THE SMITH NORMAL FORMS OF DESIGNS WITH CLASSICAL PARAMETERS

by

David Blanchard Chandler

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

Summer 2004

© 2004 David Blanchard Chandler
All Rights Reserved

THE SMITH NORMAL FORMS OF DESIGNS WITH CLASSICAL PARAMETERS

by

David Blanchard Chandler

Approved: _____

Philip Broadbridge, Ph.D.
Chairman of the Department of Mathematical Sciences

Approved: _____

Mark W. Huddleston, Ph.D.
Dean of the College of Arts and Sciences

Approved: _____

Conrado M. Gempesaw II, Ph.D.
Vice Provost for Academic and International Programs

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Qing Xiang, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Gary L. Ebert, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Felix G. Lazebnik, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Robert P. Gilbert, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

B. David Saunders, Ph.D.
Member of dissertation committee

ACKNOWLEDGEMENTS

This work was done in close collaboration with the author's advisor, Qing Xiang. From the author's first semester as a graduate student, Dr. Xiang promoted the study of Gauss sums and Jacobi sums. Indeed, Jacobi sums proved to be the key to this work. The biggest part of our results have been incorporated into a paper currently in the referee process [11], also coauthored with Peter Sin of University of Florida. Peter Sin previously conjectured the main result, and proved it in the prime field case [37] and the point-hyperplane case [36] using representation theory. His help was invaluable in making a concise presentation of some representation theory arguments in our submitted article. In the present work we have tried to expand some of these arguments to make them plainer from a combinatorial point of view.

The last chapter of this work reflects a paper with Dr. Xiang which has appeared [12]. Dr. Xiang previously converted the Smith normal form problem into a counting problem involving Gauss sums and gave it to the present author to do the counting. We also had to prove our criterion for using characters to determine the invariants of difference sets. We are indebted to W. K. (Billy) Chan for his elegant method of proof involving local rings, which replaces the present author's somewhat brute force efforts. We are also grateful to Dave Saunders of the Computer Science Department for direct computation of the Smith normal forms of two roughly 10000 by 10000 matrices.

Beyond Dr. Xiang, the other discrete mathematics graduate students and faculty were crucial to making this course of study enjoyable and productive, including Frank Fielder, Vasyl Dmytrenko, Sven Reichard, Jason Williford, Carl DeVore,

Gary Ebert, and Felix Lazebnik. Finally, thanks are due to the author's family for their support and encouragement, including his parents, Gus and Margaret Chandler, and his step-children, Jackie Shatley and Louis Broyles. The author dedicates this work to the memory of his wife Judah, who put up with him until her untimely death December 15, 2003.

TABLE OF CONTENTS

Chapter

ABSTRACT

The incidence matrix of a design is a (0,1)-matrix with rows representing blocks, columns representing points, and a one indicating incidence. The Smith normal form generalizes the idea of p-rank. We determine the Smith normal form of the incidence matrices of classical designs, those arising from the incidence of points and some other dimensional subspace of a finite geometry. The techniques involve the use of p-adic character sums and some representation theory.

We also obtain partial results in determining the Smith normal form for the incidence between sets of subspaces, neither one of which is the set of points. The p-part remains largely unknown in this case.

In the case of the designs associated with two families of difference sets with classical parameters, the p-ranks are the same when the parameters are the same. We show these difference sets are inequivalent by showing a difference in the Smith normal forms of the designs.

Chapter 1

INTRODUCTION

The most important result of this dissertation is to determine the Smith normal forms of certain classical designs arising from finite Desarguesian geometries. While we got results for both affine and projective goemetries, the more fundamental case would appear to be the projective case.

In Chapter 8 we also determine explicit formulas for part of the Smith normal forms of two families of symmetric designs which arise from difference sets. As the formulas differ, we conclude that the difference sets are inequivalent, and the corresponding designs are nonisomorphic, even though they have the same p-ranks when the parameters are the same. We begin by describing the projective geometry problem.

Let $\mathbb{F}_q$ be the finite field of order q, where $q = p^t$, p is a prime, and t is a positive integer, and let V be an $(n+1)$-dimensional vector space over $\mathbb{F}_q$. We denote by $\mathrm{PG}(V)$ (or $\mathrm{PG}(n, q)$ if we do not want to emphasize the underlying vector space) the n-dimensional projective geometry of V. The elements of $\mathrm{PG}(V)$ are subspaces of V, and two subspaces are considered to be incident if one is contained in the other. We call one-dimensional subspaces of V *points* of $\mathrm{PG}(V)$, and we call n-dimensional subspaces of V *hyperplanes* of $\mathrm{PG}(V)$. More generally, we regard r-dimensional subspaces of V as projective $(r-1)$-dimensional subspaces of $\mathrm{PG}(V)$. We will refer to r-dimensional subspaces of V as r-subspaces and denote the set of these spaces in V as $\mathcal{L}_r$. The set of projective points is then $\mathcal{L}_1$. We will consider the incidence

relation between $\mathcal{L}_r$ and $\mathcal{L}_1$. Specifically, let A be a (0,1)-matrix with rows indexed by elements Y of $\mathcal{L}_r$ and columns indexed by elements Z of $\mathcal{L}_1$, and with the (Y, Z) entry equal to 1 if and only if $Z \subset Y$. We are interested in finding the Smith normal form of A. (See Section 2.2 for the definition of Smith normal form.)

The incidence matrix A has been studied at least since the 1960s. Several authors have considered the more general incidence matrices $A_{r,s}$ of r-subspaces *vs.* s-subspaces. Of course, $A_{s,r}$ is the transpose of $A_{r,s}$, so the problems of finding the Smith normal forms of the two matrices are equivalent. Also the matrix $A_{r,s}$ is the same as the matrix $A_{n+1-r,n+1-s}$. One defines the dual of a vector subspace to be the subspace of those elements of V which are orthogonal to every point of the original subspace, using the ordinary dot product on a specified coordinatization of V. Incidence then is merely reversed when each subspace is replaced by its dual. Thus, when we consider the more general case $A_{r,s}$, we may assume that $1 < s < r < n$ and $s + r \leq n + 1$.

The known results for the general case $A_{r,s}$ are the ranks of $A_{r,s}$ over fields K of characteristics not equal to p. When $K = \mathbb{Q}$, Kantor in [24] showed that the matrix $A_{r,s}$ has full rank under certain natural conditions on r and s, and when $\mathrm{char}(K) = \ell$, where ℓ does not divide q, the rank of $A_{r,s}$ over K was given by Frumkin and Yakir [17]. The most interesting case is when $\mathrm{char}(K) = p$. In this case, with $1 < s < r < n$, the problem of finding the rank of $A_{r,s}$ is open, except in the very few cases in which n and q each are small enough to facilitate direct computation (cf. [18]). However, Hamada [19] gave a complete solution to the problem of finding the p-rank of A (known as Hamada's formula). In this work we completely determine the Smith normal form of $A = A_{r,1}$ as an integral matrix.

There are at least two reasons for us to study this problem. First, the Smith normal form may be useful to distinguish between nonisomorphic designs and between inequivalent difference sets (see Chapter 8). If we take the elements of $\mathcal{L}_1$

as points and take the elements of $\mathcal{L}_r$ as blocks, then we obtain what is called a 2-design [4] with "classical parameters". It is known that there exist many 2-designs with classical parameters [8]. A standard way to distinguish nonisomorphic designs with the same parameters is by comparing the p-ranks of their incidence matrices. Unfortunately, nonisomorphic designs sometimes have the same p-rank. In such a situation, one can try to prove nonisomorphism of designs (and the inequivalence of the associated difference sets) by comparing the Smith normal forms of the incidence matrices [12]. Therefore it is of interest to find Smith normal forms of incidence matrices of designs.

The second reason is a connection with a problem solved by Wilson [42]. Let Ω be an n-set. We say that an r-subset of Ω is *incident* with an s-subset of Ω if one is contained in the other. Wilson found a diagonal form of the incidence matrix of r-subsets versus s-subsets of Ω. The case of r-subsets versus s-subsets in an $(n+1)$-set can be viewed as the $q = 1$ analog of the r-subspace versus s-subspace problem in $\mathrm{PG}(n, q)$.

Now we summarize previous work related to the problem of finding the Smith form of the incidence between $\mathcal{L}_1$ and $\mathcal{L}_r$. Hamada [19] determined the p-rank of the incidence between projective points and r-subspaces of $\mathrm{PG}(n, q)$ for any values of p, t, r, and n. Hamada's formula in [19] is based on results in Smith's dissertation [38]. (Smith normal form is named for a much older Smith.) Lander [28] found the Smith form for the incidence between points and lines in $\mathrm{PG}(2, q)$. Black and List [9] determined the invariant factors of the incidence between points and hyperplanes in the case where $q = p$ (that is, $t = 1$). More recently, Hamada's formula follows directly from the dimension of a certain submodule determined by Bardoe and Sin in [7]. Sin used the submodule structure to determine the Smith normal form of the incidence between points and arbitrary r-spaces when $q = p$ [37], and to determine the Smith normal form of the incidence between points and hyperplanes for general

q [36]. Liebler used a different approach to determine the Smith normal form of the incidence between points and hyperplanes [30]. Finally, Liebler and Sin had conjectured the formulas for the invariant factors of the incidence between points and arbitrary r-subspaces for general q, and could prove their formulas in the cases where $q = p$, p^2, or p^3 [30]. We use a combination of techniques from number theory and representation theory to confirm this conjecture.

Much of the time we will argue in terms of the incidence map. If E is any ring, we let $E^{\mathcal{L}_i}$ denote the free E-module of rank $|\mathcal{L}_i|$. We will use the same symbols to denote elements of $\mathcal{L}_i$ and basis vectors of $E^{\mathcal{L}_i}$. We define the incidence map

$$\eta_{1,r} : \mathbb{Z}^{\mathcal{L}_1} \to \mathbb{Z}^{\mathcal{L}_r}$$

by letting $\eta_{1,r}(Z) = \sum_{Y \in \mathcal{L}_r, Z \subset Y} Y$ for every $Z \in \mathcal{L}_1$. Then we extend $\eta_{1,r}$ linearly to $\mathbb{Z}^{\mathcal{L}_1}$. The matrix of $\eta_{1,r}$ with respect to the basis $\mathcal{L}_1$ of $\mathbb{Z}^{\mathcal{L}_1}$ and the basis $\mathcal{L}_r$ of $\mathbb{Z}^{\mathcal{L}_r}$ is exactly the matrix A defined above. We will use the same $\eta_{1,r}$ to denote the linear map from $R^{\mathcal{L}_1}$ to $R^{\mathcal{L}_r}$ defined in the same way as above. R is a certain p-adic local ring with maximal ideal $\mathfrak{p}$ and residue field $\mathbb{F}_q$.

This work is organized as follows. Chapter 2 is all preliminary material. In Chapter 3 we explain the problem we are solving. Not until the last section of that chapter do we state the main theorem. We include (in Section 3.2) an elementary proof of a well-known fact: all but one of the invariant factors of A are powers of p. Then in Section 3.3 we introduce the monomial basis $\mathcal{M}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ and its Teichmüller lifting to a basis $\mathcal{M}_R$ of $R^{\mathcal{L}_1}$. These bases are the key to finding the Smith normal form of A. It is with respect to the $\mathcal{M}_R$ of $R^{\mathcal{L}_1}$ and a certain basis of $R^{\mathcal{L}_r}$ that the matrix of $\eta_{1,r}$ is in Smith normal form.

In Section 3.4 we summarize the results of Bardoe and Sin [7]. They completely determined the submodules of $\mathbb{F}_q^{\mathcal{L}_1}$ which are invariant under the action of the general linear group acting as permutation group on the subspaces $\mathcal{L}_1$ of V. These submodules have certain subsets of $\mathcal{M}$ as bases. Then at last, we actually

state our Theorem A, the determination of the Smith normal form of the incidence matrix A.

In Chapter 4 we treat the point-to-hyperplane incidence map $\eta_{1,n}$. For each monomial basis element $f \in \mathcal{M}_R$ we use Jacobi sums and Stickelberger's relation to compute $\eta_{1,n}(f)$ explicitly–in terms of polynomials in the dual coordinates for the elements of $\mathcal{L}_n$. The invariants of $\eta_{1,n}$ can be read from these images.

Chapter 5 is dedicated to proving Theorem A. We are able to get lower bounds on the invariants by direct calculation. We express the image $\eta_{1,r}(f)$ for each $f \in \mathcal{M}_R$ as character sums. That is, each coordinate of the image vector with respect to the basis $\mathcal{L}_r$ is such a character sum. Theorem 2.5.6 (Wan's Theorem) gives p-adic estimates for these sums. We know that these estimates must divide the invariants of $\eta_{1,r}$. It remains to prove that these estimates are sharp in our case.

The monomial basis $\mathcal{M}_R$ of $R^{\mathcal{L}_1}$ reduces (mod $\mathfrak{p}$) to the basis $\mathcal{M}$ of $\mathbb{F}_q^{\mathcal{L}_1}$. We will call a basis of $\mathcal{M}_R$ an *SNF basis* if the matrix of $\eta_{1,r}$ is in Smith normal form with respect to that basis and some basis of $R^{\mathcal{L}_r}$. We want to show that $\mathcal{M}_R$ is an SNF basis. In Section 5.2 we use the submodule structure of $\mathbb{F}_q^{\mathcal{L}_1}$ to prove that an SNF basis can be chosen so that at least its reduction (mod $\mathfrak{p}$) is $\mathcal{M}$. We can also group these basis elements into certain *types*, according to which submodules their images in $\mathcal{M}$ generate, and we show that basis elements of the same type correspond to the same p-adic invariant.

In Section 5.3 we examine the action of the general linear group G on $R^{\mathcal{L}_1}$. We use the notions of Jacobi sums and the character group. For most elements of $\mathcal{M}_R$ (unless $q = 2$) we can construct an element $g \in RG$, the group ring of R and G, with the following property. Given an arbitrary function $f \in R^{\mathcal{L}_1}$, the image gf is the desired monomial with the same coefficient it has in f. In particular, we can replace most of our basis elements with the corresponding elements of $\mathcal{M}_R$.

We complete the proof of Theorem A in Section 5.4. Again we use Stickelberger's theorem applied to Jacobi sums. We construct an element of RG which acts on a given element of $\mathcal{M}_R$ of one type to give an element of $\mathcal{M}_R$ of a certain other type times a factor of p. Doing so we put an upper bound on the p-adic invariant corresponding to the first element of $\mathcal{M}_R$. For the convenience of the reader, we then provide in Section 5.5 a modified proof of the main result of [7], the $\mathbb{F}_q G$-submodule structure of $\mathbb{F}_q^{\mathcal{L}_1}$. We avoid most of the language of representation theory.

In Chapter 6 we obtain the Smith normal form for the incidence map in the affine geometry case (Theorem B). We separate the projective geometry into its affine part and the hyperplane at infinity. Those monomials which are zero on the hyperplane at infinity are the ones which contribute to the invariants of this matrix.

Frumkin and Yakir ([17]) computed the rank of $\eta_{r,s}$ over any field not of characteristic p. In Chapter 7 we extend the work of Frumkin and Yakir to obtain the ℓ-adic Smith normal form for any prime $\ell \neq p$. Thus we know everything about the Smith normal form of $A_{r,s}$ except the powers of p, even when strict inequality, $1 < s < r < n$, holds. In this chapter we also obtain an eigenvalue result with some relevance to the p-powers.

In Chapter 8 we compute the multiplicities of the second (3-adic) invariant for two other families of difference sets with classical parameters (HKM and Lin), showing that the difference sets are inequivalent. The multiplicity of the first invariant gives the 3-rank. In this case the 3-ranks are the same when the two difference sets from different families have the same parameters, but the multiplicities of the second invariant are different. This work was actually done before, and motivated our interest in, the calculation of the Smith normal forms of designs form projective geometry. We determined that the multiplicities of the second invariant are two different fourth degree polynomials (or possibly near polynomials) in m, where the size of the group is $(3^m - 1)/2$. What we actually proved is that the multiplicity of

the second invariant (except for very small values of m) is either equal to a certain polynomial, or for some values of m the multiplicity might be less by exactly m. The proof that the Lin sets are difference sets is due to Arasu and Dillon [2]. Interestingly, from what we have seen of their technique, they may be able to resolve the ambiguity, and possibly compute the rest of the invariants.

Chapter 2

PRELIMINARIES

The main theme of this work was determining the *Smith normal form* of the incidence matrices of some designs. We begin by explaining the basic concepts.

2.1 Designs

Designs were introduced in the 1930s as designs for statistically balanced experiments. They were soon found to be interesting objects in their own right, with applications to finite geometry, coding theory, and other fields.

