. An example of an oval is a nondegenerate quadric. If q is even, then the tangents to an oval are coincident with a point called the *nucleus* of the oval. Together, an oval and its nucleus form a $(q+2)$-set of type $(0,2)$ called a *hyperoval.*

Let σ be a Singer cycle of $\mathrm{PG}(m-1,q)$. It turns out that the sets described in Examples 5.2 and 5.3 can sometimes arise as an orbit under a subgroup of $\langle\sigma\rangle$. It will shortly been seen that orbits of subgroups of Singer cycles are good candidates for examples of sets with few intersection numbers. The idea to consider these Singer subgroup orbits as a source of such examples for isn't particularly new; see [4], for example. What is new is the main result of the next chapter which characterize the parameters of those Singer subgroup orbits which are two-intersection sets. Before proceeding further, some notation is needed.

Let $q=p^t$ for some prime p and some $t\in\mathbf{Z}_+$. Let $\mathbf{F}=\mathrm{GF}(q)$ and let $\mathbf{L}=\mathrm{GF}(q^m)$. Let Σ denote the geometry $\mathrm{PG}(\mathbf{L})$, which will serve as the model of $\mathrm{PG}(m-1,q)$. The points of Σ are then of the form $x\mathbf{F}$, for $x\in\mathbf{L}^*$. Two elements $x,y\in\mathbf{L}^*$ represent

the same projective point if and only if $\frac{x}{y} \in \mathbf{F}^*$. For $\alpha \in \mathbf{L}^*$ let

$$H_\alpha = \{x \in \mathbf{L} \mid \mathrm{Tr}_{\mathbf{L}/\mathbf{F}}(\alpha x) = 0\}.$$

The collection $\{H_\alpha \mid \alpha \in \mathbf{L}^*\}$ is then the set of hyperplanes of Σ. Note that if $x = \lambda y$ with $\lambda \in \mathbf{F}^*$ then $H_x = H_y$. Finally, let $\sigma \in \mathrm{PGL}(\mathbf{L})$ be determined by the linear map $x \mapsto \omega x$, where ω is a primitive element of $\mathbf{L}$. Thus σ is a Singer cycle of Σ.

The order of σ is $(q^m - 1)/(q - 1)$. The main problem is the determination of conditions on the parameters q, m, u so that the orbits under the subgroup $\langle \sigma^u \rangle$ of index u in $\langle \sigma \rangle$ are two-intersection sets. Suppose u divides $(q^m - 1)/(q - 1)$ and let U be the subgroup of $\mathbf{L}^*$ of index u. Set

$$s(q, m, u) = \{x\mathbf{F} \mid x \in U\},$$

a collection of points of Σ. Note that ω^u generates U and that $\mathbf{F}^* < U$. Thus, $s(q, m, u)$ is an orbit under the action of $\langle \sigma^u \rangle$.

Let $h(\alpha) = |\{x\mathbf{F} \mid x \in H_\alpha \cap U\}|$, the number of points of $s(q, m, u)$ incident with the hyperplane H_α.

Proposition 5.6. $h(\alpha) = \frac{1}{q-1}|H_1 \cap (\alpha U)|$.

Proof. Simply note that $H_1 \cap (\alpha U) = H_\alpha \cap U$. Also, $x \in H_\alpha \cap U$ if and only if $\lambda x \in H_\alpha \cap U$ for $\lambda \in \mathbf{F}^*$, as H_α is an $\mathbf{F}$-subspace of $\mathbf{L}$ and $U < \mathbf{L}^*$. □

Here is a simple but important corollary. It explains why the sets $s(q, m, u)$ are good candidates for sets with few intersection numbers, motivating in part these investigations.

Corollary 5.7. *The number of distinct values of the hyperplane intersection function h is at most the number of orbits of $x \mapsto px$ on $\mathbf{Z}_u$.*

Proof. The field automorphism $x \mapsto x^p$ acts on each subgroup of $\mathbf{L}^*$, hence $U^p = U$.

Also, $\mathrm{Tr}_{\mathbf{L}/\mathbf{F}}(x^p) = \mathrm{Tr}_{\mathbf{L}/\mathbf{F}}(x)^p$, so $H_1^p = H_1$. Therefore,

$$h(\alpha^p) = \frac{1}{q-1}|H_1 \cap \alpha^p U| = \frac{1}{q-1}|H_1 \cap \alpha U| = h(\alpha).$$

As $h(a) = h(ax)$ for every $x \in U$, it follows that h can be regarded as a function on $\mathbf{L}^*/U \cong \mathbf{Z}_u$. □

The rest of this section is devoted to a brief description of two problems which are equivalent to the one considered so far.

5.1.1 Two-weight irreducible cyclic codes

For the necessary terminology from coding theory, see [42].

Definition 5.8. Let f be an irreducible divisor of $x^n - 1$ over GF(q) where $(q, n) = 1$. The cyclic code of length n over GF(q) generated by $(x^n - 1)/f$ is called a *minimal cyclic code* or an *irreducible cyclic code.*

The following definition is narrower, but essentially equivalent to Definition 5.8, see Remark 5.10 below. It will prove to be more useful in understanding the correspondence between these codes and projective two-intersection sets.

Definition 5.9. Let $\mathbf{L}/\mathbf{F}$ be an extension of finite fields of degree m where $\mathbf{F}$ has order q. Let n be a divisor of $q^m - 1$, write $u = (q^m - 1)/n$, and let ω be a primitive nth root of unity in $\mathbf{L}$. Define

$$c(q, m, u) := \left\{ c(y) := \left(\mathrm{Tr}_{\mathbf{L}/\mathbf{F}}(y\omega^i)\right)_{i=0}^{n-1} \;\middle|\; y \in L \right\}.$$

$c(q, m, u)$ is called an *irreducible cyclic code* over $\mathbf{F}$.

It can be shown that the dimension of $c(q, m, u)$ is $\mathrm{ord}_n(q)$, cf. [42, Thm. 6.3.1].

Remark 5.10. If ω is allowed to be an arbitrary nth root of unity in Definition 5.9, then by the argument of [42, Thm. 6.5.1], the two definitions above would be equivalent. However, in the case where ω is a non-primitive nth root of unity, the

codewords of $c(q, m, u)$ are periodic with period $\mathrm{ord}(\omega)$. Thus it suffices to consider the case where ω is a *primitive* nth root of unity.

Definition 5.11. Let $w(y)$ denote the Hamming weight, or number of nonzero coordinates, of $c(y) \in c(q, m, u)$. If w takes at most two nonzero values, $c(q, m, u)$ is called a *two-weight irreducible cyclic code.*

Important contributions to the determination of the weight distributions of irreducible cyclic codes can be found in [5, 7, 24, 31]. In general, this is a very difficult problem. Even the two-weight irreducible cyclic codes have not yet been classified.

The following simple fact establishes the equivalence of two-weight irreducible cyclic codes and cyclic two-intersection sets.

Proposition 5.12. *Let σ be a Singer cycle of* $\mathrm{PG}(m-1, q)$ *and suppose u divides* $(q^m - 1)/(q - 1)$. *Then the irreducible cyclic code $c(q, m, u)$ has at most two nonzero weights if and only if each orbit under $\langle \sigma^u \rangle$ on the points of* $\mathrm{PG}(m-1, q)$ *is a two-intersection set.*

Proof. The definitions of the functions w and h immediately imply that

$$w(a) = \frac{q^m - 1}{u} - (q-1)h(a).$$

□

5.1.2 Sub-difference sets

Recall that a (v, k, λ)-*difference set* in a finite group $\mathcal{G}$ of order v is a k-subset D of $\mathcal{G}$ such that every element $g \neq 1$ of $\mathcal{G}$ has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. The parameter $k - \lambda$ is called the order of D. For a detailed treatment of difference sets, see [8].

Let $\mathbf{L}$ and $\mathbf{F}$ be as before and let $\mathcal{G} = \mathbf{L}^*/\mathbf{F}^*$. It is a well-known fact that $L_0 = \{x\mathbf{F}^* \in \mathcal{G} \mid \mathrm{Tr}_{\mathbf{L}/\mathbf{F}}(x) = 0\}$ is a difference set in $\mathcal{G}$ with parameters

$$(v, k, \lambda) = \left(\frac{q^m - 1}{q-1}, \frac{q^{m-1} - 1}{q-1}, \frac{q^{m-2} - 1}{q-1} \right),$$

called the *Singer* or *trace zero* difference set.

The following observation is basically due to McFarland [32].

Proposition 5.13. *Let D be a (v, k, λ)-difference set in a group G, and let N be a normal subgroup of G. If $|D \cap Ng| \in \{a, b\}$ for some nonnegative integers a, b and all $g \in G$, then*

$$E := \{Ng : |D \cap Ng| = a\}$$

is a difference set in G/N.

In the situation of Proposition 5.13, call E a *sub-difference set* of D in G/N. It is straightforward to prove the following.

Corollary 5.14. *Let q be a power of a prime p, let $\mathbf{F} = \mathrm{GF}(q)$ and let $\mathbf{L} = \mathrm{GF}(q^m)$. Let $U < \mathbf{L}^*$ of index u. Finally, let L_0 be the Singer difference set of $\mathcal{G} = \mathbf{L}^*/\mathbf{F}^*$. The set $s(q, m, u)$ is a two-intersection set in $\mathrm{PG}(\mathbf{L})$ if and only if L_0 has a sub-difference set E in $\mathcal{G}/(U/\mathbf{F}^*) \cong \mathbf{L}^*/U$. Furthermore, p is a multiplier of E.*

5.2 The role of Gauss sums

An identity of McEliece [31] expresses the weights of irreducible cyclic codes as linear combinations of Gauss sums. Under the correspondence discussed in Section 5.1.1, an analogous result holds for orbits of powers of Singer cycles and their hyperplane intersection numbers.

Before stating the result, the definition of a Gauss sum is recalled, along with one very basic fact. For a proof, see [26, Thm. 5.11]. The notation $\xi_t = e^{2\pi i/t}$ will be used.

Definition 5.15. Let $r = p^a$ be a prime power, $F = \mathrm{GF}(r)$, and let χ be a character of F^*. We define

$$G_F(\chi) := \sum_{x \in F} \chi(x) \xi_p^{\mathrm{Tr}(x)}$$

where Tr denotes the absolute trace map from F to $GF(p)$.

Lemma 5.16. *If χ is nontrivial, then*

$$|G_F(\chi)|^2 = r.$$

The following is essentially McEliece's identity from [31]. Here it has been translated into the geometric language from the language of irreducible cyclic codes. For the convenience of the reader, a proof is included.

Lemma 5.17 (McEliece). *Let $\mathbf{L}/\mathbf{F}$ be an extension of finite fields of degree m where $\mathbf{F} = \mathrm{GF}(q)$. Let u be a divisor of $(q^m - 1)/(q - 1)$. Let U be the subgroup of $\mathbf{L}^*$ of index u and let Γ be the subgroup of characters of $\mathbf{L}^*$ which are trivial on U. For $a \in \mathbf{L}^*$, the number of points of $s(q, m, u)$ incident with H_α is given by*

$$h(a) = \frac{1}{u}\left(\frac{q^{m-1} - 1}{q - 1} + \frac{1}{q}\sum_{\chi \in \Gamma \setminus \{1\}} G_{\mathbf{L}}(\chi)\overline{\chi}(a)\right); \tag{5.1}$$

for $\chi \in \Gamma \setminus \{1\}$,

$$G_L(\chi) = q\sum_{a \in \mathbf{L}^*/U} h(a)\chi(a). \tag{5.2}$$

Proof. Note that (5.1) follows from (5.2) by Fourier inversion, see Lemma 5.27 of the Section 5.3, and the fact that

$$\sum_{a \in \mathbf{L}^*/U} h(a) = \frac{q^{m-1} - 1}{q - 1}.$$

Using Lemma 5.25 of Section 5.3, one obtains

$$\begin{aligned}
G_{\mathbf{L}}(\chi) &= \sum_{x\in\mathbf{L}^*} \chi(x)\xi_p^{\mathrm{Tr}(x)} \\
&= \sum_{a\in\mathbf{L}^*/U} \chi(a) \sum_{x\in U} \xi_p^{\mathrm{Tr}(ax)} \\
&= \sum_{a\in\mathbf{L}^*/U} \chi(a)\Big(\sum_{x\in U\cap H_a} \xi_p^{\mathrm{Tr}(ax)} + \sum_{x\in U\setminus H_a} \xi_p^{\mathrm{Tr}(ax)}\Big) \\
&= \sum_{a\in\mathbf{L}^*/U} \chi(a)\Big(|U\cap H_\alpha| - \frac{|U\setminus H_\alpha|}{q-1}\Big) \\
&= \sum_{a\in\mathbf{L}^*/U} \chi(a)\Big(qh(a) - \frac{q^m-1}{u(q-1)}\Big) \\
&= q\sum_{a\in\mathbf{L}^*/U} h(a)\chi(a)
\end{aligned}$$