Definition 2.1.1. *Let $\mathcal{P}$ be a set of v elements, called* points*, and let $\mathcal{B}$ be a collection (possibly a multiset) of b subsets of $\mathcal{P}$, each of size k, called* blocks*. We call $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ a* 2-design*, or* 2-(v, k, λ) design*, if there is an integer $\lambda = \lambda_2$ such that every pair of points in $\mathcal{P}$ is contained in exactly λ blocks of $\mathcal{B}$.*

In general, for $t < k$, $\mathcal{D}$ is a t-design*, or* t-(v, k, λ) design*, if there is an integer $\lambda = \lambda_t$ such that every t-subset of $\mathcal{P}$ is contained in exactly λ blocks of $\mathcal{B}$.*

Theorem 2.1.2. *If $\mathcal{D}$ is a t-design for some positive integer t, then $\mathcal{D}$ is also a $(t-1)$-design. In particular, if $\mathcal{D}$ is a 2-design, then each point occurs in exactly $r = \lambda_1$ blocks. We call r the* replication number *of $\mathcal{D}$. Every system of k-subsets is trivially a 0-design with $\lambda_0 = b$.*

Proof: See for instance [10, p. 259].

In this work we will be concerned specifically with 2-designs. The parameters of the 2-design, (v, k, λ, b, r), are not all independent. Counting the number of pairs (p, B) of one point and one block, with $p \in B$, yields

$$bk = vr.$$

Second, we can count the number of triples $(p_1, p_2, B),\ p_1 \neq p_2,\ \{p_1, p_2\} \subset B$, of a block and two of its points, in either of two ways. The number of ordered distinct pairs in each block is $k(k-1)$, so we get $bk(k-1)$. Also, the total number of ordered pairs of distinct points is $v(v-1)$ and each is in λ blocks, so we get

$$bk(k-1) = v(v-1)\lambda$$

which reduces to

$$r(k-1) = (v-1)\lambda.$$

The classical examples of 2-designs arise from projective and affine geometries over finite fields. Let $\mathrm{PG}(m, q)$ be the m-dimensional projective geometry over the finite field $\mathbb{F}_q$, where q is a prime power. That is, $\mathrm{PG}(m, q)$ is the set of subspaces of an $(m+1)$-dimensional vector space over $\mathbb{F}_q$, with inclusion the incidence relation. Similarly let $\mathrm{AG}(m, q)$ be the m-dimensional affine geometry over $\mathbb{F}_q$. This geometry includes all cosets of subspaces of an m-dimensional vector space over $\mathbb{F}_q$. Let $\begin{bmatrix} m \\ i \end{bmatrix}_q$ denote the number of i-dimensional subspaces of an m-dimensional vector space over $\mathbb{F}_q$. We have

$$\begin{bmatrix} m \\ i \end{bmatrix}_q = \prod_{j=1}^{i} \frac{(q^{m-i+j} - 1)}{(q^j - 1)}.$$

(We call these numbers generalized binomial or Gaussian coefficients and note that if we treat q as a continuous variable and let $q \to 1$, the limits are the ordinary binomial coefficients.)

The following are the classical examples of 2-designs.

Example 2.1.3. *The points of* $\mathrm{PG}(m,q)$ *and the* $(d-1)$*-dimensional subspaces of* $\mathrm{PG}(m,q)$ *(*d*-dimensional vector subspaces) form a 2-design with parameters*

$$v = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q = \frac{q^{m+1}-1}{q-1}$$

$$k = \begin{bmatrix} d \\ 1 \end{bmatrix}_q = \frac{q^d-1}{q-1}$$

$$\lambda = \begin{bmatrix} m-1 \\ d-2 \end{bmatrix}_q,\ r = \begin{bmatrix} m \\ d-1 \end{bmatrix}_q,\ \text{and } b = \begin{bmatrix} m+1 \\ d \end{bmatrix}_q.$$

We can obtain these parameters from the following general principle: given an i-dimensional vector subspace U of an m-dimensional vector space W over $\mathbb{F}_q$, the number of j-dimensional vector subspaces of W containing U is $\begin{bmatrix} m-i \\ j-i \end{bmatrix}_q$.

Example 2.1.4. *The points of* $\mathrm{AG}(m,q)$ *and the* d*-flats of* $\mathrm{AG}(m,q)$ *form a 2-design with parameters*

$$v = q^m,\ k = q^d,\ \lambda = \begin{bmatrix} m-1 \\ d-1 \end{bmatrix}_q,\ r = \begin{bmatrix} m \\ d \end{bmatrix}_q,\ \text{and } b = q^{m-d}\begin{bmatrix} m \\ d \end{bmatrix}_q.$$

By d*-flats of* $\mathrm{AG}(m,q)$ *we mean all cosets of* d*-dimensional vector subspaces of the* m*-dimensional vector space over* $\mathbb{F}_q$*.*

We obtain the parameter r by noting that the d-flats through the origin are precisely the d-dimensional vector subspaces. Similarly, λ in this case is the number of d-dimensional vector subspaces containing the 1-dimensional vector subspace determined by the origin and one other point.

A design is nontrivial if not every (but at least one) k-subset of $\mathcal{P}$ occurs as a block. Nontrivial designs are sometimes called B.I.B.D.'s, or balanced incomplete block designs.

Fisher's theorem states that the number of blocks b in a 2-design is greater than or equal to the number of points v. If $v = b$ then we call $\mathcal{D}$ a *symmetric* design. Symmetric designs have the special property that their duals are also designs, and

the dual designs have the same parameters. That is, we can view $\mathcal{B}$ as the point set, $\mathcal{P}$ as the block set, and reverse the relation of containment. A symmetric design in which each pair of points is contained in λ blocks also has the property that each pair of blocks intersects in λ points. Thus a nontrivial symmetric design cannot have repeated blocks.

Definition 2.1.5. *Two designs, $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ and $\mathcal{D}_1 = (\mathcal{P}_2, \mathcal{B}_2)$, are said to be* isomorphic *if there exist a bijection $\sigma : \mathcal{P}_1 \to \mathcal{P}_2$ and a bijection $\rho : \mathcal{B}_1 \to \mathcal{B}_2$ such that for all $p \in \mathcal{P}_1$ and $B \in \mathcal{B}_1$, $p \in B$ if and only if $\sigma(p) \in \rho(B)$.*

Clearly isomorphic designs have identical parameters.

We will often treat a design interchangeably with its incidence matrix.

Definition 2.1.6. *Given a design $\mathcal{D}$ with set of points $\{p_1, p_2, \ldots, p_v\}$ and set of blocks $\{B_1, B_2, \ldots, B_b\}$, we call the $b \times v$ matrix $A = (a_{ij})$ an* incidence matrix *for $\mathcal{D}$ if the entry $a_{ij} = 1$ if $p_j \in B_i$ and $a_{ij} = 0$ otherwise.*

If we permute the order in which we label the points, and the order in which we label the blocks, the new incidence matrix will be that of an isomorphic design. Algebraically, two designs $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic if there are a $b \times b$ permutation matrix S and a $v \times v$ permutation matrix T such that the corresponding incidence matrices satisfy

$$SA_1T = A_2.$$

It may happen that $SA_1T = A_1$. In that case we call the transformation (S, T) an *automorphism* of the design. The set of all automorphisms of a design forms a group, the *full automorphism group* of the design. An *automorphism group* of a design is a subgroup of the full automorphism group.

Let I_k denote the $k \times k$ identity matrix, let $J_{i \times j}$ denote the $i \times j$ matrix whose entries all equal 1, and let E denote the diagonal matrix with diagonal entries

$r_1, r_2, \ldots, r_v$, where r_i is the replication number of point p_i. Then the definition of a 2-design with incidence matrix A can be stated in matrix form as

$$\begin{aligned} A^\top A &= E - \lambda I_{v\times v} + \lambda J_{v\times v} && (2.1)\\ AJ_{v\times v} &= kJ_{b\times v}. && (2.2) \end{aligned}$$

Some authors state in the definition of a 2-design that the replication number is constant. We now prove this fact, which is Theorem 2.1.2 in the case $t = 2$.

Proof: For simplicity let $J = J_{v\times v}$ and let $I = I_{v\times v}$. Right multiply each side of (2.1) by J and use (2.2) to get

$$\begin{aligned} A^\top AJ &= (E - \lambda I + \lambda J)J \\ A^\top kJ_{b\times v} &= EJ - \lambda J + v\lambda J \\ kEJ &= EJ - \lambda J + v\lambda J \\ (k-1)EJ &= (v-1)\lambda J \end{aligned}$$

which shows that $(k-1)r_i = (v-1)\lambda$ for each i, that is, $r = (v-1)\lambda/(k-1)$ and $E = rI$. □

2.2 Smith normal form

We will be interested in the Smith normal form of incidence matrices.

Definition 2.2.1. *Let R be a principal ideal domain (P.I.D.) and let $A = (a_{ij})$ be an $n \times m$ matrix with entries from R and let the rank of A be r. We will call a matrix $S = (s_{ij})$ the* Smith normal form *of A if it satisfies these properties:*

(1) $s_{i,j} = 0$ if $i \neq j$. The nondiagonal entries of S are 0.

(2) $s_{i,i} \mid s_{i+1,i+1}$ if $1 \leq i < r$. Each diagonal entry divides its successor, up to the rank of A.

(3) $s_{i,i} = 0$ if $i > r$.

(4) $S = PAQ$, where P and Q are invertible matrices over R.

By performing elementary row and column operations, it is always possible to transform A into the Smith normal form. The diagonal entries of S are unique up to multiplication by units of the ring R, and are called the *invariants* of A or the *elementary divisors* of A. (For proofs, see [31].)

The following lemma is not difficult to prove, (See [25] for references.)

Lemma 2.2.2. *Let $C = AB$ be the product of matrices over a principal ideal ring. For a matrix M, let $d_i(M)$ denote the i^{th} invariant of M. Also define $D_i(M) = d_1(M) \cdots d_i(M)$ for $1 \leq i \leq \text{rank}(M)$. Then*

$$d_i(A) \mid d_i(C) \text{ and } d_i(B) \mid d_i(C), \quad 1 \leq i \leq \text{rank}(C).$$

Furthermore

$$\big(D_i(A)D_i(B)\big) \mid D_i(C).$$

Klemm proved some basic results about the invariants of incidence matrices of 2-designs. In fact, he considers a slightly more general class of incidence structure, which he calls a partial block design (*Semiblockplan*). He still assumes that the number of blocks through any one point is

$$r = n + \lambda \quad n > 0,\ r > 0$$

and that the number of blocks through any pair of points is λ. He omits the assumption that every block has the same number of points. Then we have ([25, Theorem A]):

Theorem 2.2.3. *Let A be the incidence matrix for a partial block design with v points and b blocks and let n, λ, and the invariants $d_1, \ldots, d_v$ be as above. Let δ*

be the greatest common divisor of n and λ. Let p be any prime number dividing n. Then

$$
\begin{aligned}
(a) \qquad & d_1 = 1, \\
& (d_1 \cdots d_i)^2 \mid \delta n^{i-1} \qquad \text{for } 2 \le i \le v-1, \\
& (d_1 \cdots d_v)^2 \mid (n+\lambda v) n^{v-1}. \\
(b) \qquad & d_i \mid n \qquad \text{for } 2 \le i \le v-1, \\
& d_v \mid rn/\delta. \\
(c) \qquad & p \mid d_i \qquad \text{for } (b+1)/2 < i \le v.
\end{aligned}
$$

Note that frequently $b + 1 \ge 2v$. For the symmetric case we have this result ([25, Theorem B]):

Theorem 2.2.4. *Let A be the incidence matrix for a symmetric 2-design, so that $v = b$ and $k = r$. Let p be any prime dividing n and not dividing λ, and let x_p denote the p-part of x. Then*

$$
\begin{aligned}
(a) \quad & d_1 \cdots d_v = k n^{(v-1)/2}. \\
(b) \quad & d_v = kn/\delta. \\
(c) \quad & (d_i d_{v+2-i})_p = n_p \qquad \text{for } 3 \le i \le v-1.
\end{aligned}
$$

2.3 Cyclic difference sets

We first define difference set.

Definition 2.3.1. *A subset D of a group $(G, +)$ is a* difference set *if every non-identity element of G can be represented in exactly λ distinct ways as a difference $d_1 - d_2$ of members of the set D.*

If a difference set D has size k in a group of size v, we call D a (v, k, λ)-difference set. The relation to designs is immediate. We can take the elements of G

to be the point set, and take the block set to be $\{g+D \mid g \in G\}$, where $g+D$ denotes $\{g+d \mid d \in D\}$. The result is a (v,k,λ)-design $\mathcal{D}$, which we call the *development* of D.

We can also take a (v,k,λ)-symmetric design and ask whether there is a corresponding difference set. The answer is yes, if the design admits a regular group action—that is—if there is a group of order v acting transitively on the points, such that the image of any block is another block.

The reader should be aware that group operation is often written as multiplication, in which case 'differences' would be written as $d_1 {d_2}^{-1}$. In this work we shall be interested in certain *cyclic* difference sets, that is, difference sets in the additive group $\mathbb{Z}_v$.

We now give the Singer construction of the family of difference sets whose development is the same design as Example 2.1.3 with $d = m$ (points are projective points and blocks are projective hyperplanes). Let $q = p^t$ be a prime power, and let $m > 2$ be an integer. Then we will view $\mathbb{F}_{q^m}$, the field with q^m elements, as the vector space V over the field $\mathbb{F}_q$. The trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$,

$$\begin{aligned} \mathrm{Tr}_{q^m/q} : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto x + x^q + \cdots + x^{q^{m-1}}, \end{aligned}$$

is a linear functional on V. Therefore, if $a \neq 0 \in \mathbb{F}_{q^m}$ and $c \in \mathbb{F}_q$, the elements $x \in \mathbb{F}_{q^m}$ which satisfy

$$\mathrm{Tr}_{q^m/q}(ax) = c$$

form an affine hyperplane in V, and if $c = 0$, they form a subspace of codimension 1.

Now let γ be a generator of $\mathbb{F}_{q^m}^*$, the cyclic multiplicative group of $\mathbb{F}_{q^m}$. Then the map $\beta : \ x \mapsto \gamma x$ is a vector space automorphism on V, and also an automorphism on the projective geometry $\mathrm{PG}(m-1,q) \cong \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. The cyclic group

generated by β in $\mathrm{Aut}\big(\mathrm{PG}(m-1,q)\big)$ permutes all the points of $\mathrm{PG}(m-1,q)$ in one cycle, the *Singer* cycle. It must also permute all the hyperplanes of $\mathrm{PG}(m-1,q)$ in a Singer cycle. The reason is that two linear functionals on V have the same set of zeros if and only if one is a multiple of the other (over $\mathbb{F}_q$). Since for $e \in \mathbb{F}_q$, $\mathrm{Tr}_{q^m/q}(cx) - e\,\mathrm{Tr}_{q^m/q}(dx) = \mathrm{Tr}_{q^m/q}\big((c-de)x\big)$ is not an identically zero function of x unless $c = de$, the equations

$$\mathrm{Tr}_{q^m/q}(\gamma^i x) = 0,\ 0 \le i \le \frac{q^m-1}{q-1} - 1,$$

give $\frac{q^m-1}{q-1}$ distinct hyperplanes.

Since we have a symmetric design with a regular automorphism group, any block determines a difference set. In particular, let ρ be the natural epimorphism $\rho:\ \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. The set

$$\big\{\rho(x) \mid x \in \mathbb{F}_{q^m}^*,\ \mathrm{Tr}_{q^m/q}(x) = 0\big\}$$

is the *Singer* difference set in the cyclic group $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$.

2.4 p-adic numbers

Every field of characteristic 0 contains the rational numbers. We find that the rational numbers are not complete with respect to a norm, that is, not all Cauchy sequences of rational numbers converge to a rational number. Usually we take the Archimedean norm, which is the absolute value of a rational. Then if we complete the rational numbers by including the limits of all sequences which are Cauchy with respect to this norm, we get the real numbers. If we adjoin $i = \sqrt{-1}$, and complete $\mathbb{Q}(i)$ with respect to the Archimedean norm, we get all the complex numbers.

The Archimedean norm is not the only choice of a norm. We define a norm in this sense to be any map $\| * \|$ from the field to the nonnegative real numbers satisfying

1. $\|x\| = 0$ if and only if $x = 0$.

2. $\|x \cdot y\| = \|x\| \cdot \|y\|$

3. $\|x + y\| \leq \|x\| + \|y\|$.

It turns out that the only other norm possible is based on *p-adic valuation*. That is, given a prime p, and integers a and $b \neq 0$, the p-adic valuation $\nu_p(a/b)$ of the fraction a/b is the number of times p divides a minus the number of times p divides b. The valuation of 0 is infinite, and we define the norm to be

$$\|x\| = p^{-\nu_p(x)}.$$

With this norm we get $\|x + y\| \leq \max\{\|x\|, \|y\|\}$. We can write any rational number, as well the the limit of any sequence that is Cauchy under this norm, as the convergent series

$$x = p^{\nu_p(x)}(a_0 + a_1 p + a_2 p^2 + \cdots), \quad a_0 \neq 0,\ 0 \leq a_i < p,\ i = 0, 1, 2, \ldots.$$

We call this field the p-adic numbers $\mathbb{Q}_p$ and say it is a *local* field, localized at p. Further, we call those numbers with nonnegative valuation $\mathbb{Z}_p$, the ring of p-adic integers, a local ring. In general, we can define a local ring as any integral domain with a unique maximal ideal, and we can define a local field as the field of fractions of a local ring. The unique maximal ideal of $\mathbb{Z}_p$ is the set of integers with positive valuation, $\mathfrak{p} = p\mathbb{Z}_p$, and we have $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Now let $q = p^t$, and extend $\mathbb{Q}_p$ by adjoining the roots of $x^q = x$. We designate by ξ_{q-1} a primitive $(q-1)^{\text{th}}$ root of unity and we designate the set of all roots of $x^q = x$ by T_q. It is a consequence of Hensel's lemma that $K = \mathbb{Q}_p(\xi_{q-1})$ is an extension of degree t over $\mathbb{Q}_p$, and it is the unique unramified extension of degree t (see [26], pp. 67-68). The ring of integers is $R = \mathbb{Z}_p[\xi_{q-1}]$, $\mathfrak{P} = pR$ is the unique maximal ideal and $R/pR \cong \mathbb{F}_q$. In fact, we can write any element of the field K in the form

$$x = p^{\nu_p(x)}(a_0 + a_1 p + a_2 p^2 + \cdots), \quad a_0 \neq 0,\ a_i \in T_q,\ i = 0, 1, 2, \ldots$$

and we see that each element of $\mathbb{F}_q$ is the reduction of an element of T_q.