□

Remark 5.18. With $U = \mathbf{F}^*$ above, one has $h(a) = 1$ if $a \in H_1$ and $h(a) = 0$ otherwise. Hence,

$$G_{\mathbf{L}}(\chi) = q\chi(L),$$

where L is the Singer difference set in $\mathbf{L}^*/\mathbf{F}^*$. This result, relating character values of the Singer difference set to Gauss sums, is due to Yamamoto [46],[17].

Corollary 5.19. *Suppose p is prime and u divides $(p^{mt}-1)/(p-1)$. Then $s(p^t,m,u)$ is a two-intersection set in* $\mathrm{PG}(m-1,q)$ *if and only if $s(p,mt,u)$ is a two-intersection set in* $\mathrm{PG}(mt-1,p)$.

Proof. By equation (5.1), there are exactly two distinct hyperplane intersection numbers if and only if the map

$$a \mapsto \sum_{\chi\in\Gamma\setminus\{1\}} G_{\mathbf{L}}(\chi)\bar{\chi}(a)$$

is two-valued. Simply note that this sum depends only on the field $\mathbf{L}$ and u, parameters which are the same for $s(p^t,m,u)$ and $s(p,mt,u)$. □

Remark 5.20. In view of Corollary 5.19, for the classification of which sets $s(q, m, u)$ are two-intersection sets, it is enough to consider the case where q is prime. Of course, it is always assumed that u divides $(q^m - 1)/(q - 1)$.

The following are some facts concerning Gauss sums which will be needed later. A well known result of Stickelberger [41] completely determines the factorization of Gauss sums into prime ideals. As a preparation for the formulation of Stickelberger's theorem, it is worth recalling the factorization of rational primes in certain cyclotomic fields. A proof of this result can be found in [22, pp. 196-198]. Let φ denote the Euler totient function.

Result 5.21. *Let p be a prime and $q = p^f$. Then p factors in $\mathbf{Q}(\xi_{q-1})$ as*

$$(p) = \prod_{i=1}^{t} \pi_i,$$

where $t = \varphi(q-1)/f$ and the π_i are prime ideals. Furthermore, in $\mathbf{Q}(\xi_{q-1}, \xi_p)$, each π_i is the $(p-1)$th power of a prime ideal.

The next result is known as Stickelberger's theorem. For a proof, see [45, Prop. 6.13]. For a positive integer x, let $S_p(x)$ denote the sum of the p-digits of x.

Result 5.22. *Let p be a prime, and $q = p^a$ be a power of p. Let π be a prime ideal of $\mathbf{Q}(\xi_{q-1})$ above p, let $\tilde{\pi}$ be the prime ideal of $\mathbf{Q}(\xi_{q-1}, \xi_p)$ above π. Let $\nu_{\tilde{\pi}}$ denote the $\tilde{\pi}$-adic evaluation. Let $\omega = \omega(\pi)$ be the Teichmüller character of $\mathrm{GF}(q)^*$ corresponding to π (see* [45, p. 96] *for the definition of ω). Then*

$$\nu_{\tilde{\pi}}(G(\omega^j)) = S_p(j)$$

for $1 \leq j < q - 1$.

The final background result is the Daveport-Hasse Theorem, see [26, Thm. 5.14], concerning values of Gauss sums relative to field extensions.

Result 5.23. *Let r be a prime power and let $\mathbf{E}$ be an extension field of $\mathbf{F} = \mathrm{GF}(r)$ of degree s. Let χ be a character of $\mathbf{F}^*$ and define a character χ' of $\mathbf{E}^*$ by $\chi'(x) = \chi(\mathrm{N}_{\mathbf{E}/\mathbf{F}}(x))$ where $\mathrm{N}_{\mathbf{E}/\mathbf{F}}$ denotes the norm function of $\mathbf{E}$ relative to $\mathbf{F}$. Then*

$$G_{\mathbf{E}}(\chi') = (-1)^{s-1} G_{\mathbf{F}}(\chi)^s.$$

The above results yield the following corollary which will prove to be quite useful in later analysis.

Corollary 5.24. *Let p be a prime u be a positive integer with $(u,p) = 1$. Write $f := ord_u(p)$. Define*

$$\theta(u,p) := \frac{1}{p-1} \min\{S_p(\tfrac{j(p^f-1)}{u}) \mid 1 \le j < u\}.$$

Let s be a positive integer. If u divides $(p^{sf}-1)/(p-1)$, then $p^{s\theta(u,p)}$ is the largest p-power dividing $G(\chi)$ for every nontrivial character χ of $\mathrm{GF}(p^{sf})^*$ such that χ^u is trivial.

Proof. By (5.2), $G(\chi) \in Z[\xi_u]$. Thus Stickelberger's theorem and Result 5.21 imply that $\theta(u,p)$ is an integer. Now the assertion follows from Stickelberger's theorem together with the Davenport-Hasse theorem. □

5.3 Appendix: Fourier analysis

This appendix lists some very basic facts about Fourier analysis on finite abelian groups. See [29] for proofs. For an abelian group G, let $\hat{G}$ denote its character group, and for a subgroup W of G, write $W^\perp$ for the subgroup of all characters which are trivial on W. Identify G with $\hat{\hat{G}}$ by $g \leftrightarrow \tau_g$ where τ_g is the character of $\hat{G}$ with $\tau_g(\chi) = \overline{\chi(g)}$. The following *orthogonality relations* are extremely useful.

Lemma 5.25. *Let G be an abelian group, let U be a subgroup of G, and let W be a subgroup of $\hat{G}$. Then*

(a) $\sum_{g \in U} \chi(g) = 0$ *for all* $\chi \in \hat{G} \setminus U^{\perp}$; *and*

(b) $\sum_{\chi \in W} \chi(g) = 0$ *for all* $g \in G \setminus W^{\perp}$.