2.5 Character sums

The results of this work depend on the use of character sums over finite fields. In this section we will assume that G is an abelian group. We first define a character of a finite abelian group.

Definition 2.5.1. *Let G be a group with v elements. A* character *of the group G is a mapping χ of the elements of G to the v^{th} roots of unity of some field $\mathbb{F}$ satisfying*

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$$

for any elements g_1 and g_2 of G.

If the group operation is written additively, we instead have

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2).$$

It is useful to define the product of two characters on G by

$$\chi_1\chi_2(g) = \chi_1(g)\chi_2(g).$$

With this definition the characters form a group G^* which is isomorphic to G.

If R is a ring and G is a group, then the group ring RG consists of elements of the form

$$\sum_{g \in G} a_g g, \quad a_g \in R, \ \forall g \in G.$$

The summation is formal and has nothing to do with the group operation, which we will write multiplicatively. We define the ring product by specifying for $a, b \in R$ and $g, h \in G$ that

$$(ag)(bh) = (ab)(gh)$$

and extending the operation linearly to any group ring elements. Of course, we also take $ag + bg = (a + b)g$. For any character χ mapping G into an extension of R, we also define

$$\chi\big(\sum_{g\in G} a_g g\big) = \sum_{g\in G} a_g \chi(g).$$

We can use characters to determine whether a subset of an abelian group is a difference set. Let $D \subset G$ be a subset of the abelian group G with identity element 1_G. We also let D and G denote the elements of the group ring $\mathbb{Z}G$ which are the formal sums of their elements, and we let $D^{(-1)}$ denote the formal sum of the inverses of the elements of D. If D is a (v, k, λ)-difference set, from the definition of a difference set we immediately get

$$D^{(-1)}D = (k - \lambda)1_G + \lambda G. \tag{2.3}$$

Now let χ be any nontrivial character. We apply χ to both sides of (2.3). Since $\chi(G) = 0$, we get

$$\chi^{-1}(D)\chi(D) = k - \lambda \tag{2.4}$$

for any nontrivial character. By the inversion formula (5.6), we can also conclude that if (2.4) holds for every nontrivial character, and the size of D is k, then (2.3) holds and D is a (v, k, λ)-difference set.

If our characters are the complex characters, we can go a little further, since $\chi^{-1}(g)$ is then the complex conjugate of $\chi(g)$ and $\chi^{-1}(D)$ is the complex conjugate of $\chi(D)$. The criterion (2.4) is then that a proper nonempty subset of G is a difference set if and only if the magnitude of $\chi(D)$ is the same for every nontrivial complex character χ.

2.5.1 Characters of a finite field

Let $q = p^t$ be a power of a prime and let $\mathbb{F}_q$ be the field with q elements. We will be interested in characters of the additive group of the finite field $(\mathbb{F}_q, +)$,

which map the elements of the field to the p^{th} roots of unity of some other field. We will also be interested in characters of the multiplicative group of nonzero elements $(\mathbb{F}_q^*, \cdot)$, which map the elements of the field to the $(q-1)$-roots of unity of some other field.

We also extend the definition of a multiplicative character χ by setting $\chi(0) = 0$. The only exception will be the trivial multiplicative character, which sends every element, including 0, to 1. We also have a character that sends 0 to 0 and every nonzero element to 1. We will call this character the (multiplicative) *principal* character. With this definition we have a total of q multiplicative characters. The nontrivial characters form a group which is isomorphic to the multiplicative group of the field $(\mathbb{F}_q^*, \cdot)$. The principal character acts as the identity.

In the additive character group, we will use *principal* character and *trivial* character interchangeably.

2.5.2 Gauss sums

We define the Gauss sum.

Definition 2.5.2 (Gauss sum). *Let ψ be an additive character of $\mathbb{F}_q$ and let χ be a multiplicative character of $\mathbb{F}_q$. Then we define the* Gauss sum *$G(\psi, \chi)$ by*

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q} \psi(x)\chi(x).$$

We list some properties of Gauss sums.

1. If ψ and χ are both trivial, then $G(\psi, \chi) = q$.
2. If ψ is trivial and χ is principal, then $G(\psi, \chi) = q - 1$.
3. If ψ is trivial and χ is neither trivial nor principal, then $G(\psi, \chi) = 0$.
4. If ψ is nontrivial and χ is trivial, then $G(\psi, \chi) = 0$.

5. If ψ is nontrivial and χ is principal, then $G(\psi, \chi) = -1$.

6. If ψ is nontrivial and $a \in \mathbb{F}_q$ we define ψ_a via $\psi_a(x) = \psi(ax)$. With this definition ψ_a is an additive character, ψ_0 is the principal character, $\psi_a\psi_b = \psi_{a+b}$, and all additive characters are obtained in this way. Since for $a \neq 0$,

$$G(\psi_a, \chi) = \chi(a^{-1})G(\psi, \chi),$$

we can write all the Gauss sums in terms of our favorite additive character ψ.

We now consider the absolute trace function

$$\begin{aligned} \mathrm{Tr}: \mathbb{F}_q &\rightarrow \mathbb{F}_p \quad \text{via} \\ \mathrm{Tr}\,(x) &= x + x^p + \cdots + x^{p^{t-1}}. \end{aligned}$$

Let ξ_p be a p^{th} root of unity in some field. Trace is an additive function, so

$$\psi(x) := \xi_p^{\mathrm{Tr}(x)}$$

is an additive character of $\mathbb{F}_q$. Now we define

$$g(\chi) := G(\psi, \chi).$$

2.5.3 Jacobi sums

We will also need to use Jacobi sums of multiplicative characters of a finite field.

Definition 2.5.3. *Let χ_1 and χ_2 be multiplicative characters of the finite field $\mathbb{F}_q$ with the convention that $\chi_i(0) = 0$ if χ_i is nontrivial. Then the* Jacobi sum *is defined as*

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x).$$

We list some properties of the Jacobi sum.

1. $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$.

2. If χ_1 and χ_2 are both trivial, then $J(\chi_1, \chi_2) = q$.

3. If χ_1 is trivial and χ_2 is principal, then $J(\chi_1, \chi_2) = q - 1$.

4. If χ_1 and χ_2 are both principal, then $J(\chi_1, \chi_2) = q - 2$.

5. If χ_1 is trivial and χ_2 is neither trivial nor principal, then $J(\chi_1, \chi_2) = 0$.

6. If χ_1 is principal and χ_2 is neither trivial nor principal, then $J(\chi_1, \chi_2) = -1$.

7. If neither χ_1 nor χ_2 is principal but $\chi_1\chi_2$ is principal, then $J(\chi_1, \chi_2) = -\chi(-1)$.

8. If none of χ_1, χ_2, and $\chi_1\chi_2$ is trivial or principal, then

$$J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}.$$

We include a proof of the last fact.

Proof: Letting $z = x + y$ we get

$$\begin{aligned} g(\chi_1)g(\chi_2) &= \sum_{x\in\mathbb{F}_q} \chi_1(x)\xi_p^{\mathrm{Tr}(x)} \sum_{y\in\mathbb{F}_q} \chi_2(y)\xi_p^{\mathrm{Tr}(y)} \\ &= \sum_{x\in\mathbb{F}_q} \sum_{z\in\mathbb{F}_q} \chi_1(x)\chi_2(z-x)\xi_p^{\mathrm{Tr}(z)} \\ &= \sum_{z\neq 0} \chi_1(z)\chi_2(z)\xi_p^{\mathrm{Tr}(z)} \sum_{x\in\mathbb{F}_q} \chi_1(x/z)\chi_2(1-x/z) \\ &= g(\chi_1\chi_2)J(\chi_1, \chi_2) \end{aligned}$$

□

2.5.4 The Stickelberger congruence

Using the Stickelberger congruence we know the p-adic valuation of Gauss sums and Jacobi sums in both the local case and the global case. Again let $q = p^t$.

Definition 2.5.4. *Let $R = \mathbb{Z}_p[\xi_{q-1}]$ be as before with maximal ideal $\mathfrak{p}$. Let $R/\mathfrak{p} = \mathbb{F}_q$ be the field with q elements. We define the* Teichmüller *character T to be the map from $\mathbb{F}_q$ to the $(q-1)^{\text{th}}$ roots of unity of R such that $T(x) \pmod{\mathfrak{p}} = x$ for each $x \in \mathbb{F}_q$. Each multiplicative character of $\mathbb{F}_q$ can be expressed as a power of T.*

If we let ξ_{q-1} denote a primitive complex $(q-1)$th root of unity and let $\mathfrak{p}$ denote a maximal ideal of $\mathbb{Z}[\xi_{q-1}]$ dividing p, then we can similarly define the (global) Teichmüller character which maps elements of $\mathbb{F}_q$ to powers of ξ_{q-1} in the complex numbers. We refer the reader to [41, p. 95] for details.

Theorem 2.5.5. *Let k be either the field of rational numbers or of p-adic numbers, let ξ_{q-1} be a primitive $(q-1)^{\text{th}}$ root of unity in some extension of k, let ξ_p be a primitive p^{th} root of unity in some extension of k, and let $\tilde{K} = k(\xi_{q-1}, \xi_p)$. Let $\tilde{R}$ be the ring of integers of $\tilde{K}$, and let $\tilde{\mathfrak{P}}$ be a maximal ideal of $\tilde{R}$ lying over p. Let r be an integer with $0 < r < q-1 = p^t - 1$ and with p-adic expansion*

$$r = r_0 + r_1 p + \cdots + r_{t-1} p^{t-1}$$

with $0 \leq r_i \leq p-1$. Define

$$s(r) = r_0 + r_1 + \cdots + r_{t-1}$$

$$\gamma(r) = r_0! r_1! \cdots r_{t-1}!$$

Then we have the congruence

$$g(T^{-r}) \equiv -\frac{(\xi_p - 1)^{s(r)}}{\gamma(r)} \pmod{\tilde{\mathfrak{P}}^{s(r)+1}}.$$

The proof of this theorem in the global case can be found in [29, p. 7]. We will give a proof of the theorem in the local case by using the so-called splitting of an additive character of a finite field. This proof is due to Dwork [15]. First, we briefly explain the splitting of an additive character of $\mathbb{F}_q$. Let $\psi : \mathbb{F}_q \to \{1, \xi_p, \xi_p^2, \ldots, \xi_p^{p-1}\}$

be the additive character defined by $\psi(x) = \xi_p^{\mathrm{Tr}(x)}$, for all $x \in \mathbb{F}_q$. Dwork (cf. [15], [26, p. 117]) constructed a p-adic power series $\theta(X) = \sum_{i=0}^{\infty} \beta_i X^i \in \mathbb{Q}_p[[X]]$ satisfying the following properties:

$$\begin{aligned}
&(1). \quad \nu_p(\beta_i) \geq i/(p-1), \\
&(2). \quad \nu_p(\beta_i) = i/(p-1), \text{ if } 0 \leq i < p, \\
&(3). \quad \beta_i = \frac{(\xi_p - 1)^i}{i!}, \text{ if } 0 \leq i < p.
\end{aligned}$$

Thus, $\theta(x)$ converges p-adically for those x with p-adic norm satisfying $\|x\|_p < p^{\frac{1}{p-1}}$. In particular, θ is defined at the Teichmüller lifts of the nonzero finite field elements, whose p-adic norms are equal to 1. The importance of the function θ is that it *splits* ψ as follows:

$$\psi(\overline{x}) = \theta(x)\theta(x^p)\cdots\theta(x^{p^{t-1}}),$$

where x is the Teichmüller representative of $\overline{x} \in \mathbb{F}_q$. We can now give the proof of the Stickelberger congruence in the local case.

Proof: For $\overline{x} \in \mathbb{F}_q$, let x be its Teichmüller lifting. We have

$$\begin{aligned}
g(T^{-r}) &= \sum_{\overline{x} \in \mathbb{F}_q^*} x^{-r}\psi(\overline{x}) \\
&= \sum_{x \in T_q, x \neq 0} x^{-r}\theta(x)\theta(x^p)\cdots\theta(x^{p^{t-1}}) \\
&= \sum_{(i_0 \geq 0, i_1 \geq 0, \ldots, i_{t-1} \geq 0)} \beta_{i_0}\beta_{i_1}\cdots\beta_{i_{t-1}} \sum_{x \in T_q, x \neq 0} x^{(i_0 + p i_1 + \cdots + p^{t-1} i_{t-1} - r)} \\
&= (q-1) \sum_{\sum_{\ell=0}^{t-1} i_\ell p^\ell \equiv r \pmod{q-1}} \beta_{i_0}\beta_{i_1}\cdots\beta_{i_{t-1}}
\end{aligned}$$

Note that we are summing over all t-tuples $(i_0, i_1, \ldots, i_{t-1})$ of nonnegative integers such that $\sum_{\ell=0}^{t-1} i_\ell p^\ell \equiv r \pmod{q-1}$. For these t-tuples we have

$$\sum_{\ell=0}^{t-1} i_\ell \geq \sum_{\ell=0}^{t-1} r_\ell = s(r).$$

By Property (1) above satisfied by the β_i, we have

$$\nu_p(\beta_{i_0}\beta_{i_1}\cdots\beta_{r_{t-1}}) \geq \frac{\sum_{\ell=0}^{t-1} i_\ell}{p-1} \geq \frac{s(r)}{p-1}.$$

Therefore

$$\nu_p(g(T^{-r})) \geq \frac{s(r)}{p-1}.$$

Now note that $\sum_{\ell=0}^{t-1} i_\ell = s(r)$ if and only if $(i_0, i_1, \ldots, i_{t-1}) = (r_0, r_1, \ldots, r_{t-1})$. That is, there is a unique term in the summation above for $g(T^{-r})$ which has the lowest p-adic valuation $\frac{s(r)}{p-1}$. Hence

$$\nu_p(g(T^{-r})) = \nu_p(\beta_{r_0}\beta_{r_1}\cdots\beta_{r_{t-1}}),$$

which, by Property (2) above, is equal to $\frac{s(r)}{p-1}$. Thus far, we obtained the p-adic valuation of the Gauss sum $g(T^{-r})$. To prove the Stickelberger congruence, we simply use Property (3) above. By the preceding discussion, we have

$$g(T^{-r}) \equiv -\beta_{r_0}\beta_{r_1}\cdots\beta_{r_{t-1}} \pmod{\tilde{\mathfrak{P}}^{s(r)+1}},$$

which, by Property (3) above, is equal to $-\frac{(\xi_p-1)^{s(r)}}{\gamma(r)}$. This completes the proof. □

2.5.5 Wan's theorem

To pin down the Smith normal form of the designs given in Example 2.1.3, we had to show that the invariants are divisible by at least certain powers of p, and then show that those divisibilities are sharp. The first problem was the easier one. The key was a theorem of Daqing Wan which we now state and prove.

Again let $q = p^t$, let $K = \mathbb{Q}_p(\xi_{q-1})$ be the unique unramified extension of degree t over $\mathbb{Q}_p$, let $R = \mathbb{Z}_p[\xi_{q-1}]$ be the ring of integers in K, and let $\mathfrak{p}$ be the unique maximal ideal in R. Define $\bar{x}$ to be $x \pmod{\mathfrak{p}}$ for $x \in R$. Let T_q be the set of roots of $x^q = x$ in R and let T be the Teichmüller character of $\mathbb{F}_q$, so that $T(\bar{x}) = x$ for $x \in T_q$. Then T is a p-adic multiplicative character of $\mathbb{F}_q$ of order $(q-1)$ and all

multiplicative characters of $\mathbb{F}_q$ are powers of T. Following the convention of Ax [6], let T^0 be the character that maps all elements of $\mathbb{F}_q$ to 1 (which we have called the trivial multiplicative character), and let T^{q-1} (which we have called the principal multiplicative character) map 0 to 0 and all other elements to 1.

For $0 \leq i \leq n$ let $F_i(x_1, \ldots, x_r)$ be polynomials of degree d_i over $\mathbb{F}_q$ and let

$$\chi_i = T^{b_i} \quad (0 \leq b_i \leq q-1)$$

be multiplicative characters. We want the p-adic valuation $\nu_p(S_q(\chi, F))$ of the multiplicative character sum

$$S_q(\chi, F) = \sum_{\mathbf{x} \in \mathbb{F}_q^r} \chi_0(F_0(\mathbf{x})) \cdots \chi_n(F_n(\mathbf{x})).$$

For an integer $k \geq 0$ we define $\sigma_q(k)$ to be the sum of the digits in the expansion of k as a base q number and $\sigma(k)$ as the sum of the digits in the expansion of k as a base p number. Wan's Theorem ([40], Theorem 3.1) is the following:

Theorem 2.5.6 (Wan). *Let $d = \max_i d_i$ and $q = p^t$. Then the p-adic valuation of $S_q(\chi, F)$ is at least*

$$\sum_{\ell=0}^{t-1} \left\lceil \frac{r - \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i) d_i}{d} \right\rceil.$$

Here we state a slightly stronger version of the theorem, which follows immediately from the proof in [40]:

Theorem 2.5.7.

$$\nu_p(S_q(\chi, F)) \geq \sum_{\ell=0}^{t-1} \max \left\{ 0, \left\lceil \frac{r - \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i) d_i}{d} \right\rceil \right\}.$$

We will use this theorem only in the case where each F_i is a linear homogeneous function. For the convenience of the reader we specialize the proof given in [40].

Theorem 2.5.8. *For each i, $0 \le i \le n$, let $\overline{F}_i(\bar{\mathbf{x}}) = \bar{\gamma}_{i1}\bar{x}_1 + \cdots + \bar{\gamma}_{ir}\bar{x}_r$ be a linear functional on $\mathbb{F}_q^r$. Then*

$$\nu_p(S_q(\chi, \overline{F})) \ge \sum_{\ell=0}^{t-1} \max\{0, r - \frac{1}{q-1}\sum_{i=0}^{n} \sigma_q(p^\ell b_i)\}.$$

Proof: We will write

$$F_i(\mathbf{x}) = \gamma_{i1}\, x_1 + \cdots + \gamma_{ir}\, x_r$$

to represent the lifted functions from T_q^r to R with $\gamma_{ij} = T(\bar{\gamma}_{ij})$. Using the congruence

$$T(\bar{x}) \equiv x^{q^r} \pmod{q^r}$$

for all $x \in R$ we get

$$S_q(\chi, \overline{F}) \equiv \sum_{x \in {T_q}^r} \big(F_0(x)\big)^{b_0 q^r} \cdots \big(F_n(x)\big)^{b_n q^r} \pmod{q^r}. \tag{2.5}$$

Expanding (2.5) we get

$$S_q(\chi, \overline{F}) \equiv$$

$$\sum_{\substack{k_{i1} + \cdots + k_{ir} = b_i q^r \\ 0 \le i \le n}} \prod_{i=0}^{n} \binom{b_i q^r}{k_{i1}, \ldots, k_{ir}} \Big(\prod_{i=0}^{n}\prod_{j=1}^{r} {\gamma_{ij}}^{k_{ij}}\Big)\Big(\prod_{j=1}^{r}\sum_{x \in T_q} x^{\sum_i k_{ij}}\Big) \pmod{q^r} \tag{2.6}$$

We use the formula of Legendre, $\nu_p(k!) = (k - \sigma(k))/(p-1)$ and get that the p-adic valuation of the multinomial coefficient part of (2.6) is

$$\frac{1}{p-1}\sum_{i=0}^{n}\big(b_i q^r - \sigma(b_i) - \sum_{j=1}^{r}(k_{ij} - \sigma(k_{ij}))\big) = \frac{1}{p-1}\sum_{i=0}^{n}\Big(\sum_{j=1}^{r}\sigma(k_{ij}) - \sigma(b_i)\Big). \tag{2.7}$$

For the Teichmüller set T_q we have

$$\sum_{x \in T_q} x^k = \begin{cases} 0, & \text{if } (q-1) \text{ does not divide } k, \\ q, & \text{if } k = 0, \\ q-1, & \text{if } (q-1)|k \text{ and } k > 0. \end{cases} \tag{2.8}$$

Therefore, in (2.6) we only need to consider those terms for which

$$\sum_{i=0}^{n} k_{ij} \equiv 0 \pmod{q-1} \tag{2.9}$$

for all $j = 1, 2, \ldots, r$. Since $k \equiv \sigma_q(k) \pmod{q-1}$, we also have

$$\sum_{i=0}^{n} \sigma_q(k_{ij}) \equiv 0 \pmod{q-1}. \tag{2.10}$$

Given k_{ij} such that $\sum_{j=1}^{r} k_{ij} = b_i q^r$ for $0 \le i \le n$ and (2.9) is satisfied, assume that s coordinates of the vector

$$\left(\sum_{i=0}^{n} k_{i1}, \sum_{i=0}^{n} k_{i2}, \ldots, \sum_{i=0}^{n} k_{ir} \right)$$

are not identically 0. Then the same is true for the corresponding entries of the vector

$$\left(\sum_{i=0}^{n} \sigma_q(k_{i1}), \sum_{i=0}^{n} \sigma_q(k_{i2}), \ldots, \sum_{i=0}^{n} \sigma_q(k_{ir}) \right). \tag{2.11}$$

Summing up the entries of the vector in (2.11) we get

$$s(q-1) - \sum_{i=0}^{n} b_i \le \sum_{i=0}^{n} \left(\sum_{j=1}^{r} \sigma_q(k_{ij}) - b_i \right). \tag{2.12}$$

We note that for a non-negative integer ℓ, (2.10) still holds with $\sigma_q(k_{ij})$ replaced by $\sigma_q(p^\ell k_{ij})$. Also $\sum_{i=0}^{n} \sigma_q(p^\ell k_{ij})$ is not identically 0 for the same s subscripts of j. Thus we have

$$s(q-1) - \sum_{i=0}^{n} \sigma_q(p^\ell b_i) \le \sum_{i=0}^{n} \left(\sum_{j=1}^{r} \sigma_q(p^\ell k_{ij}) - \sigma_q(p^\ell b_i) \right).$$

Noting that the right-hand side is non-negative since $\sum_{j=1}^{r} k_{ij} = b_i q^r$, we sum over ℓ to get

$$\sum_{\ell=0}^{t-1} \max\left\{0, s(q-1) - \sum_{i=0}^{n} \sigma_q(p^\ell b_j)\right\} \le \frac{q-1}{p-1} \sum_{i=0}^{n} \left(\sum_{j=1}^{r} \sigma(k_{ij}) - \sigma(b_i) \right),$$

using the fact that

$$\sum_{\ell=0}^{t-1} \sigma_q(p^\ell k) = \frac{q-1}{p-1}\sigma(k).$$

Comparing with (2.7) we get that each term of (2.6) (with k_{ij} satisfying (2.9)) has p-adic valuation at least

$$t(r-s)+\sum_{l=0}^{t-1} \max\left\{0, s-\frac{1}{q-1}\sum_{i=0}^{n}\sigma_q(p^\ell b_i)\right\} \geq \sum_{l=0}^{t-1} \max\left\{0, r-\frac{1}{q-1}\sum_{i=0}^{n}\sigma_q(p^\ell b_i)\right\}.$$

This completes the proof. □

2.6 Representations of finite groups

2.6.1 Modules

We begin with the definition of a module.

Definition 2.6.1. *Let R be a ring and let M be an abelian group (with group operation written additively). We say that M is a (left) R-*module *if there is a map from $R \times M$ to M (written as juxtaposition) which satisfies the following for every $r, s \in R$ and for every $X, Y \in M$:*

1. $r(X+Y) = rX + rY$,
2. $(r+s)X = rX + sY$,
3. $(rs)X = r(sX)$,
4. $1_R X = X$
5. $0_R X = 0_M$.

*If N is a subgroup of M, we will say that N is an R-*submodule *of M if for every $r \in R$ and for every $X \in N$, $rX \in N$.*

If there exists a set of generators $\{X_1, X_2, \ldots, X_k\}$ *such that* M *is the direct sum* $RX_1 \oplus RX_2 \oplus \cdots \oplus RX_k$*, with* $RX_i \cong R$ *for each* i*, then we say that* M *is a* free *module of (finite) rank* k*.*

If the only submodules of a module M *are* M *itself and* 0*, we say that* M *is a* simple *module.*

Since a module is abelian as an additive group, every submodule is automatically a normal subgroup of every module which contains it. Additionally, the property of being a submodule is an invariance property. Under these conditions, the Jordan-Hölder theorem tells us that the composition factors of a module are well defined (see [22, pp. 130-133]).

Theorem 2.6.2 (Jordan-Hölder). *Suppose*

$$\mathcal{A} : 0 = A_0 \lhd \cdots \lhd A_a = M$$

and

$$\mathcal{B} : 0 = B_0 \lhd \cdots \lhd B_b = M$$

are two series of R*-submodules of* M*, such that each factor* A_{i+1}/A_i *for* $0 \leq i < a$ *and each factor* B_{i+1}/B_i *for* $0 \leq i < b$ *is a simple* R*-module. Then* $a = b$*, and the two lists of factor modules are rearrangements of each other up to isomorphism as* R*-modules.*

The modules we use can be thought of initially as free modules over a field (vector spaces), or free modules over the integer ring of a field. A generator set, which we will call the natural basis, will be a set of vectors indexed by geometric subspaces. For instance, in Example 2.1.3, we denote the set of projective points by $\mathcal{L}_1$ and the set of projective $(r-1)$-spaces by $\mathcal{L}_r$. We have the corresponding free modules $\mathbb{F}_q^{\mathcal{L}_1}$, $\mathbb{F}_q^{\mathcal{L}_r}$, $R^{\mathcal{L}_1}$, and $R^{\mathcal{L}_r}$.

Now let the general linear group $G = \mathrm{GL}(n+1, \mathbb{F}_q)$ have its natural permutation action on $\mathcal{L}_1$ and on $\mathcal{L}_r$. We extend this action linearly to an action of

the group ring $\mathbb{F}_q G$ on the free modules, which we continue to call $\mathbb{F}_q^{\mathcal{L}_1}$ and $\mathbb{F}_q^{\mathcal{L}_r}$ as $\mathbb{F}_q G$-modules. We similarly extend the action of G linearly to get the RG-modules $R^{\mathcal{L}_1}$, and $R^{\mathcal{L}_r}$.

2.6.2 Representations

Definition 2.6.3. *An* F-representation *of a finite group* G *is a homomorphism from* G *to the general linear group* $\mathrm{GL}(v, F)$ *for some positive integer* v.

Since every group permutes its own elements by multiplication, every finite group has the *regular* representation of these $|G| \times |G|$ permutation matrices. It is also true that for a field F, every FG-module M can be viewed as an F-representation of G in $\mathrm{GL}(v, F)$ with v now being the dimension of M as an F-vector space. In particular, every submodule is also a representation. Thus representation theory and submodule structure are closely intertwined. In Section 3.4 will will give the complete module structure of $\mathbb{F}_q^{\mathcal{L}_1}$, which was determined by Bardoe and Sin in [7].

Chapter 3

THE STATEMENT OF THEOREM A

3.1 The incidence map

We have defined $A = (a_{i,j})$ to be the incidence matrix with columns indexed by points of $\mathrm{PG}(n, q)$ and rows indexed by $(r-1)$-dimensional projective subspaces of $\mathrm{PG}(n, q)$ (referred to as r-subspaces), and with $a_{i,j} = 1$ if the j^{th} point is contained in the ith r-subspace. We can view A as a linear map from the module $\mathbb{Z}^{\mathcal{L}_1}$ to the module $\mathbb{Z}^{\mathcal{L}_r}$ as follows:

Definition 3.1.1. *Let V be an $(n+1)$-dimensional vector space over $\mathbb{F}_q$ as before, and let $\mathcal{L}_r$ and $\mathcal{L}_s$ be the sets of r-dimensional and s-dimensional vector subspaces of V, respectively. If $Z \in \mathcal{L}_r$ and $Y \in \mathcal{L}_s$, we will say that Z is incident with Y, and write $Z \sim Y$, if either $Z \subset Y$ or $Y \subset Z$. We define the map*

$$\eta_{r,s} : \mathbb{Z}^{\mathcal{L}_r} \to \mathbb{Z}^{\mathcal{L}_s} \tag{3.1}$$

by letting

$$\eta_{r,s}(Z) = \sum_{Y \in \mathcal{L}_s, Z \sim Y} Y$$

for every $Z \in \mathcal{L}_r$, and then extending $\eta_{r,s}$ linearly to $\mathbb{Z}^{\mathcal{L}_r}$. In particular, if we write $U \in \mathbb{Z}^{\mathcal{L}_1}$ as a column vector indexed by points, then AU is the column vector indexed by r-subspaces representing $\eta_{1,r}(U)$.

Note that we are using the same symbols, Y and Z, both to denote subspaces of V, and to denote basis vectors of the respective modules.

Also, if $s \leq \ell \leq r$ or $s \geq \ell \geq r$, we have the composition maps:

$$\begin{aligned} \eta_{\ell,r} \circ \eta_{s,\ell} &= \begin{bmatrix} r-s \\ \ell-s \end{bmatrix}_q \eta_{s,r} \\ \eta_{\ell,s} \circ \eta_{r,\ell} &= \begin{bmatrix} r-s \\ \ell-s \end{bmatrix}_q \eta_{r,s}. \end{aligned} \tag{3.2}$$

The reason is that $\eta_{s,\ell}$ maps $Y \in \mathcal{L}_s$ to all those elements of $\mathcal{L}_\ell$ which are incident with Y. Those elements of $\mathcal{L}_\ell$ which are incident with both Y and Z contribute 1 to the coefficient of Z in $\eta_{\ell,r} \circ \eta_{s,\ell}(Y)$. If $Y \sim Z$, the total number of such elements of $\mathcal{L}_\ell$ is $\begin{bmatrix} r-s \\ \ell-s \end{bmatrix}_q$, while if Y and Z are not incident, there are no intermediate elements of $\mathcal{L}_\ell$.

In Section 3.5 we will state the Smith normal form of A.

3.2 The p'-part of the Smith normal form of $\mathrm{PG}(n, q)$

In this section we give the part of the Smith normal form of $\mathrm{PG}(n, q)$ which is coprime to p. Let $q = p^t$, and let V be an $(n+1)$-dimensional space over $\mathbb{F}_q$. As before we use A to denote the $|\mathcal{L}_r| \times |\mathcal{L}_1|$ matrix of the linear map $\eta_{1,r} : \mathbb{Z}^{\mathcal{L}_1} \to \mathbb{Z}^{\mathcal{L}_r}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{L}_1}$ and $\mathbb{Z}^{\mathcal{L}_r}$. It is known that all invariant factors of A (as a matrix over $\mathbb{Z}$) are p-powers except the last one, which is also divisible by $(q^r - 1)/(q - 1)$. In [37], a proof was given using the structure of the permutation module for $\mathrm{GL}(n+1, q)$ acting on $\mathcal{L}_1$ over fields of characteristic prime to p. We give an elementary proof of the result.

Theorem 3.2.1. *Let A be the matrix of the map $\eta_{1,r}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{L}_r}$ and $\mathbb{Z}^{\mathcal{L}_1}$, and let $v = |\mathcal{L}_1|$. The invariant factors of A are all p-powers except for the v^{th} invariant, which is a p-power times $(q^r - 1)/(q - 1)$.*

Proof: It will be more convenient to work with the map $\eta_{r,1} : \mathbb{Z}^{\mathcal{L}_r} \to \mathbb{Z}^{\mathcal{L}_1}$, which we define to be the linear map sending each element of $\mathcal{L}_r$ to the formal sum of all the 1-spaces incident with it. Then the matrix of $\eta_{r,1}$ with respect to the standard

bases of $\mathbb{Z}^{\mathcal{L}_r}$ and $\mathbb{Z}^{\mathcal{L}_1}$ is $A^\top$. Let $A^\top = PDQ$, where P and Q are two unimodular matrices of order $|\mathcal{L}_1|$ and $|\mathcal{L}_r|$ respectively, and D is the Smith normal form of $A^\top$ with diagonal entries $d_1, d_2, \ldots, d_v$. Let y_i be the i^{th} column of P, $1 \leq i \leq v$. Then $\{y_i : 1 \leq i \leq v\}$ and $\{d_i y_i : 1 \leq i \leq v\}$ are bases of the free $\mathbb{Z}$-modules $\mathbb{Z}^{\mathcal{L}_1}$ and $\mathrm{Im}(\eta_{r,1})$ respectively.

We define the augmentation map

$$\epsilon : \mathbb{Z}^{\mathcal{L}_1} \to \mathbb{Z}$$

to be the function sending each element in $\mathcal{L}_1$ to 1. Clearly ϵ maps $\mathbb{Z}^{\mathcal{L}_1}$ onto $\mathbb{Z}$ and $\epsilon \circ \eta_{r,1}$ maps $\mathbb{Z}^{\mathcal{L}_r}$ onto $\frac{q^r-1}{q-1}\mathbb{Z}$. As a consequence,

$$\epsilon(y_i) d_i \in \frac{q^r - 1}{q - 1}\mathbb{Z},$$

for all $i = 1, 2, \ldots, v$.