As a consequence of the orthogonality relations, one gets the so-called *Fourier inversion formula.*

Lemma 5.26. *Let* G *be an abelian group, and let* $A = \sum_{g \in G} a_g g \in \mathbf{Z}[G]$. *Then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(Ag^{-1})$$

for all $g \in G$.

Sometimes it is convenient to express Lemma 5.26 in terms of Fourier transforms. Let G be an abelian group, and let $f : G \to \mathbf{C}$ be a function, where $\mathbf{C}$ is the field of complex numbers. The *Fourier transform* of f is a function $\hat{f} : \hat{G} \to \mathbf{C}$ defined by

$$\hat{f}(\chi) = |G|^{-\frac{1}{2}} \sum_{g \in G} f(g)\chi(g).$$

Lemma 5.27. *Let* G *be an abelian group, and let* $f : G \to \mathbf{C}$. *Then* $\hat{\hat{f}} = f$.

One consequence of Lemma 5.26, is *Parseval's identity.* Note that $\sum_{g \in G} |f(g)|^2$ is the coefficient of 1 in $AA^{(-1)}$ if we let $A = \sum_{g \in G} f(g)g$.

Lemma 5.28. *Let* G *be an abelian group, and let* $f : G \to \mathbf{C}$ *be a function. Then*

$$\sum_{g \in G} |f(g)|^2 = \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^2.$$

Chapter 6 Necessary and Sufficient Conditions

The main result of this chapter gives necessary and sufficient conditions in order that orbits under a subgroup of a Singer cycle are two-intersection sets. In addition to furnishing a computationally more efficient method to determine if an orbit $s(q, m, u)$ is a two-intersection set, these conditions also furnish a method for classifying the resulting two-intersection sets according to properties of the corresponding solutions to the necessary equations. The two known infinite families of two-intersection sets which are of the form $s(q, m, u)$ can be identified among all solutions to the necessary equations, leaving what is conjectured to be a small list of exceptions.

6.1 The main result

In light of Remark 5.20, it suffices to consider the sets $s(p, m, u)$, where p is prime.

Theorem 6.1. *Let p be a prime, and let u, m be positive integers such that u divides $(p^m - 1)/(p - 1)$. Let θ denote $\theta(u, p)$, let $f = ord_u(p)$, and let $fs = m$. Then $s(p, m, u)$ is a two-intersection set in Σ if and only if there exists a positive integer k satisfying*

$$k \mid u - 1 \tag{6.1a}$$

$$kp^{s\theta} \equiv \pm 1 \pmod{u} \tag{6.1b}$$

$$k(u - k) = (u - 1)p^{s(f-2\theta)}. \tag{6.1c}$$

Proof. As usual, $\mathbf{L}$ denotes GF(p^m). Let U be the subgroup of $\mathbf{L}^*$ of index u and let Γ be the subgroup of characters of $\mathbf{L}^*$ which are trivial on U. Let $G = \mathbf{L}^*/U$.

Necessity. Define $\nu(a) = p(h(a) - h(1))$. Note that ν, like h, may be considered as a function on G. Also note that $\Gamma \cong \hat{G}$.

As

$$\sum_{a \in G} h(a) = \frac{1}{p-1}|H| = \frac{p^{sf-1}-1}{p-1},$$

it holds that

$$\hat{\nu}(\chi) = \frac{p(p^{sf-1}-1)}{\sqrt{u}(p-1)} - pu^{\frac{1}{2}}h(1), \quad \text{by Lemma 5.25} \tag{6.2a}$$

$$= u^{-\frac{1}{2}}G_{\mathbf{L}}(\chi), \quad \text{by Lemma 5.17.} \tag{6.2b}$$

Now suppose $s(p, m, u)$ is a two-intersection set. Then there exists some nonzero integer δ such that $\nu(a) \in \{0, \delta\}$ for all $a \in G$. For $\chi \in \Gamma \setminus \{1\}$, it was just seen that

$$G_{\mathbf{L}}(\chi) = \sum_{a \in G} \nu(a)\chi(a). \tag{6.3}$$

As δ divides $\nu(a)$ for each $a \in G$, then δ divides the right side of equation (6.3) in the ring $\mathbf{Z}[\xi_u]$. Thus, δ divides $G_{\mathbf{L}}(\chi)$ in $\mathbf{Z}[\xi_u]$ for each $\chi \in \Gamma \setminus \{1\}$. By Lemma 5.16 and Corollary 5.24,

$$\delta = p^e \text{ for some } e \leq s\theta. \tag{6.4}$$

On the other hand, equation (5.1) of Lemma 5.17 implies that for each $a \in G$,

$$u\nu(a) = \sum_{\chi \in \Gamma \setminus \{1\}} G_{\mathbf{L}}(\chi)\big(\bar{\chi}(a) - 1\big). \tag{6.5}$$

Recall that $p^{s\theta} | G_{\mathbf{L}}(\chi)$ in $\mathbf{Z}[\xi_u]$ for every $\chi \in \Gamma \setminus \{1\}$, by Corollary 5.24. Therefore, as $(u, p) = 1$, it follows that $p^{s\theta} | \nu(a)$ in $\mathbf{Z}[\xi_u]$ for every $a \in G$. Hence, $p^{s\theta}$ divides δ. Combine this fact with equation (6.4) to obtain $\delta = \pm p^{s\theta}$.

Next, define $D = \{a \in G \mid \nu(a) = \delta\}$; $d = |D|$. Thus,

$$\hat{\nu}(1) = u^{-\frac{1}{2}} \sum_{a \in G} \nu(a) = \pm dp^{s\theta} u^{-\frac{1}{2}}.$$

Comparing this with the previous expression for $\hat{\nu}(1)$ given in equation (6.2), one obtains

$$dp^{s\theta} \equiv \pm 1 \pmod{u}.$$

Finally, Parseval's identity applied to the function ν yields

$$dp^{2s\theta} = \frac{d^2 p^{2s\theta}}{u} + \frac{(u-1)p^{sf}}{u},$$

by Lemma 5.16. This expression simplifies to

$$d(u-d) = (u-1)p^{s(f-2\theta)}.$$

If $f = 2\theta$, take $k = u - 1$. Otherwise, p divides exactly one of d and $u - d$; the other must divide $u - 1$. Take k equal to the latter.