First we show that $\frac{q^r-1}{q-1}$ indeed divides d_v. Let ℓ be a prime. If $\ell^\beta \mid \frac{q^r-1}{q-1}$ but $\ell^\beta \nmid d_v$ then ℓ^β does not divide any of the invariants d_i. Note that $\ell^\beta \mid \frac{q^r-1}{q-1}$, which in turn divides $\epsilon(y_i)d_i$ for all i, so ℓ must be a common divisor of $\epsilon(y_i)$, $i = 1, 2, \ldots, v$. This contradicts with the fact that ϵ is a surjective map from $\mathbb{Z}^{\mathcal{L}_1}$ to $\mathbb{Z}$.

Next we show that if the index $[\mathrm{Ker}(\epsilon) : \mathrm{Ker}(\epsilon) \cap \mathrm{Im}(\eta_{r,1})]$ is a p-power, then the theorem holds. (Note that $[\mathrm{Ker}(\epsilon) : \mathrm{Ker}(\epsilon) \cap \mathrm{Im}(\eta_{r,1})]$ is a p-power if and only if for any $x \in \mathrm{Ker}(\epsilon)$ there is a positive integer α such that $p^\alpha x \in \mathrm{Im}(\eta_{r,1})$.) Assume to the contrary that there exists some prime $\ell \neq p$ such that $\ell \mid d_i$ for some $i < v$ or $\ell \cdot \frac{q^r-1}{q-1} \mid d_v$.

Suppose that $\ell \mid d_i$ for some $i < v$. Since ϵ is surjective there exists a basis vector y_k such that $\ell \nmid \epsilon(y_k)$.

If $i \neq k$, then

$$x = \epsilon(y_k)\, y_i - \epsilon(y_i)\, y_k$$

is a nonzero vector in $\mathrm{Ker}(\epsilon)$. Since $\ell \nmid \epsilon(y_k)$ and $\ell \mid d_i$, $p^\alpha \epsilon(y_k)$ can not be a multiple of d_i for any α, hence $p^\alpha x \notin \mathrm{Im}(\eta_{r,1})$ for any α, a contradiction.

If $i = k < v$, then instead we consider the nonzero vector

$$x := \epsilon(y_k)\, y_v - \epsilon(y_v)\, y_k$$

in $\mathrm{Ker}(\epsilon)$. Since $\ell \nmid \epsilon(y_k)$ and $\ell \mid d_i \mid d_v$, $p^\alpha \epsilon(y_k)$ can not be a multiple of d_v for any α, hence $p^\alpha x \notin \mathrm{Im}(\eta_{r,1})$ for any α, again a contradiction.

Now suppose that $\ell \cdot \frac{q^r-1}{q-1} \mid d_v$. Note that $\frac{q^r-1}{q-1} \mid \epsilon(y_i) d_i$ for each i, but for some k that

$$\ell \cdot \frac{q^r-1}{q-1} \nmid \epsilon(y_k) d_k,$$

since $\epsilon \circ \eta_{r,1}$ is a surjective map from $\mathbb{Z}^{\mathcal{L}_r}$ to $\frac{q^r-1}{q-1}\mathbb{Z}$. So $\ell \nmid \epsilon(y_k) d_k$. We similarly get a contradiction by considering the nonzero vector $\epsilon(y_k)\, y_v - \epsilon(y_v)\, y_k$ in $\mathrm{Ker}(\epsilon)$.

To finish the proof of the theorem, we are reduced to showing that

$$(\mathrm{Ker}\, \epsilon + \mathrm{Im}\, \eta_{r,1}) / \mathrm{Im}\, \eta_{r,1}$$

is a p-group. We show that if $x \in \mathrm{Ker}\, \epsilon$ then $q^{r-1} x \in \mathrm{Im}\, \eta_{r,1}$. Now $\mathrm{Ker}\, \epsilon$ is spanned by vectors of the form $u - w$, where u and w are vectors representing individual elements in $\mathcal{L}_1$, so it is enough to show that $q^{r-1}(u-w)$ is in $\mathrm{Im}\, \eta_{r,1}$. Let U be some $(r+1)$-subspace of V which contains both u and w. We define $\tilde{\eta}_{1,r}$ to be the linear map which maps a projective point to the formal sum of the r-subspaces which both contain the point and are contained in U and define $\mathbf{j}_U$ to be the formal sum of all the projective points inside U. Then $\eta_{r,1}$ restricted to r-subspaces inside U and $\tilde{\eta}_{1,r}$ are simply the hyperplane-to-point and point-to-hyperplane maps for the space U. By standard formula from design theory we have

$$\eta_{r,1}(\tilde{\eta}_{1,r}(z)) = q^{r-1} z + \frac{q^{r-1}-1}{q-1} \mathbf{j}_U$$

for every $z \in \mathcal{L}_1$. Hence by setting $z = u$ and $z = w$ respectively, and subtracting the resulting equations, we get

$$\eta_{r,1}(\tilde{\eta}_{1,r}(u-w)) = q^{r-1}(u-w)$$

which is the desired result. □

Note: A shorter proof of this theorem can be found in [11].

In view of Theorem 3.2.1, in order to get the Smith normal form of A, we just need to view A as a matrix with entries from $\mathbb{Z}_p$, the ring of p-adic integers, and get its Smith normal form over $\mathbb{Z}_p$. This will be the approach we take. To state Theorem A, we need to explain the monomial basis developed in [7].

3.3 Monomial bases

As we have seen, most of the invariant factors of A are p-powers. It will be helpful to view the entries of A as coming from some p-adic local ring. Let $q = p^t$ and let $K = \mathbb{Q}_p(\xi_{q-1})$ be the unique unramified extension of degree t over $\mathbb{Q}_p$, the field of p-adic numbers, where ξ_{q-1} is a primitive $(q-1)^{\text{th}}$ root of unity in K. Let $R = \mathbb{Z}_p[\xi_{q-1}]$ be the ring of integers in K and let $\mathfrak{p}$ be the unique maximal ideal in R. Then R is a principal ideal domain, and the reduction of $R \pmod{\mathfrak{p}}$ will be $\mathbb{F}_q$. Define $\bar{x}$ to be $x \pmod{\mathfrak{p}}$ for $x \in R$. Let T_q be the set of roots of $x^q = x$ in R (a Teichmüller set) and let T be the Teichmüller character of $\mathbb{F}_q$, so that $T(\bar{x}) = x$ for $x \in T_q$. We will use T to lift a basis of $\mathbb{F}_q^{\mathcal{L}_1}$ to a basis of $R^{\mathcal{L}_1}$.

In (3.1), we defined the map $\eta_{1,r}$ from $\mathbb{Z}^{\mathcal{L}_1}$ to $\mathbb{Z}^{\mathcal{L}_r}$. Now we use the same $\eta_{1,r}$ to denote the map from $R^{\mathcal{L}_1}$ to $R^{\mathcal{L}_r}$ sending a 1-space to the formal sum of all r-spaces incident with it. The matrix A is then the matrix of $\eta_{1,r}$ with respect to the (standard) basis $\mathcal{L}_1$ of $R^{\mathcal{L}_1}$ and the (standard) basis $\mathcal{L}_r$ of $R^{\mathcal{L}_r}$. Crucial to our approach of finding the Smith form of A is what we call a monomial basis for $R^{\mathcal{L}_1}$. We introduce this basis below.

We start with the monomial basis of $\mathbb{F}_q^{\mathcal{L}_1}$. This basis was discussed in detail in [7]. Let $V = \mathbb{F}_q^{n+1}$. Then V has a standard basis $v_0, v_1, \ldots, v_n$, where

$$v_i = (\underbrace{0, 0, \ldots, 0, 1}_{i+1}, 0, \ldots, 0).$$

We regard $\mathbb{F}_q^V$ as the space of functions from V to $\mathbb{F}_q$. Any function $f \in \mathbb{F}_q^V$ can be given as a polynomial function of $n+1$ variables corresponding to the $n+1$ coordinate positions: write the vector $\mathbf{x} \in V$ as

$$\mathbf{x} = (x_0, x_1, \ldots, x_n) = \sum_{i=0}^{n} x_i v_i;$$

then $f = f(x_0, x_1, \ldots, x_n)$. The function x_i is, for example, the linear functional that projects a vector in V onto its i^{th} coordinate in the standard basis.

As a function on V, $x_i^q = x_i$, for each $i = 0, 1, \ldots, n$, so we obtain all the functions via the q^{n+1} monomial functions

$$\left\{ \prod_{i=0}^{n} x_i^{b_i} \mid 0 \leq b_i < q, i = 0, 1, \ldots, n \right\}. \tag{3.3}$$

Since the characteristic function of $\{0\}$ in V is $\prod_{i=0}^{n}(1 - x_i^{q-1})$, we obtain a basis for $\mathbb{F}_q^{V\setminus\{0\}}$ by excluding $x_0^{q-1}x_1^{q-1}\cdots x_n^{q-1}$ from the set in (3.3).

The functions on $V \setminus \{0\}$ which descend to $\mathcal{L}_1$ are exactly those which are invariant under scalar multiplication by $\mathbb{F}_q^*$. Therefore we obtain a basis $\mathcal{M}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ as follows.

$$\mathcal{M} = \left\{ \prod_{i=0}^{n} x_i^{b_i} \mid 0 \leq b_i < q, \sum_i b_i \equiv 0 \pmod{q-1}, \right.$$
$$\left. (b_0, b_1, \ldots, b_n) \neq (q-1, q-1, \ldots, q-1) \right\}.$$

This basis $\mathcal{M}$ will be called the *monomial basis* of $\mathbb{F}_q^{\mathcal{L}_1}$, and its elements are called *basis monomials*.

Now we lift the function $x_i : V \to \mathbb{F}_q$ to a function $T(x_i) : V \to R$, where T is the Teichmüller character of $\mathbb{F}_q$. For $(a_0, a_1, \ldots, a_n) \in V$, we have

$$T(x_i)(a_0, a_1, \ldots, a_n) = T(a_i) \in R.$$

For each basis monomial $\prod_{i=0}^{n} x_i^{b_i}$, we define $T(\prod_{i=0}^{n} x_i^{b_i})$ similarly. We have the following lemma.

Lemma 3.3.1. *The elements in the set*

$$\mathcal{M}_R = \left\{ T(\prod_{i=0}^{n} x_i^{b_i}) \mid 0 \leq b_i < q, \quad \sum_i b_i \equiv 0 \pmod{q-1}, \right.$$
$$\left. (b_0, b_1, \ldots, b_n) \neq (q-1, q-1, \ldots, q-1) \right\}$$

form a basis of the free R-module $R^{\mathcal{L}_1}$.

Proof: To simplify notation, we use M to denote the free R-module $R^{\mathcal{L}_1}$, set $v = |\mathcal{L}_1|$, and enumerate the elements of $\mathcal{M}_R$ as $f_1, f_2, \ldots, f_v$. Since the images of the elements of $\mathcal{M}_R$ in the quotient $M/\mathfrak{p}M$ are exactly the elements in $\mathcal{M}$, which form a basis of $\mathbb{F}_q^{\mathcal{L}_1} \cong M/\mathfrak{p}M$ (as vector spaces over $\mathbb{F}_q$) , by Nakayama's lemma [5], the elements in $\mathcal{M}_R$ generate N and since their number equals $\operatorname{rank} M$, they form a basis. □

The basis $\mathcal{M}_R$ will be called the *monomial basis* of $R^{\mathcal{L}_1}$, and its elements are called *basis monomials*.

3.4 The module structure of $\mathbb{F}_q{}^{\mathcal{L}_1}$

In this section we state the main results of [7]. We give a modified version of the proof in Section 5.5.

Let $\mathcal{H}$ denote the set of t-tuples $\xi = (s_0, s_1, \ldots, s_{t-1})$ of integers satisfying (for $0 \le j \le t-1$) the following:

$$\begin{aligned} &(1) \quad 1 \le s_j \le n, \\ &(2) \quad 0 \le ps_{j+1} - s_j \le (p-1)(n+1), \end{aligned} \tag{3.4}$$

with the subscripts read (mod t). The set $\mathcal{H}$ was introduced in [19], and used in [7] to describe the module structure of $\mathbb{F}_q^{\mathcal{L}_1}$ under the natural action of $\mathrm{GL}(n+1, q)$.

For a nonconstant basis monomial

$$f(x_0, x_1, \ldots, x_n) = x_0^{b_0} \cdots x_n^{b_n},$$

in $\mathcal{M}$, we expand the exponents

$$b_i = a_{i,0} + pa_{i,1} + \cdots + p^{t-1}a_{i,t-1} \quad 0 \le a_{i,j} \le p-1$$

and let

$$\lambda_j = a_{0,j} + \cdots + a_{n,j}. \tag{3.5}$$

Because the total degree $\sum_{i=0}^{n} b_i$ is divisible by $q-1$, there is a uniquely defined t-tuple $(s_0, \ldots, s_{t-1}) \in \mathcal{H}$ [7] such that

$$\lambda_j = ps_{j+1} - s_j.$$

Explicitly

$$s_j = \frac{1}{q-1} \sum_{i=0}^{n} \Big(\sum_{\ell=0}^{j-1} p^{\ell+t-j} a_{i,\ell} + \sum_{\ell=j}^{t-1} p^{\ell-j} a_{i,\ell} \Big) \tag{3.6}$$

One way of interpreting the numbers s_j is that the total degree of f^{p^i} is $s_{t-i}(q-1)$, when the exponent of each coordinate x_i is reduced to be no more than $q-1$ by the substitution $x_i^q = x_i$. We will say that f is of *type* $\xi = (s_0, s_1, \ldots, s_{t-1})$. Also we say

that the corresponding basis monomial $T(f) \in \mathcal{M}_R$ is of *type* ξ. (Note that in [7] ξ is called *a tuple in* $\mathcal{H}$ and the term *type* is used for certain other t-tuples in bijection with $\mathcal{H}$. However, since we will not use the latter there is no risk of confusion.)

Let d_i be the coefficient of x^i in the expansion of $(\sum_{k=0}^{p-1} x^k)^{n+1}$. Explicitly,

$$d_i = \sum_{j=0}^{\lfloor i/p \rfloor} (-1)^j \binom{n+1}{j} \binom{n+i-jp}{n}.$$

Lemma 3.4.1. *Let d_i and λ_j be as defined above. The number of basis monomials in both $\mathcal{M}$ and $\mathcal{M}_R$ of type $\xi = (s_0, s_1, \ldots, s_{t-1})$ is $\prod_{j=0}^{t-1} d_{\lambda_j}$.*

Proof: From (3.5) each λ_j is the sum of $n+1$ integers which can be anywhere from 0 to $p-1$. The number of such choices is the same as the coefficient of x^{λ_j} in $(\sum_{k=0}^{p-1} x^k)^{n+1}$. Counting the choices for each λ_j as j runs from 0 to $t-1$ we get $\prod_{j=0}^{t-1} d_{\lambda_j}$. □

We can now state the complete submodule structure of $\mathbb{F}_q^{\mathcal{L}_1}$ ([7, Theorem A]).

Theorem 3.4.2. *Let $\mathbb{F}_q^{\mathcal{L}_1}$ be the $\mathbb{F}_q G$-module as above. Every $\mathbb{F}_q G$-submodule W of $\mathbb{F}_q^{\mathcal{L}_1}$ consists of the subspace of functions from $\mathcal{L}_1$ to $\mathbb{F}_q$ which is spanned by certain basis monomials. If one basis monomial of a certain type $(s_0, s_1, \ldots, s_{t-1})$ is in W, then every basis monomial of type $(s'_0, s'_1, \ldots, s'_{t-1})$ is also in W if $1 \leq s'_i \leq s_i$ for each $i \in 0, \ldots, t-1$. In particular, $\mathbb{F}_q^{\mathcal{L}_1}$ is the direct sum of the span of the all-one function (of type $(0, \ldots, 0)$) and the span of all the other monomial functions. Either the constant functions are in W, or all the functions in W can be expressed in terms of nonconstant monomials only.*

The following corollary is [7, Theorem B].

Corollary 3.4.3. *Let $f(x_0, \ldots, x_n)$ be a polynomial function in $\mathbb{F}_q^{\mathcal{L}_1}$ and let $\mathcal{H}_f \subset \mathcal{H} \cup \{(0, \ldots, 0)\}$ be the set of the tuples $(s_0, \ldots, s_{t-1})$ of the basis monomials appearing with nonzero coefficients in the expression for f. Then the submodule generated by f is the smallest submodule containing all those basis monomials.*

Proof: Every submodule is spanned by the basis monomials which it contains. □

3.5 The Smith normal form of $\mathrm{PG}(n, q)$

We can now state the main theorem.