Sufficiency. Suppose conditions (6.1) hold. Let

$$x = \frac{p^{sf} - 1}{u(p-1)} - \frac{p^{s\theta-1}(p^{s(f-\theta)} - \varepsilon k)}{u}, \tag{6.6}$$

where $\varepsilon \in \{\pm\}$ is determined by (6.1b) so that

$$\varepsilon k p^{s\theta} \equiv 1 \pmod{u}. \tag{6.7}$$

Define

$$\gamma(a) = \frac{h(a) - x}{p^{s\theta-1}}.$$

It is claimed that $\gamma(a) \in \mathbf{Z}$ for every $a \in G$. Note that

$$\gamma(a) = \frac{uh(a) - \frac{p^{sf}-1}{p-1}}{up^{s\theta-1}} + \frac{p^{s(f-\theta)} - \varepsilon k}{u}. \tag{6.8}$$

By equation (6.7) and the fact that $p^{sf} \equiv 1 \pmod{u}$, it follows that u divides $\left(p^{s(f-\theta)} - \varepsilon k\right)$. Next, note that by equation (5.1)

$$uh(a) - \frac{p^{sf}-1}{p-1} = \frac{p^{sf-1}-1}{p-1} + \frac{1}{p}\left(\sum_{\chi \in \Gamma \setminus \{1\}} G_{\mathbf{L}}(\chi)\bar{\chi}(a)\right) - \frac{p^{sf}-1}{p-1} \tag{6.9a}$$

$$= -p^{sf-1} + \frac{1}{p}\sum_{\chi \in \Gamma \setminus \{1\}} G_{\mathbf{L}}(\chi)\bar{\chi}(a). \tag{6.9b}$$

Since u divides $uh(a) - \frac{p^{sf}-1}{p-1}$ and $(u,p) = 1$, it remains only to show that $p^{s\theta-1}$ divides $uh(a) - \frac{p^{sf}-1}{p-1}$. This fact follows from equation (6.9), since $f > \theta$, and also from the fact that $p^{s\theta}$ divides $G_{\mathbf{L}}(\chi)$ for every $\chi \in \Gamma \setminus \{1\}$, by Corollary 5.24. Hence, the function γ is integer-valued.

Since $\sum_{a \in G} h(a) = (p^{sf}-1)/(p-1)$ then

$$\sum_{a \in G} \gamma(a) = \frac{p^{sf-1}-1}{p^{s\theta-1}(p-1)} - \frac{p^{sf}-1}{p^{s\theta-1}(p-1)} + p^{s(f-\theta)} - \varepsilon k \tag{6.10a}$$

$$= -\varepsilon k. \tag{6.10b}$$

Hence, $\hat{\gamma}(1) = -\varepsilon k u^{-\frac{1}{2}}$. For $\chi \in \Gamma \setminus \{1\}$,

$$\hat{\gamma}(\chi) = \frac{\hat{h}(\chi)}{p^{s\theta-1}} = \frac{G_{\mathbf{L}}(\chi)}{p^{s\theta}u^{-\frac{1}{2}}}.$$

Applying Parseval's identity results in

$$\sum_{a \in G} \gamma(a)^2 = \frac{k^2}{u} + \frac{(u-1)p^{s(f-2\theta)}}{u}.$$

As it is assumed that $k(u-k) = (u-1)p^{s(f-2\theta)}$, it follows that

$$\sum_{a \in G} \gamma(a)^2 = k.$$

Since γ is integer-valued, then $\gamma(a) \in \{0, -\varepsilon\}$ for every $a \in G$. Thus, $s(p,m,u)$ is met by hyperplanes of Σ in one of two numbers of points. $\square$

Corollary 6.2. *Suppose the set $s(p,m,u)$ is a two-intersection set of Σ. With k and ε as in Theorem 6.1, the hyperplanes meet $s(p,m,u)$ in one of the following numbers of points:*

$$h_1 = \frac{p^{sf}-1}{u(p-1)} - \frac{p^{s\theta-1}(p^{s(f-\theta)}-\varepsilon k)}{u},$$
$$h_2 = h_1 - \varepsilon p^{s\theta-1}.$$

6.2 On the classification

Theorem 6.1 can be used to classify those two-intersections sets arising as orbits under subgroups of Singer cycles by classifying the corresponding solutions of (6.1). In the following, only the sets $s(p,m,u)$ with p prime are considered; see Remark 5.20.

6.2.1 Subspaces and semiprimitive sets

There are two known infinite families of two-intersection arising as orbits under subgroups of Singer cycles: the subspaces and the semiprimitive sets. The corresponding solutions of (6.1) are described in this section.

The most obvious two-intersection sets of the form $s(p,m,u)$ arise if the index u subgroup of $\mathbf{L}^*$ is the multiplicative group a subfield of $\mathbf{L}$, see Example 5.2. U is the multiplicative group of a subfield $\mathbf{K} \cong \mathrm{GF}(p^a)$ of $\mathbf{L} = \mathrm{GF}(p^m)$ if and only if $u = (p^m-1)/(p^a-1)$ for some $a|m$. From the proof of Theorem 6.1, one can see that $k = (p^{m-a}-1)/(p^a-1)$ in (6.1) and thus $\theta(u,p) = a$ for a subspace of the form $s(p,m,u)$.

Proposition 6.3. *The subspaces which arise as $s(p,m,u)$ exactly correspond to the solutions of* (6.1) *of the form*

$$u = (p^m-1)/(p^a-1)$$
$$k = (p^{m-a}-1)/(p^a-1)$$
$$s = 1.$$

The next class of two-intersection sets arising as orbits under subgroups of Singer cycles is the class of semiprimitive sets. A prime p is called *semiprimitive* modulo u if -1 is power of p modulo u. The orbit $s(p, m, u)$ will be called a *semiprimitive set* if p is semiprimitive modulo u. Note that (6.1) has a solution with $k \in \{1, u-1\}$ if and only if $\theta(u,p) = f/2$. By [6, Thms. 1,4], $\theta(u,p) = f/2$ if and only if p is semiprimitive modulo u, giving the following result.

Proposition 6.4. *There is a solution of* (6.1) *with* $k \in \{1, u-1\}$ *if and only if* p *is semiprimitive modulo* u.