Theorem 3.5.1 (Theorem A). *Let $\mathcal{L}_1$ be the set of projective points and let $\mathcal{L}_r$ be the set of projective $(r-1)$-spaces in $\mathrm{PG}(n, q)$, and let d_i and $\mathcal{H}$ be as above. For each t-tuple $\xi = (s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H}$ let*

$$\lambda_i = ps_{i+1} - s_i$$

and let

$$d_\xi = \prod_{i=0}^{t-1} d_{\lambda_i}.$$

Then the p-adic invariant factors of the incidence matrix A between $\mathcal{L}_1$ and $\mathcal{L}_r$ are p^α, $0 \leq \alpha \leq (r-1)t$, with multiplicity

$$m_\alpha = \sum_{\xi \in \mathcal{H}_\alpha} d_\xi + \delta(0, \alpha)$$

where

$$\mathcal{H}_\alpha = \Big\{(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H} \mid \sum_{i=0}^{t-1} \max\{0, r - s_i\} = \alpha\Big\}, \tag{3.7}$$

and

$$\delta(0, \alpha) = \begin{cases} 1, & \text{if } \alpha = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{3.8}$$

Remark 3.5.2. *The theorem was conjectured by Liebler and Sin [30].*

Remark 3.5.3. *The multiplicity of 1 among the p-adic invariant factors, m_0, is exactly the p-rank of A. From Theorem 3.5.1, we have*

$$m_0 = 1 + \sum_{(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H}, s_i \geq r, \forall i} d_{(s_0, s_1, \ldots, s_{t-1})}.$$

We mention that $d_{(s_0,\ldots,s_{t-1})} = d_{(n+1-s_0,\ldots,n+1-s_{t-1})}$ *for each* $(s_0,\ldots,s_{t-1}) \in \mathcal{H}$, $d_i = 0$ *if* $i < 0$, $d_{(0,\ldots,0)} = d_{(n+1,\ldots,n+1)} = 1$ *(but we are not counting the monomial of type* $(n+1,\ldots,n+1)$*), and* $d_\xi = 0$ *for all other cases that* $\xi \notin \mathcal{H}$*. So the above p-rank formula is the same as the formula of Hamada [19].*

Remark 3.5.4. *We also mention that the largest* α *of the exponents of the p-adic invariant factors of A is* $(r-1)t$*. It arises in the case where* $\xi = (1,1,\ldots,1)$*. From Theorem 3.5.1, we find that the multiplicity of* $p^{(r-1)t}$ *is*

$$m_{(r-1)t} = d_{(1,1,\ldots,1)} = \binom{n+p-1}{n}^t,$$

which is one less than the p-rank of $\eta_{1,n}$*.*

We indicate how we proceed to prove Theorem 3.5.1. In order to get the Smith normal form of A over R, we will find two invertible matrices P and Q^{-1} with entries in R, such that

$$A = PDQ^{-1},$$

where D is a $|\mathcal{L}_r| \times |\mathcal{L}_1|$ diagonal matrix with p powers on its diagonal. The matrices Q and P will come from basis changes in $R^{\mathcal{L}_1}$ and $R^{\mathcal{L}_r}$ respectively.

Let $\{e_1, e_2, \ldots, e_v\}$, where $v = |\mathcal{L}_1|$, be the standard basis of $R^{\mathcal{L}_1}$, and let $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ be the monomial basis of $R^{\mathcal{L}_1}$ constructed in Lemma 3.3.1. For $1 \le j \le v$, let $f_j = \sum_{i=1}^{v} q_{ij} e_i$, $q_{ij} \in R$, and let $Q = (q_{ij})$. Then

$$\eta_{1,r}(f_j) = \sum_{i=1}^{v} q_{ij} \eta_{1,r}(e_i).$$

Therefore the columns of AQ are the vectors $\eta_{1,r}(f_j)$, written with respect to the standard basis of $R^{\mathcal{L}_r}$. For $1 \le j \le v$, let p^{a_j} be the largest power of p dividing

every coordinate of $\eta_{1,r}(f_j)$. Then we factorize AQ as PD, where

$$D = \begin{pmatrix} p^{\alpha_1} & 0 & 0 & \cdots & 0 \\ 0 & p^{\alpha_2} & 0 & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & p^{\alpha_{v-1}} & 0 \\ 0 & & \cdots & 0 & p^{\alpha_v} \\ 0 & & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix},$$

and P is an $|\mathcal{L}_r| \times |\mathcal{L}_r|$ matrix whose first v columns are $\frac{1}{p^{\alpha_j}}\eta_{1,r}(f_j)$, $j = 1, 2, \ldots, v$. The matrix D will be the Smith normal form of A if the determinant of P is a unit of R. First we find a lower bound on the numbers α_j, the minimum p-adic valuations of the coordinates of $\eta_{1,r}(f_j)$. Let f_j be a typical basis monomial $T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})$ in $\mathcal{M}_R$, and let $Y \in \mathcal{L}_r$. Then the Y-coordinate of $\eta_{1,r}(f_j)$ is

$$\begin{aligned} \eta_{1,r}(f_j)(Y) &= \sum_{Z \subset Y, Z \in \mathcal{L}_1} f_j(Z) \\ &= \frac{1}{q-1} \sum_{\mathbf{x} \in \mathbb{F}_q^{n+1} \setminus \{(0,0,\ldots,0)\}, \mathbf{x} \in Y} T^{b_0}(x_0)T^{b_1}(x_1)\cdots T^{b_n}(x_n), \end{aligned}$$

where in the last summation, $\mathbf{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$. Therefore the coordinates of $\eta_{1,r}(f_j)$ are all multiplicative character sums. Thanks to a theorem of Wan [40], one can indeed obtain lower bounds on the p-adic valuations of these multiplicative character sums. We discuss Wan's theorem and its application in Chapter 5.

Chapter 4

THE HYPERPLANE CASE

4.1 An explicit formula

Sin proved Theorem A in the case $r = n$, that is for hyperplanes, using representation theory ([36]). Liebler [30] also had a proof for the same case using Gauss sums. Even though we prove Theorem A in the general case in Chapter 5, we give here a new proof of the theorem in the case $r = n$. In the process we derive an explicit formula for $\eta_{1,n}(f)$ for any basis monomial f in $\mathcal{M}_R$. The formula involves p-adic Gauss sums. The Smith form for $\eta_{1,n}$ follows from Stickelberger's theorem (see [21]). Let T^b be a multiplicative p-adic character of $\mathbb{F}_q$, tr the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$, and ξ_p a p-adic primitive p^{th} root of unity. The p-adic Gauss sum is defined to be

$$g(T^b) = \sum_{x \in \mathbb{F}_q} T^b(x) {\xi_p}^{\text{tr}(x)}.$$

We also need the Jacobi sums for more than two multiplicative characters (see [21, p. 98-100]).

$$\begin{aligned} J_0(\chi_0, \ldots, \chi_n) &= \sum_{\substack{\mathbf{x} \in {\mathbb{F}_q}^{n+1} \\ x_0 + \cdots + x_n = 0}} \chi_0(x_0) \cdots \chi_n(x_n) \\ J(\chi_0, \ldots, \chi_n) &= \sum_{\substack{\mathbf{x} \in {\mathbb{F}_q}^{n+1} \\ x_0 + \cdots + x_n = 1}} \chi_0(x_0) \cdots \chi_n(x_n) \end{aligned}$$

We state explicitly the image of any monomial function.

Proposition 4.1.1. *Let $f(\mathbf{x}) = T({x_0}^{b_0} \cdots {x_n}^{b_n})$ be a basis monomial in $\mathcal{M}_R$. The coordinate of $\eta_{1,n}(f)$ indexed by the hyperplane $\gamma_0\, x_0 + \cdots + \gamma_n\, x_n = 0$ is*

$$\frac{1}{q}\prod_{i=0}^{n}\phi_i + \frac{1}{q(q-1)}\prod_{i=0}^{n}\theta_i - \frac{1}{q-1}\prod_{i=0}^{n}\psi_i \tag{4.1}$$

where

$$\phi_i \;=\; \begin{cases} g(T^{b_i})T(\gamma_i)^{-b_i} & \text{if } \; 0 < b_i < q-1 \\ (1 - T(\gamma_i)^{q-1})q & \text{if } \; b_i = 0 \\ (1 - T(\gamma_i)^{q-1})q - 1 & \text{if } \; b_i = q-1 \end{cases} \tag{4.2}$$

$$\theta_i \;=\; \begin{cases} 0 & \text{if } \; 0 < b_i < q-1 \\ q & \text{if } \; b_i = 0 \\ q-1 & \text{if } \; b_i = q-1 \end{cases} \tag{4.3}$$

$$\psi_i \;=\; \begin{cases} 1 & \text{if } \; b_i = 0 \\ 0 & \text{if } \; b_i \neq 0 \end{cases} \tag{4.4}$$

Proof: Let Y denote the hyperplane in $\mathcal{L}_n$ defined by the equation $\gamma \cdot \mathbf{x} = 0$, where $\gamma = (\gamma_0, \ldots, \gamma_n)$, $\mathbf{x} = (x_0, x_1, \ldots, x_n) \in {\mathbb{F}_q}^{n+1}$ and $\gamma \cdot \mathbf{x} = \gamma_0 x_0 + \cdots + \gamma_n x_n$. The Y-coordinate of $\eta_{1,n}(f)$ is

$$\eta_{1,n}(f)(Y) = \frac{1}{q-1} \sum_{\substack{\mathbf{x} \in {\mathbb{F}_q}^{n+1} \\ \mathbf{x} \neq (0,\ldots,0) \\ \gamma \cdot \mathbf{x} = 0}} T^{b_0}(x_0)T^{b_1}(x_1)\cdots T^{b_n}(x_n). \tag{4.5}$$

We will compute $\eta_{1,n}(f)(Y)$ explicitly by considering three cases.

Case 1: *Some exponent b_ℓ in f is strictly between 0 and $q-1$.* In this case (4.1) reduces to $\frac{1}{q}\prod_{i=0}^{n}\phi_i$ because $\theta_\ell = \psi_\ell = 0$.

First we consider the case where all the exponents b_i are strictly between 0 and $q-1$. If all the γ_i's are nonzero, then

$$\begin{aligned}\eta_{1,n}(f)(Y) &= \frac{T^{-1}(\prod_{i=0}^{n}\gamma_i^{b_i})}{q-1}\sum_{\gamma\cdot\mathbf{x}=0}T^{b_0}(\gamma_0x_0)\cdots T^{b_n}(\gamma_nx_n)\\ &= \frac{T^{-1}(\prod_{i=0}^{n}\gamma_i^{b_i})}{q-1}J_0(T^{b_0},\ldots,T^{b_n}) \qquad (4.6)\end{aligned}$$

from the definition of the Jacobi sum, while if $\gamma_i = 0$ for some i, (4.5) is 0 because $\sum_{x_i\in\mathbb{F}_q}T^{b_i}(x_i) = \sum_{x_i\in\mathbb{F}_q^*}T^{b_i}(x_i)0$ and (4.6) is also 0 because $\prod_{i=0}^{n}\gamma_i^{b_i} = 0$. Hence (4.6) is valid in both cases.

Since $(q-1)\,|\,(b_0+\cdots+b_n)$ and $\sum_{i=0}^{n}b_i \neq 0$, by our convention, $T^{b_0}\cdots T^{b_n}$ is the multiplicative character of $\mathbb{F}_q$ sending 0 to 0, and every nonzero element of $\mathbb{F}_q$ to 1. Note that none of the individual characters T^{b_i} is trivial. We have (see [21, p. 98-100] for details)

$$\begin{aligned}J_0(T^{b_0},T^{b_1},\ldots,T^{b_n}) &= T^{b_n}(-1)(q-1)J(T^{b_0},T^{b_1},\ldots,T^{b_{n-1}}),\\ g(T^{b_0})g(T^{b_1})\cdots g(T^{b_{n-1}}) &= J(T^{b_0},T^{b_1},\ldots,T^{b_{n-1}})g(T^{b_0+b_1+\cdots+b_{n-1}}),\\ g(T^{b_n})g(T^{-b_n}) &= qT^{b_n}(-1).\end{aligned}$$

Combining the above identities with the fact that $T^{b_0}\cdots T^{b_{n-1}} = T^{-b_n}$, we have

$$\begin{aligned}\eta_{1,n}(f)(Y) &= \frac{T^{-1}(\prod_{i=0}^{n}\gamma_i^{b_i})}{q-1}J_0(T^{b_0},\ldots,T^{b_n})\\ &= \frac{T^{-1}(\prod_{i=0}^{n}\gamma_i^{b_i})}{q}g(T^{b_0})\cdots g(T^{b_n})\\ &= \frac{1}{q}\prod_{i=0}^{n}\phi_i.\end{aligned}$$

Now suppose that all but one b_i are strictly between 0 and $q-1$. Without loss of generality, assume that $b_0 = 0$ or $q-1$, and $0 < b_i < q-1$ for $i = 1,2,\ldots,n$.

If $b_0 = 0$ and $\gamma_0 = 0$, then

$$\eta_{1,n}(f)(Y) = q \cdot \frac{1}{q-1} \sum_{\substack{\mathbf{x} \in \mathbb{F}_q{}^n \\ \sum_{i=1}^n \gamma_i x_i = 0}} T^{b_1}(x_1) \cdots T^{b_n}(x_n),$$

which, by our computations above, is equal to

$$q \cdot \frac{1}{q} \prod_{i=1}^n \phi_i = \frac{1}{q}\Big((1 - T(\gamma_0)^{q-1})q\Big) \prod_{i=1}^n \phi_i = \frac{1}{q} \prod_{i=0}^n \phi_i.$$

If $b_0 = 0$ and $\gamma_0 \neq 0$, then we can solve for x_0 and the values of $x_1, \ldots, x_n$ are unrestricted. We have

$$\eta_{1,n}(f)(Y) = \frac{1}{q-1} \prod_{i=1}^n \sum_{x_i \in \mathbb{F}_q} T^{b_i}(x_i) = 0,$$

since T^{b_i} is nontrivial for $i = 1, 2, \ldots, n$. Hence in this case we also have

$$\eta_{1,n}(f)(Y) = \frac{1}{q}\Big((1 - T(\gamma_0)^{q-1})q\Big) \prod_{i=1}^n \phi_i.$$

If $b_0 = q - 1$ and $\gamma_0 = 0$, then we sum over nonzero values of x_0.

$$\eta_{1,n}(f)(Y) = \frac{q-1}{q} \prod_{i=1}^n \phi_i = \frac{1}{q}\Big((1 - T(\gamma_0)^{q-1})q - 1\Big) \prod_{i=1}^n \phi_i.$$

If $b_0 = q - 1$ and $\gamma_0 \neq 0$, note that $T^{q-1}(0) = 0$. We sum over values of $x_1, \ldots, x_n$ with $\gamma_1 x_1 + \cdots + \gamma_n x_n \neq 0$.

$$\eta_{1,n}(f)(Y) = -\frac{1}{q} \prod_{i=1}^n \phi_i = \frac{1}{q}\Big((1 - T(\gamma_0)^{q-1})q - 1\Big) \prod_{i=1}^n \phi_i.$$

We have established (4.1) in this case. The rest of Case 1 follows by induction.

Case 2: *All the exponents are either $q-1$ or 0, but $(b_0, b_1, \ldots, b_n) \neq (0, 0, \ldots, 0)$.* We consider two subcases.

Case 2a: Suppose for some i that $b_i = 0$ and $\gamma_i \neq 0$. Say $b_0 = 0$ but $\gamma_0 \neq 0$. Then the values of $x_1, \ldots, x_n$ are unrestricted since we can solve for x_0 and

$$\eta_{1,n}(f)(Y) = \frac{1}{q-1} \prod_{i=1}^{n} \sum_{x_i \in \mathbb{F}_q} T^{b_i}(x_i).$$

Note that $\sum_{x_i \in \mathbb{F}_q} T^{q-1}(x_i) = q-1$ while $\sum_{x_i \in \mathbb{F}_q} T^0(x_i) = q$. We have

$$\eta_{1,n}(f)(Y) = (q-1)^{s-1} q^{n-s},$$

where $s = \{b_i | b_i = q-1, i = 1, \ldots, n\}$. That is, $\eta_{1,n}(f)(Y) = \frac{1}{q(q-1)} \prod_{i=0}^{n} \theta_i$, with θ_i defined by (4.3).

Case2b: Next suppose $\gamma_i = 0$ whenever $b_i = 0$. Now the sum $\eta_{1,n}(f)(Y)$ depends on how many γ_i's are nonzero. Let d be the number of γ_i's that are not zero (say, $\gamma_i \neq 0$, for $i = 0, 1, \ldots, d-1$), let s be the number of the exponents that are $q-1$, and $n+1-s$ be the number of the exponents that are 0 (say, the last $n+1-s$ exponents are all 0). We have $d \leq s$ and $\gamma_i = 0$ for all $i = s, s+1, \ldots, n$.

Define N_d be the number of solutions of

$$x_0 + \cdots + x_{d-1} = 0$$

with $(x_0, \ldots x_{d-1}) \in (\mathbb{F}_q^*)^d$. We get the recursion

$$N_d = (q-1)^{d-1} - N_{d-1}, \ N_0 = 1, \ N_1 = 0.$$

Therefore

$$N_d = \frac{(q-1)^d + (-1)^d (q-1)}{q}.$$

Now we compute $\eta_{1,n}(f)(Y)$. we have

$$\begin{aligned}
\eta_{1,n}(f)(Y) &= \frac{1}{q-1}q^{n+1-s}\sum_{\gamma_0 x_0+\cdots+\gamma_{d-1}x_{d-1}=0} T^{q-1}(x_0)\cdots T^{q-1}(x_{s-1}) \\
&= \frac{1}{q-1}q^{n+1-s}(q-1)^{s-d}\sum_{\gamma_0 x_0+\cdots+\gamma_{d-1}x_{d-1}=0} T^{q-1}(x_0)\cdots T^{q-1}(x_{d-1}) \\
&= \frac{1}{q-1}N_d(q-1)^{s-d}q^{n+1-s} \\
&= \frac{1}{q(q-1)}\prod_{i=0}^{n}\theta_i + \frac{1}{q}(-1)^d(q-1)^{s-d}q^{n+1-s}.
\end{aligned}$$

Note that here $\frac{1}{q}(-1)^d(q-1)^{s-d}q^{n+1-s} = \frac{1}{q}\prod_{i=0}^{n}\phi_i$, so that (4.1) is established in this subcase.

Case 3: *All the exponents are 0.*

Since there must be $\gamma_i \neq 0$ for some i we have $\phi_i = 0$ and (4.1) reduces to $\frac{q^n-1}{q-1}$. From (4.5), we see that in this case

$$\eta_{1,n}(f)(Y) = \frac{q^n-1}{q-1},$$

agreeing with (4.1). □

Corollary 4.1.2. *Theorem 3.5.1 holds in the hyperplane case (i.e., $r = n$).*

Proof: Let $\{e_1, e_2, \ldots, e_v\}$, where $v = |\mathcal{L}_1|$, be the standard basis of $R^{\mathcal{L}_1}$, and let $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ be the monomial basis of $R^{\mathcal{L}_1}$ constructed in Lemma 3.3.1. For $1 \leq \ell \leq v$, let $f_\ell = \sum_{i=1}^{v} q_{i\ell}e_i$, $q_{i\ell} \in R$, and let $Q = (q_{i\ell})$. Then

$$\eta_{1,r}(f_\ell) = \sum_{i=1}^{v} q_{i\ell}\eta_{1,r}(e_i).$$

Therefore the columns of AQ are the vectors $\eta_{1,r}(f_\ell)$, written with respect to the standard basis of $R^{\mathcal{L}_r}$.

Let $f_\ell = T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})$ be a basis monomial in $\mathcal{M}_R$ and let p^{α_ℓ} be the largest power of p dividing every coordinate of $\eta_{1,r}(f_\ell)$. We also specify that $f_1 = T(x_0^0x_1^0\cdots x_n^0)$ (i.e., the constant basis monomial in $\mathcal{M}_R$). We will show that $\alpha_1 = 0$ and for $1 < \ell \leq v$, $\alpha_\ell = \sum_{j=0}^{t-1}(n - s_j)$, where $(s_0, s_1, \ldots, s_{t-1})$ is the type of f_ℓ.

Let $\mathfrak{P}$ be the prime ideal of $R[\xi_p]$ lying over p. Stickelberger's theorem states that the number of times that $\mathfrak{P}$ divides $g(T^{-b})$ is $\sigma(b)$, where $0 < b < q-1$ and $\sigma(b)$ is the sum of the digits in the p-adic expansion of b. Since $(p) = \mathfrak{P}^{p-1}$ we have $\nu_{\mathfrak{P}}(q) = (p-1)t$.

In each case of (4.2), we have

$$\nu_{\mathfrak{P}}(\phi_i) = (p-1)t - \sigma(b_i)$$

except when $b_i = 0$ and $\gamma_i \neq 0$ (in which case, $\phi_i = 0$). Thus in Case 1 of the proof of Proposition 4.1.1 the p-adic valuation of any nonzero coordinate of $\eta_{1,n}(f_\ell)$ is

$$\frac{1}{p-1}\sum_{i=0}^{n}\nu_{\mathfrak{P}}(\phi_i) - t = nt - \frac{1}{p-1}\sum_{i=0}^{n}\sigma(b_i) = nt - \frac{1}{p-1}\sum_{j=0}^{t-1}\lambda_j = \sum_{j=0}^{t-1}(n - s_j)$$

recalling that λ_j is the j^{th} column sum of the p-adic digits of b_i (see (3.5)) and $\lambda_j = ps_{j+1} - s_j$. So in this case, the largest power of p dividing every coordinate of $\eta_{1,n}(f_\ell)$ is $\sum_{j=0}^{t-1}(n - s_j)$.

In Case 2a of the proof of Proposition 4.1.1, we have $\eta_{1,n}(f_\ell)(Y) = (q-1)^{s-1}q^{n-s}$, which has p-adic valuation $t(n-s)$. In Case 2b of the proof of Proposition 4.1.1, $\eta_{1,n}(f_\ell)(Y)$ is a sum of two terms, each with p-adic valuation $t(n-s)$. So the sum will have p-adic valuation at least $t(n-s)$. In summary, in Case 2 of the proof of Proposition 4.1.1, every coordinate of $\eta_{1,n}(f_\ell)$ has p-adic valuation at least $t(n-s)$, and since we can always find a hyperplane $\sum_{i=0}^{n}\gamma_i x_i = 0$ such that for some $0 \leq i \leq n$, $\gamma_i \neq 0$ while $b_i = 0$, we see that the largest power of p dividing every coordinate of $\eta_{1,n}(f_\ell)$ is $t(n-s)$.

In Case 3 of the proof of Proposition 4.1.1, the basis monomial under consideration is $f_1 = T(x_0^0\cdots x_n^0)$. Every coordinate of $\eta_{1,n}(f_1)$ is $\frac{q^n-1}{q-1}$, which is not

divisible by p; hence, 1 is the largest power of p dividing every coordinate of $\eta_{1,n}(f_1)$, and $\alpha_1 = 0$.

Now we factorize the matrix AQ as PD, where

$$D = \begin{pmatrix} p^{\alpha_1} & 0 & 0 & \cdots & 0 \\ 0 & p^{\alpha_2} & 0 & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & p^{\alpha_{v-1}} & 0 \\ 0 & & \cdots & 0 & p^{\alpha_v} \end{pmatrix},$$

and P is an $|\mathcal{L}_n| \times |\mathcal{L}_n| = v \times v$ matrix with the v columns being $\frac{1}{p^{\alpha_\ell}}\eta_{1,r}(f_\ell)$, $\ell = 1, 2, \ldots, v$. It remains to show that P is invertible as a matrix with entries from R. We use the well-known formula for the determinant of a symmetric design. (See Theorem 2.2.4 (a).) Thus if A is the incidence matrix for a symmetric 2-design with block size k and order $n = r - \lambda = k - \lambda$, then

$$\det(A) = kn^{(v-1)/2}.$$

In our case $k = (q^n - 1)/(q - 1)$ and $n = q^{n-1}$, so

$$\det(A) = \frac{q^n - 1}{q - 1} \cdot q^{(n-1)(v-1)/2}.$$

Hence

$$\nu_p(\det(A)) = t(n-1)(v-1)/2.$$

From our discussion above, we have

$$\sum_\ell \alpha_\ell = \sum_{(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H}} d_{(s_0, s_1, \ldots, s_{t-1})} \left(\sum_{j=0}^{t-1} (n - s_j) \right).$$

Now using the fact that for every $(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H}$, we have

$$d_{(s_0, s_1, \ldots, s_{t-1})} = d_{(n+1-s_0, n+1-s_1, \ldots, n+1-s_{t-1})},$$

and $\sum_{(s_0,s_1,\ldots,s_{t-1})\in\mathcal{H}} d_{(s_0,s_1,\ldots,s_{t-1})} = v-1$, we find that

$$\sum_{\ell} \alpha_\ell = t(n-1)(v-1)/2 = \nu_p(\det(A)).$$

Since $\det(A) = p^{\sum_\ell \alpha_\ell}\det(P)\det(Q^{-1})$, and $\sum_\ell \alpha_\ell = \nu_p(\det(A))$, we see that $\det(P)$ is a unit in R; hence, P is invertible. This completes the proof. □

Note that we could also argue that P is invertible by writing the columns of P as polynomials in the dual coordinates γ_i. Changing to the dual-coordinate monomial basis, we get column vectors which can clearly be seen to be independent (mod $\mathfrak{p}$), using the formulas derived in this chapter.

Chapter 5

THE PROOF OF THEOREM A

In this chapter we prove Theorem A by showing that the lower bounds for the invariants which we can get from Wan's theorem are also the upper bounds. In the last section we also provide a proof of the result of Bardoe and Sin, Theorem 3.4.2.

5.1 Lower bounds on the invariants

To get lower bounds on the p-powers dividing the invariants of $\eta_{1,r}$ we apply Wan's theorem. Let $f = T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n}) \in \mathcal{M}_R$ be a basis monomial. Using Theorem 2.5.8, we get the lower bound on the p-adic valuation of the coordinates of $\eta_{1,r}(f)$. Note that the coordinates of $\eta_{1,r}(f)$ are indexed by the r-spaces in $\mathcal{L}_r$. An r-subspace Y of $V = \mathbb{F}_q^{n+1}$ can be defined by a system of $(n+1-r)$ independent linear homogeneous equations. Putting the $n+1-r$ equations in reduced row echelon form, we have r independent coordinates which run through $\mathbb{F}_q$. The remaining $n+1-r$ coordinates are linear functions of those r coordinates. Without loss of generality, we label the free coordinates $(x_0,\ldots,x_{r-1}) = \mathbf{x}$ and express the defining equations of Y as $x_i = F_i(\mathbf{x})$ for $(r \le i \le n)$. The Y-coordinate of $\eta_{1,r}(f)$ is:

$$\eta_{1,r}(f)(Y) = \frac{1}{q-1}\sum_{\mathbf{x}\in{\mathbb{F}_q}^r\setminus\{(0,0,\ldots,0)\}} T^{b_0}(x_0)\cdots T^{b_{r-1}}(x_{r-1})T^{b_r}(F_r(\mathbf{x}))\cdots T^{b_n}(F_n(\mathbf{x})). \tag{5.1}$$

Lemma 5.1.1. *Let $f(x_0, \ldots, x_n) = T({x_0}^{b_0} \cdots {x_n}^{b_n})$ be a nonconstant basis monomial in $\mathcal{M}_R$. Then every coordinate of the image vector $\eta_{1,r}(f)$ is divisible by p^α with*

$$\alpha = \sum_{i=0}^{t-1} \max\{0, r - s_i\}, \tag{5.2}$$

where $(s_0, s_1, \ldots, s_{t-1})$ is the type of f as defined in (3.6).

Proof: Let Y be an arbitrary r-space in $\mathcal{L}_r$. By the above discussion, we assume that Y is defined by $x_i = F_i(\mathbf{x})$, $i = r, r+1, \ldots, n$ and $\mathbf{x} = (x_0, x_1, \ldots, x_{r-1}) \in \mathbb{F}_q^r$. The Y-coordinate of $\eta_{1,r}(f)$ is then given by (5.1), and by Theorem 2.5.8, we have

$$\nu_p(\eta_{1,n}(f)(Y)) \geq \sum_{\ell=0}^{t-1} \max\{0, r - \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i)\}.$$

Recalling that the type of f is denoted by $(s_0, s_1, \ldots, s_{t-1})$ and noting that $s_{t-\ell} = \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i)$ (reading s_t as s_0) for all $\ell = 0, 1, \ldots, t-1$, we have

$$\nu_p(\eta_{1,n}(f)(Y)) \geq \sum_{i=0}^{t-1} \max\{0, r - s_i\}.$$

This completes the proof. □

Let Q be the basis change matrix between the standard basis and the monomial basis $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ of $R^{\mathcal{L}_1}$ (as used in Section 3.5). Using Lemma 5.1.1, we see that one can factorize AQ as PD, where

$$D = \begin{pmatrix} p^{\alpha_1} & 0 & 0 & \cdots & 0 \\ 0 & p^{\alpha_2} & 0 & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & p^{\alpha_{v-1}} & 0 \\ 0 & & \cdots & 0 & p^{\alpha_v} \\ 0 & & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix},$$

p^{α_i} corresponds to the basis monomial $f_i \in \mathcal{M}_R$ with type $(s_0, s_1, \ldots, s_{t-1})$, and

$$\alpha_i = \sum_{j=0}^{t-1} \max\{0, r - s_j\}.$$

The matrix P is an $|\mathcal{L}_r| \times |\mathcal{L}_r|$ matrix whose first v columns are $\frac{1}{p^{\alpha_i}}\eta_{1,r}(f_i)$, $i = 1, 2, \ldots, v$. We still need to show that D (with the diagonal entries suitably arranged) is indeed the Smith normal form of A.

5.2 p-filtrations and Smith normal form bases

Let $R = \mathbb{Z}_p[\xi_{q-1}]$ with maximal ideal $\mathfrak{p} = pR$ and residue field $\mathbb{F}_q$, and let $\eta_{1,r} : R^{\mathcal{L}_1} \to R^{\mathcal{L}_r}$ be the map defined before. In this section we prove that there exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$, whose reduction modulo $\mathfrak{p}$ is the monomial basis of $\mathbb{F}_q^{\mathcal{L}_1}$, such that the matrix of $\eta_{1,r}$ with respect to $\mathcal{B}$ and some basis of $R^{\mathcal{L}_r}$ is the Smith normal form of $\eta_{1,r}$. We begin with some general results on injective homomorphisms of free R-modules.

For any free R-module M we set $\overline{M} = M/\mathfrak{p}M$ and for any R-submodule L of M, let $\overline{L} = (L + \mathfrak{p}M)/\mathfrak{p}M$ be the image in $\overline{M}$.

Let $\phi : M \to N$ be an injective homomorphism of free R-modules of finite rank, with $\operatorname{rank} M = m \geq 1$.

Let

$$N' = \{x \in N \mid \exists j \geq 0, p^j x \in \operatorname{Im} \phi\}$$

Then N' is the smallest R-module direct summand of N containing $\operatorname{Im} \phi$, (sometimes called its *purification*) and is also of rank m. The invariant factors of ϕ stay the same if we change the codomain to N', which will often allow us to reduce to the case $\operatorname{rank} N = m$.

Define

$$M_i = \{m \in M \ \mid \ \phi(m) \in p^i N\}, \quad i = 0, 1, ...$$

Then we have a filtration

$$M = M_0 \supseteq M_1 \supseteq \cdots$$

of M and the filtration

$$\overline{M} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots$$

of $\overline{M}$.

Since ϕ is injective, and $N'/\operatorname{Im}\phi$ has finite exponent, it follows that there exists a smallest index ℓ such that $\overline{M}_\ell = 0$. So we have a finite filtration

$$\overline{M} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots \supseteq \overline{M}_\ell = \{0\}.$$

The inclusions need not be strict, although the last one is, by minimality of ℓ.

Proposition 5.2.1. *For $0 \leq i \leq \ell - 1$, p^i is an invariant factor of ϕ with multiplicity* $\dim(\overline{M}_i/\overline{M}_{i+1})$.

Proof: The theory of modules over PIDs says there are bases of M and N' such that ϕ is represented by an $m \times m$ diagonal matrix whose entries are the invariant factors of ϕ. From this matrix we see that the multiplicity of p^i is $\dim(\overline{M}_i/\overline{M}_{i+1})$. □

Suppose we start with a basis $\overline{\mathcal{B}}_{\ell-1}$ of $\overline{M}_{\ell-1}$ and extend it to a basis of $\overline{M}_{\ell-2}$ by adding a set $\overline{\mathcal{B}}_{\ell-2}$ of vectors and so on until we have a basis

$$\overline{\mathcal{B}} = \overline{\mathcal{B}}_0 \cup \overline{\mathcal{B}}_1 \cup \ldots \cup \overline{\mathcal{B}}_{\ell-1}$$

of $\overline{M}$. At each stage we also select a set $\mathcal{B}_i \subset M_i$ of preimages of $\overline{\mathcal{B}}_i$ and expand the sets in the same way. The resulting set $\mathcal{B} = \cup_{i=0}^{\ell-1}\mathcal{B}_i$ is a basis of M, by Nakayama's lemma.

We show that this basis can be used to compute the Smith normal form of ϕ, that is, that there is a basis $\mathcal{C}$ of N such that the matrix of ϕ with respect to $\mathcal{B}$ and $\mathcal{C}$ is the Smith normal form.

For e in $\mathcal{B}_i$, we have $p^i \parallel \phi(e)$; so $y = \frac{1}{p^i}\phi(e)$ is an element of N'. The elements y thus obtained from all elements of $\mathcal{B}$ are linearly independent elements of N', since ϕ is injective. Moreover, the index of $\operatorname{Im}\phi$ in the R-submodule of N' generated by these elements y is equal to the index of $\operatorname{Im}\phi$ in N' by the proposition. Therefore, these elements y form a basis of N'. The matrix of ϕ with respect to $\mathcal{B}$

and any basis of N obtained by extending this basis will then be in Smith normal form.

For convenience, we introduce a special name for bases such as $\mathcal{B}$ above.

Definition 5.2.2. *We will call a basis $\mathcal{B}$ of M an* SNF basis of M for ϕ *if $\mathcal{B} = \cup_{i=0}^{\ell-1}\mathcal{B}_i$, where for each i we have $\mathcal{B}_i \subseteq M_i$ and $\mathcal{B}_i$ maps bijectively to a basis of $\overline{M}_i/\overline{M}_{i+1}$ under the composite map $M_i \to \overline{M}_i \to \overline{M}_i/\overline{M}_{i+1}$.*

We now apply the above general theory to our situation. We will look at the case where $M = R^{\mathcal{L}_1}$, $N = R^{\mathcal{L}_r}$, and $\phi = \eta_{1,r}$. Let $G = \mathrm{GL}(n+1, q)$. Then G acts on $\mathcal{L}_1$ and $\mathcal{L}_r$, and the map $\eta_{1,r}$ is an injective homomorphism of RG-modules; so the M_i are RG-modules and the $\overline{M}_i$ are $\mathbb{F}_qG$-modules.