Remark 6.5. If p is semiprimitive modulo u, then it follows from Corollary 6.2 that the difference of the intersection numbers for the set $s(p, m, u)$ is equal to $p^{\frac{sf}{2}-1}$, the square root of the order of the geometry. In particular, these examples occur only in geometries whose order is a square. Until recently, and aside from the subspace examples, all known two-intersection sets in geometries over fields of odd order shared this property.

6.2.2 The exceptional sets

Those sets $s(p, m, u)$ which are two-intersection sets but do not fall into either the family of subspace sets or the family of semiprimitive sets will be called *exceptional.* The corresponding solutions of (6.1) will also be called *exceptional.* Theorem 6.1 makes possible a computer search for exceptional sets. A search can be conducted as follows. For every proper divisor $k > 1$ of $u-1$, compute $k(u-k)/(u-1)$. If it is a prime power, say p^r, check whether $f - 2\theta$ divides r. If so and the quotient is s, then as long as condition (6.1b) of Theorem 6.1 holds, $s(p, fs, u)$ is a two-intersection set. Table 6.1 lists all exceptional solutions of (6.1) with $u \leq 100,000$.

The two-intersection sets from corresponding to the parameters in Table 6.1 with $u \in \{11, 19, 67, 107, 163, 499\}$ were already found by Langevin [24], although his result is stated in terms of the corresponding irreducible cyclic codes $c(p, m, u)$. His proof relies on the fact that the Gauss sums in McEliece's identity can be evaluated if u is prime and $f = (u-1)/2$. Batten and Dover [4] verified by direct calcu-

u	p	s	f	θ	k	ε
11	3	1	5	2	5	+1
19	5	1	9	4	9	+1
35	3	1	12	5	17	+1
37	7	1	9	4	9	+1
43	11	1	7	3	21	+1
67	17	1	33	16	33	+1
107	3	1	53	25	53	+1
133	5	1	18	8	33	−1
163	41	1	81	40	81	+1
323	3	1	144	70	161	+1
499	5	1	249	123	249	+1

Table 6.1: Exceptional solutions

lation that $s(5, 9, 19)$ and $s(7, 9, 37)$ are two-intersection sets. The author believes that $s(3, 12, 35)$, $s(11, 7, 43)$, $s(5, 18, 133)$ and $s(3, 144, 323)$ are new examples of two-intersection sets.

By Remark 5.20, it was enough to classify two intersection sets in geometries over fields of prime order. However, one can see many more examples from the data in Table 6.1. Indeed, for any parameters (u, p, s, f) in the table, $s(p^t, d, u)$ is a two-intersection set in $\mathrm{PG}(d-1, p^t)$ where $td = sf$ and u divides $(p^{sf}-1)/(p^t-1)$.

Example 6.6. As $5^9 - 1 = 2^2 \cdot 19 \cdot 31 \cdot 829$, then $s(5^3, 3, 19)$ is an 829-set of type $(4, 9)$ in $\mathrm{PG}(2, 5^3)$ and $s(5, 9, 19)$ is a 25,699-set of type $(5074, 5199)$ in $\mathrm{PG}(8, 5)$.

The fact that there are no exceptional solutions with $500 \leq u \leq 100,000$ and the results of the next section provide evidence for the following.

Conjecture 6.7. *An orbit under a subgroup of a Singer cycle, $s(p, m, u)$, is a two-intersection set of* $\mathrm{PG}(m-1, p)$ *if and only if it is a subspace set, a semiprimitive set, or appears in the above table of exceptional sets.*

Remark 6.8. All exceptional sets $s(p, m, u)$ share the interesting property that the difference of the intersection numbers is strictly less than the order of the geometry in which they arise. It is worth noting that $s(5^3, 3, 19)$ and $s(7^3, 3, 37)$ were the first

known examples of two-intersections sets of any kind, not just those arising as orbits under Singer subgroups, in planes whose orders are odd and not square.

Finally, see [40] for a short discussion of the classification in terms of sub-difference sets, as well as for a list of the sub-difference sets arising in $\mathbf{L}^*/U$ for each of the exceptional solutions to the necessary equations. The language of difference sets is perhaps the most satisfying in which to state the classification.

6.3 Partial proof of the classification

This section gives a partial proof of Conjecture 6.7, conditionally on the generalized Riemann hypothesis (GRH). As usual, only the sets $s(p, m, u)$ with p prime are considered; see Remark 5.20.

One of the tools that will be used is a bound on class numbers of imaginary quadratic fields due to Louboutin [27]. Let $\mathbf{K}$ be an imaginary quadratic number field, and let $\zeta_{\mathbf{K}}(s)$ denote its Dedekind zeta function; see [10, p. 309]. Recall that the generalized Riemann hypothesis for $\mathbf{K}$ asserts that $\Re s = 1/2$ for all zeros s of $\zeta_{\mathbf{K}}(s)$ with $0 < \Re s < 1$.

Result 6.9 (Louboutin [27]). *Let d be a square-free positive integer and let $h(-d)$ denote the class number of $\mathbf{K} = \mathbf{Q}(\sqrt{-d})$. Assuming GRH for $\mathbf{K}$, then*

$$h(-d) \geq \frac{\pi\sqrt{d}}{3e \log d}.$$

To prove the following Theorem, Louboutin's bound is combined with work of Baumert and Mykkelveit [7] and recent work of Mbodj [30] on Gauss sums.

Theorem 6.10. *Conditionally on GRH, no two-intersection set in Σ is of the form $s(p, m, u)$ for which the triple (p, m, u) satisfies any of the following conditions.*

(a) $u \equiv 0 \pmod 3$, $u \neq 3$, $p \equiv 1 \pmod 3$ *and*

$$m > \frac{3 \log((u+1)/4)}{\log p}. \tag{6.11}$$

(b) There is a prime divisor $r \equiv 3 \pmod 4$ *of* u *with* $r > 3$,

$$ord_r(p) = (r-1)/2 \tag{6.12}$$

and

$$m > \frac{3e(r-1)\log r \log((u+1)/4)}{2\pi\sqrt{r}\log p}. \tag{6.13}$$

(c) There are two odd prime divisors r, $s > 3$ *of* u *such that*

$$ord_r(p) = r-1,\ ord_{rs}(p) = (r-1)(s-1)/2 \tag{6.14}$$

and

$$m > \frac{3e(r-1)(s-1)\log rs \log((u+1)/4)}{2\pi\sqrt{rs}\log p}. \tag{6.15}$$

Proof. (b) Assume that $s(p,m,u)$ is a two-intersection set. Write $f = \mathrm{ord}_u(p)$, $m = ft$, $g = (r-1)/2$, and let χ be a character of $\mathrm{GF}(p^g)$ of order r. By [7], the exact power of p dividing the Gauss sum $G(\chi)$ is $p^{(g-h)/2}$ where h is the class number of $\mathbf{Q}(\sqrt{-r})$. Thus, by the Davenport-Hasse theorem and Corollary 5.24, $2\theta(u,p) \leq f - hf/g$. Recall that $k(u-k) = (u-1)p^{t(f-2\theta(u,p))}$ for some divisor k of $u-1$ by Theorem 6.1. Note that $k(u-k)/(u-1) \leq (u+1)/4$. Putting this together, one obtains

$$\frac{u+1}{4} \geq p^{t(f-2\theta(u,p))} \geq p^{mh/g}.$$

Now assertion (b) follows by taking logarithms and using Result 6.9.

The proof of part (c) is similar. If $s \equiv 3 \pmod 4$ and $\mathrm{ord}_s(p) = (s-1)/2$ then the bound from part (b), with s in place of r, implies the bound in (c). Otherwise, we may use Proposition 3.8 of [30] applied to a character of $\mathrm{GF}(p^g)$ of order rs in the estimation of $\theta(u,p)$. Here $g = (r-1)(s-1)/2$. Proceed as in part (b).

To prove (a), note that $s_p(\frac{p^f-1}{3}) = f(p-1)/3$. By Corollary 5.24, $t\theta(u,p) \leq m/3$.

As in part (b), the result follows by Theorem 6.1. □

Following Mbodj [30], the pair (u,p) is said to fall under the *index 2 case* if u is odd and $\mathrm{ord}_u(p) = \varphi(u)/2$. Note that u can have at most two distinct prime divisors in this case. The corresponding sets $s(p,m,u)$ will be called *index 2 sets*. Index 2 sets are promising candidates for two-intersection sets because of the following.

Proposition 6.11. *The number of different hyperplane intersection numbers for a set $s(p,m,u)$ is at most the number of orbits of $x \mapsto x^p$ on $\mathbf{Z}_u^*$.*

In particular, an index 2 set with u prime has at most three different nonzero weights. Note that eight of the eleven exceptional two-intersection sets listed in Section 6.2.2 are index 2 sets. Thus it is desirable to verify Conjecture 6.7 for index 2 sets.

Theorem 6.12. *Conditionally on GRH, Conjecture* 6.7 *is true for all index* 2 *sets.*

Proof. Let $\mathcal{S} = s(p,m,u)$ and suppose that $\mathcal{S}$ is a two-intersection index 2 set. If $\mathcal{S}$ is a semiprimitive set, then there is nothing to show. Thus assume that p is not semiprimitive modulo u. First suppose 3 divides u and $p \equiv 1 \pmod 3$. If $u = 3^a s^b$, for a prime $s > 3$, then Theorem 6.10 (a) implies

$$3^{a-1}(s-1)s^{b-1} \leq \frac{3\log((u+1)/4)}{\log p}.$$

Hence,

$$\frac{u\log 7}{12} \leq \log\frac{u+1}{4},$$

a contradiction. The case u is a power of 3 is similar and once again there are no admissible values of u by Theorem 6.10(a).

Next suppose that $(u,3) = 1$. It is claimed that

$$\frac{\pi\sqrt{u}\log p}{3e\log u} \leq \log\frac{u+1}{4}. \tag{6.16}$$

The proof of equation (6.16) will be carried out only for the case where u has two distinct prime divisors r, s. The case where u is a prime power is similar. Write

$u = r^a s^b$ where $a, b \geq 1$. As $\mathrm{ord}_u(p) = \varphi(u)/2$, equation (6.12) or equation (6.14) holds for the pair (u, p). If (6.12) holds, then

$$\frac{r^{a-1}s^{b-1}(s-1)}{2} \leq \frac{3e \log r \log (u+1)/4}{2\pi\sqrt{r} \log p}$$

by Theorem 6.10. If (6.14) holds, then

$$\frac{r^{a-1}s^{b-1}}{2} \leq \frac{3e \log rs \log (u+1)/4}{2\pi\sqrt{rs} \log p}$$

by Theorem 6.10. Each of these implies (6.16).

Note that equation (6.16) implies $u < 86,909$ if $p > 2$. Since the table in Section 6.2 contains all exceptional sets with $u \leq 100,000$, this shows that Theorem 6.12 is true for $p > 2$. If $p = 2$, then (6.16) implies $u < 125,383$. A computer search shows that there are no exceptional sets with $p = 2$ in this range. □

Appendix A Notation

$\mathbf{Z}$	the integers
$\mathbf{Q}$	the rationals
$\mathbf{C}$	the complex numbers
$\mathbf{Z}_n$	the cyclic group of order n
$\mathrm{GF}(q)$	Galois field of order q
$\mathbf{F}^*$	the multiplicative group of nonzero elements of the field $\mathbf{F}$
$\mathbf{F}^\circ$	$\mathbf{F} \cup \{\infty\}$
$V(n, \mathbf{F})$	vector space of dimension n over the field $\mathbf{F}$
$V(n, q)$	$V(n, \mathbf{F})$ with $\mathbf{F} = \mathrm{GF}(q)$
$\mathrm{PG}(V)$	the classical projective geometry of the vector space V
$\mathrm{PG}(n, q)$, Σ_n	$\mathrm{PG}\big(V(n+1, q)\big)$
$\mathrm{PG}^{(k)}(n, q)$, $\Sigma_n^{(k)}$	the set of k-dimensional subspaces of $\mathrm{PG}(n, q)$
$\theta(n, q)$	the number of points of $\mathrm{PG}(n, q)$
$\mathrm{GL}(V)$	the group of nonsingular linear transformations of V
$\Gamma\mathrm{L}(V)$	the group of invertible semilinear transformations of V
$\mathrm{PGL}(V)$	the projective general linear group of V
$\mathrm{P}\Gamma\mathrm{L}(V)$	the projective semilinear group of V

Bibliography

[1] E. F. Assmus, J. D. Key, *Designs and Their Codes*, Cambridge Tracts in Mathematics, 103, Cambridge University Press, 1992.

[2] R. D. Baker, Partitioning the planes of AG$(2m, 2)$ into 2-designs, *Discrete Mathematics* **15** (1976), 205–211.

[3] R. D. Baker, Orthogonal line packings of PG$(2m-1, 2)$, *Journal of Combinatorial Theory, Series A* **36** (1984), 245–248.

[4] L. Batten, J.M. Dover, Some sets of type (m, n) in cubic order planes, *Designs, Codes and Cryptography* **16** (1999), 211-213.

[5] L. D. Baumert, R. J. McEliece, Weights of irreducible cyclic codes, *Information and Control* **20** (1972), 158-175.

[6] L. D. Baumert, W.H. Mills, R.L. Ward, Uniform cyclotomy, *J. Number Theory* **14** (1982), 67-82.

[7] L. D. Baumert, J. Mykkelveit, Weight Distribution of Some Irreducible Cyclic Codes, *D.S.N. report, vol. 11* (1973), 128-131.

[8] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, Cambridge (1986).

[9] A. Beutelspacher, On parallelisms in finite projective spaces, *Geometriae Dedicata* **3** (1974), 35–40.

[10] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, New York/San Francisco/London, 1966.

[11] R. H. Bruck, Construction problems of finite projective planes, *Combinatorial Mathematics and its Applications*, The University of North Carolina Press, 1967, 426–514.

[12] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* **18** (1986), 97-122.

[13] R. H. F. Denniston, Packings of PG$(3, q)$, *Finite Geometric Structures and their Applications* (Bressanone, 1972), Cremonese, 1973, 195–199.

[14] R. H. F. Denniston, Some packings of projective spaces, *Rend. Accad. Naz. Lincei* **52** (1972), 36–40.

[15] R. H. F. Denniston, Cyclic Packings of the projective space of order 8, *Rend. Accad. Naz. Lincei* **54** (1973), 373–377.

[16] A. B. Evans, *Orthomorphism Graphs of Groups*, Lecture Notes in Mathematics 1535, Springer-Verlag, 1992.

[17] R. Evans, H. Hollman, C. Krattenthaler, Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *J. Combin. Theory Ser. A* **87** (1999), 74–119.

[18] R. Fuji-Hara, M. Jimbo, S. Vanstone, Some results on the line partioning problem in PG$(2k, q)$, *Utilitas Mathematica* **30** (1986), 235–241.

[19] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, Oxford University Press, Oxford, 1979.

[20] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, 1985.

[21] T. W. Hungerford, *Algebra*, Springer-Verlag, 1974.

[22] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Math. No. 84. Springer Verlag, Berlin/New York/Heidelberg, 1990.

[23] V. Jha, N. L. Johnson, Regular parallelisms from translation planes, *Discrete Math.* **59** (1986), 91–97.

[24] P. Langevin, A new class of two weight codes, *Finite fields and their applications*(Glasgow, 1995), 181–187, London Math. Soc. Lecture Note Ser., 233, Cambridge Univ. Press, Cambridge, 1996.

[25] R. Lidl, H. Niederreiter, *Finite Fields: Encyclopedia of Mathematics and Its Applications Vol. 20*, Addison-Wesley, 1983.

[26] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Revision of the 1986 first edition. Cambridge University Press, Cambridge, 1994.

[27] S. Louboutin: Minorations (sous l'hypothèse de Riemann généralisée) des nombres de classes des corps quadratiques imaginaires. *Application. C.R. Acad. Sci. Paris Sr. I Math.* **310** (1990), no. 12, 795-800.

[28] G. Lunardon, On regular parallelisms of PG$(3, q)$, *Discrete Math.* **51** (1984), 229–235.

[29] H.B. Mann, *Addition Theorems*, Wiley, New York (1965).

[30] O.D. Mbodj, Quadratic Gauss Sums, *Finite Fields and Their Applications* **4** (1998), 347-361.

[31] R. J. McEliece, Irreducible cyclic codes and Gauss sums. *Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory*, pp. 179–196. Math. Centre Tracts, No. 55, Math. Centrum, Amsterdam, 1974.

[32] R.L. McFarland, Sub-Difference Sets of Hadamard Difference Sets, *J. Combin. Theory A* **54** (1990), 112-122.

[33] E. H. Moore, Tactical Memoranda I-III, *American Journal of Mathematics* **18** (1896), 264–303.

[34] H. Niederreiter, K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A.* **33** (1982), 197–212.

[35] T. Ostrom, Derivable Nets, *Canadian Mathematical Bulletin* **8** (1965), 601–13.

[36] T. Pentilla and B. Williams, Regular Packings of PG3q, *Euro. J. Comb.* **19**,713–720.

[37] A. R. Prince, Uniform parallelisms of PG(3, 3), *Geometry, Combinatorial Designs and Related Structures*, London Mathematical Society Lecture Note Series 245, Cambridge University Press, 1996, 193–200.

[38] A. R. Prince, The Cyclic Parallelisms of PG(3, 5), *Euro. J. Comb.* **19** (1998), 613–616.

[39] A. R. Prince, Parallelisms of PG(3, 3) Invariant Under a Collineation of Order 5, *Mostly Finite Geometries*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, 1997, 383–390.

[40] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, *Finite Fields and Their Applications*, to appear.

[41] L. Stickelberger, Über eine Verallgemeinerung der Kreistheilung, *Math. Annalen* **37** (1890), 321-367.

[42] J. H. van Lint, *Coding Theory*, Lecture Notes in Mathematics, No. 201. Springer-Verlag, Berlin/Heidelberg/New York, 1971.

[43] J. H. van Lint, R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1992.

[44] D. Wan, On a problem of Niederreiter and Robinson, *J. Austral. Math. Soc. Ser. A.* **41** (1986), 336–38.

[45] L.C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. No. 83. Springer Verlag, Berlin/New York/Heidelberg, 1997.

[46] K. Yamamoto, On congruences arising from relative Gauss sums, *Number Theory and Combinatorics*, Japan 1984, World Scientific Publ., 1985, 423–446.