We will use the following special properties of the $\mathbb{F}_qG$-module $\mathbb{F}_q^{\mathcal{L}_1}$.

Proposition 5.2.3. *1. Two basis monomials of the same type generate the same $\mathbb{F}_qG$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$.*

2. Every $\mathbb{F}_qG$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ has a basis consisting of all of the basis monomials in the submodule.

Proof: Part (1) is immediate from Corollary 3.4.3. (See [7, Theorem B]. The field in [7] is taken to be an algebraically closed field k, not $\mathbb{F}_q$, but it follows from [7, Theorem A] that in fact all the kG-submodules of $k^{\mathcal{L}_1}$ are simply scalar extensions of $\mathbb{F}_qG$-submodules of $\mathbb{F}_q^{\mathcal{L}_1}$, so for example [7, Theorems A, B] hold also over $\mathbb{F}_q$.) Let S be an $\mathbb{F}_qG$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ and let $f \in S$. By Corollary 3.4.3, S must contain all the basis monomials needed to express f. Therefore, S is the linear span over $\mathbb{F}_q$ of all the basis monomials it contains. □

Corollary 5.2.4. *$R^{\mathcal{L}_1}$ has an SNF basis for $\eta_{1,r}$ whose image in $\mathbb{F}_q^{\mathcal{L}_1}$ is the monomial basis.*

Proof: By Proposition 5.2.3(2) we can choose $\overline{\mathcal{B}}_i$ in the construction above to be the set of monomials in $\overline{M}_i$ which are not in $\overline{M}_{i+1}$. □

Whenever we have a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ whose reduction modulo $\mathfrak{p}$ is the monomial basis, the type of an element of $\mathcal{B}$ will always mean the type of its image in the monomial basis.

Corollary 5.2.5. *Let $\mathcal{B}$ be an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$ whose image in $\mathbb{F}_q^{\mathcal{L}_1}$ is the monomial basis. Then the invariants corresponding to two elements of $\mathcal{B}$ of the same type are equal.*

Proof: Let e, $f \in \mathcal{B}$ be two such basis elements, with images $\overline{e}$ and $\overline{f}$. Then

$$\begin{aligned} e \in M_j &\iff \overline{e} \in \overline{M}_j \quad \text{(def. of SNF basis)} \\ &\iff \overline{f} \in \overline{M}_j \quad \text{(Proposition 5.2.3(1))} \\ &\iff f \in M_j \quad \text{(def. of SNF basis).} \end{aligned}$$

□

5.3 Jacobi sums and the action of the general linear group on $R^{\mathcal{L}_1}$

In this section we will prove a refinement of Corollary 5.2.4 (see Lemma 5.3.6 for details). In order to prove this refinement, we need to use Jacobi sums and the action of the general linear group on $R^{\mathcal{L}_1}$.

Again let T be the Teichmüller character of $\mathbb{F}_q$ defined in Section 2.5.4, where $q = p^t$. We know that T is a p-adic multiplicative character of $\mathbb{F}_q$ of order $(q-1)$ and all multiplicative characters of $\mathbb{F}_q$ are powers of T. Again we adopt the convention that T^0 is the character that maps all elements of $\mathbb{F}_q$ to 1, while T^{q-1} maps 0 to 0 and all other elements to 1. Recall that given two multiplicative characters on $\mathbb{F}_q^*$, T^{b_0} and T^{b_1}, the Jacobi sum is

$$J(T^{b_0}, T^{b_1}) = \sum_{x_0 \in \mathbb{F}_q} T^{b_0}(x_0) T^{b_1}(1 - x_0). \tag{5.3}$$

From the above definition and our convention on T^0 and T^{q-1}, we see that if $b_0 \not\equiv 0 \pmod{q-1}$, then

$$J(T^{b_0}, T^0) = 0, \text{ and } J(T^{b_0}, T^{q-1}) = -1.$$

Also we have $J(T^{-1}, T) = 1$. The Jacobi sum $J(T^{b_0}, T^{b_1})$ lies in $R = \mathbb{Z}_p[\xi_{q-1}]$. Naturally we want to know its p-adic valuation. Using Stickelberger's theorem on Gauss sums (Section 2.5.4 and see [15, 39] for further reference) and the relation between Gauss and Jacobi sums (Section 2.5.3),

$$J(\chi_1, \chi_2) = \frac{g(\chi_1) g(\chi_2)}{g(\chi_1 \chi_2)},$$

we have the following relation.

Theorem 5.3.1. *Let b_0 and b_1 be integers such that $b_i \not\equiv 0 \pmod{q-1}$, $i = 0, 1$, and $b_0 + b_1 \not\equiv 0 \pmod{q-1}$. For any integer b, we use $\sigma(b)$ to denote the sum of digits in the expansion of the least nonnegative residue of b modulo $q-1$ as a base p number. Then*

$$\nu_p(J(T^{-b_0}, T^{-b_1})) = \frac{\sigma(b_0) + \sigma(b_1) - \sigma(b_0 + b_1)}{p-1}.$$

In other words, the number of times that p divides $J(T^{-b_0}, T^{-b_1})$ is equal to the number of carries in the addition $b_0 + b_1 \pmod{q-1}$.

We will now construct an element of RG with certain special properties. For this purpose, we will first describe the action of G on $R^{\mathcal{L}_1}$. In this section, we think of elements of $\mathcal{L}_1$ in homogeneous coordinates as row vectors and elements of G as matrices acting by right multiplication. Then $R^{\mathcal{L}_1}$ is the left RG-module given in the following way. For each function $f \in R^{\mathcal{L}_1}$, the function gf is given by

$$(gf)(Z) = f(Zg), \qquad Z \in \mathcal{L}_1.$$

Let $f_i = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R$ be an arbitrary basis monomial. Let $\xi = \xi_{q-1}$ be a primitive $(q-1)^{\text{th}}$ root of unity in the Teichmüller set $T_q \subset R$, and let $\bar{\xi}$ be its reduction modulo p. We define $g_\ell \in G$ to be the element which replaces x_0 by $x_0 + \bar{\xi}^\ell x_1$ and leaves all other x_i unchanged. Then

$$g_\ell f_i = T\big((x_0 + \bar{\xi}^\ell x_1)^{b_0} x_1^{b_1} \cdots x_n^{b_n}\big).$$

Let $g = \sum_{\ell=0}^{q-2} \xi^{-\ell} g_\ell \in RG$. The following lemma gives us gf_i.

Lemma 5.3.2. *Let f_i and g be as given. Then*

$$gf_i = \begin{cases} 0, & \text{if } b_0 = 0 \\ T(x_0^{q-2} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = q-1 \\ \big(q(1 - T(x_0^{q-1})) - 1\big) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = 1 \\ -J(T^{-1}, T^{b_0}) T(x_0^{b_0-1} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}), & \text{otherwise.} \end{cases}$$

Proof: First note that

$$\begin{aligned} J(T^{-1}, T^0) &= 0, \\ J(T^{-1}, T^{q-1}) &= -1, \end{aligned}$$

so the cases $b_0 = 0$ and $b_0 = q-1$ are really covered by the general case. Therefore we will only consider two cases.

Case 1. $b_0 \neq 1$. First assume that x_0 and x_1 are both nonzero. We have

$$\begin{aligned} gf_i &= \sum_{\ell=0}^{q-2} \xi^{-\ell} g_\ell f_i \\ &= T(x_1^{b_1} \cdots x_n^{b_n}) \sum_{\ell=0}^{q-2} T^{-1}(\bar{\xi}^\ell) T^{b_0}(x_0 + \bar{\xi}^\ell x_1) \qquad (5.4) \\ &= T(x_1^{b_1} \cdots x_n^{b_n}) \sum_{u \in \mathbb{F}_q} T^{-1}(-\frac{x_1 u}{x_0}) T^{b_0}\left(1 - (-\frac{x_1 u}{x_0})\right) T(-1) T(x_0^{b_0 - 1} x_1) \\ &= -J(T^{-1}, T^{b_0}) T(x_0^{b_0-1} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}). \qquad (5.5) \end{aligned}$$

If $x_1 = 0$ we verify directly that (5.4) and (5.5) are both zero, so the formula is still valid. If $x_0 = 0$, since $b_0 \neq 1$, we see that (5.5) is 0; and (5.4) is also 0, since a nontrivial (multiplicative) character summed over $\mathbb{F}_q$ is zero. Therefore the formula still holds.

Case 2. $b_0 = 1$. In this case

$$gf_i = T(x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}) \sum_{\ell=0}^{q-2} T(\bar{\xi}^{-\ell} x_0 + x_1).$$

If $x_0 = 0$, then $gf_i = (q-1) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n})$. If $x_0 \neq 0$ but $x_1 = 0$, then clearly we have $gf_i = 0$. If $x_0 \neq 0$ and $x_1 \neq 0$, then using the same calculations as in the case $b_0 \neq 1$, we have

$$gf_i = -J(T^{-1}, T) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}) = -T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}).$$

In summary, the formula for gf_i in this case is

$$\big(q(1 - T(x_0^{q-1})) - 1\big) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}).$$

This completes the proof. □

Corollary 5.3.3. *Let $f_i = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R$ be a basis monomial, and let $g(j) = \sum_{\ell=0}^{q-2} \xi^{-\ell} g_{\ell p^{-j}}$ be the j^{th} Frobenius analog of g in Lemma 5.3.2 above. Then*

$$g(j)f_i = \begin{cases} 0, & \text{if } b_0 = 0 \\ T(x_0^{q-1-p^j} x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = q-1 \\ \big(q(1-T(x_0^{q-1})) - 1\big) T(x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = p^j \\ -J(T^{-p^j}, T^{b_0}) T(x_0^{b_0-p^j} x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b_n}), & \text{otherwise.} \end{cases}$$

Proof: Let ρ denote the Frobenius automorphism of R, which maps an element of the Teichmüller set T_q to its p^{th} power, and let $\mathbf{y} = (y_0, \ldots, y_n) = (x_0^{p^j}, \ldots, x_n^{p^j})$. We can write $f_i(\mathbf{x}) = f_i^{\rho^{-j}}(\mathbf{y}) = T(y_0^{b_0 p^{-j}} \cdots y_n^{b_n p^{-j}})$. We observe that $g_{\ell p^{-j}}$ replaces y_0 by $y_0 + \bar{\xi}^{\ell} y_1$. Therefore we can apply the previous lemma to get

$$g(j) f_i^{\rho^{-j}}(\mathbf{y}) = \begin{cases} 0, & \text{if } b_0 = 0 \\ T(y_0^{q-2} y_1^{b_1 p^{-j}+1} y_2^{b_2 p^{-j}} \cdots y_n^{b_n p^{-j}}), & \text{if } b_0 = q-1 \\ \big(q(1-T(y_0^{q-1})) - 1\big) T(y_1^{b_1 p^{-j}+1} y_2^{b_2 p^{-j}} \cdots y_n^{b_n p^{-j}}), & \text{if } b_0 = p^j \\ -J(T^{-1}, T^{b_0 p^{-j}}) T(y_0^{b_0 p^{-j}-1} y_1^{b_1 p^{-j}+1} y_2^{b_2 p^{-j}} \cdots y_n^{b_n p^{-j}}) & \text{otherwise.} \end{cases}$$

Substituting $\mathbf{x}$ back in and noting that $J(\chi^p, \psi^p) = J(\chi, \psi)$ we get the result. □

For each basis monomial in $\mathcal{M}_R$ with at least one exponent strictly between 0 and $q-1$, we want to construct an element of RG which acts as the identity on that basis monomial and annihilates all other members of $\mathcal{M}_R$. To begin we define a finite abelian group

$$(\widetilde{\mathcal{M}}, *) = \{X_0^{b_0 \pmod{q-1}} \cdots X_n^{b_n \pmod{q-1}} \mid \sum_{i=0}^{n} b_i \text{ is divisible by } q-1\},$$

where the operation $*$ is the (natural) componentwise multiplication. The group $(\widetilde{\mathcal{M}}, *)$ has order $(q-1)^n$. Next we define a map from $\mathcal{M}_R$ to $(\widetilde{\mathcal{M}}, *)$.

$$\begin{array}{rccc} \tau: & \mathcal{M}_R & \longrightarrow & \widetilde{\mathcal{M}} \\ & T(x_0^{b_0} \cdots x_n^{b_n}) & \longmapsto & X_0^{b_0 \pmod{q-1}} \cdots X_n^{b_n \pmod{q-1}} \end{array}$$

If $\widetilde{m} \in \widetilde{\mathcal{M}}$ has $i \leq n$ of its exponents divisible by $q-1$, then $\widetilde{m}$ has 2^i preimages in $\mathcal{M}_R$. If all exponents are divisible by $(q-1)$ then there are (2^n-1) preimages since we have excluded $T(x_0^{q-1} \cdots x_n^{q-1})$ from $\mathcal{M}_R$.

The following formulas are well known (see [8, p. 314]).

Lemma 5.3.4. (Inversion formulas) *Let H be a finite abelian group of exponent e, R a ring containing $\frac{1}{|H|}$ and a primitive e^{th} root of unity, and H' the group of characters from H to R. Let $A = \sum_{h \in H} a_h h \in RH$ and $B = \sum_{\chi \in H'} b_\chi \chi \in RH'$. Then*

$$a_h = \frac{1}{|H|} \sum_{\chi \in H'} \chi(A)\chi^{-1}(h) \tag{5.6}$$

$$b_\chi = \frac{1}{|H|} \sum_{h \in H} B(h)\chi^{-1}(h) \tag{5.7}$$

In what follows we will apply Lemma 5.3.4 to the group $(\widetilde{\mathcal{M}}, *)$. We construct an element of RG that kills each basis monomial except those which are preimages of $\tau(f_i) \in \widetilde{\mathcal{M}}$. Then we construct elements of RG that kill each element of the preimage set except the one we choose.

Let $S = \{\lambda I \mid \lambda \in \mathbb{F}_q^*\}$ be the subgroup of scalar matrices in G. The diagonal matrices of G form a maximal abelian subgroup or torus, and their images in $\mathrm{PGL}(n+1,q) = G/S$ form a torus in that group. Let $\mathcal{T} \subset G$ be a complete set of coset representatives in G of this torus of $\mathrm{PGL}(n+1,q) = G/S$. There is a 1-to-1 correspondence between elements of $\mathcal{T}$ and characters of the group $(\widetilde{\mathcal{M}}, *)$. For $\widetilde{m} = \tau(m) \in \widetilde{\mathcal{M}},\ g \in \mathcal{T}$ we define χ_g via $gm = \chi_g(\widetilde{m})m$. Hence if

$$g = \begin{pmatrix} d_0 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \in \mathcal{T}$$

then

$$\chi_g(X_0^{b_0 \pmod{q-1}} \cdots X_n^{b_n \pmod{q-1}}) = T({d_0}^{b_0} \cdots {d_n}^{b_n}) \in R.$$

We want to find B such that

$$\begin{aligned} B(\tau(f_i)) &= \sum_{g\in\mathcal{T}} b_g\chi_g(\tau(f_i)) = 1 \\ B(\tau(f_j)) &= 0, \text{ if } \tau(f_i) \neq \tau(f_j). \end{aligned}$$

Using (5.7) in Lemma 5.3.4 to solve for b_g we get

$$B = \frac{1}{|\mathcal{T}|}\sum_{g\in\mathcal{T}} \chi_g^{-1}(\tau(f_i))\chi_g$$

and the corresponding element of RG is

$$\frac{1}{(q-1)^n}\sum_{g\in\mathcal{T}} \chi_g^{-1}(\tau(f_i))g.$$

This element is in RG because p does not divide the order of $\widetilde{\mathcal{M}}$, and it annihilates all basis monomials in $\mathcal{M}_R$ except those in the preimage of $\tau(f_i)$.

In the language of representation theory, we would say that two monomials afford the same character if and only if their exponents are all congruent (mod $q-1$).

Lemma 5.3.5. *Let $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ be the monomial basis of $R^{\mathcal{L}_1}$. For each $f_i = T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n}) \in \mathcal{M}_R$ with some b_j strictly between 0 and $q-1$, there is an element $h_i \in RG$ with the following property. If*

$$f = c_1f_1 + c_2f_2 + \cdots + c_vf_v$$

is any element in $R^{\mathcal{L}_1}$ then

$$h_if = c_if_i.$$

Proof: We will construct the required h_i in two steps. Let H denote the subgroup of diagonal matrices of G. Then each basis monomial in $\mathcal{M}_R$ spans a rank one RH-submodule of $R^{\mathcal{L}_1}$, which is the direct sum of all such submodules. Two basis monomials $f_i = T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})$ and $f_j = T(x_0^{b'_0}x_1^{b'_1}\cdots x_n^{b'_n})$ afford the same character of H if and only if $b_i \equiv b'_i \pmod{q-1}$ for $0 \leq i \leq n$.

Since the order of H is not divisible by p, for each character χ of H, the group ring RH contains an idempotent element projecting onto the χ-isotypic component of $R^{\mathcal{L}_1}$, the span of all the basis monomials affording χ. In other words, we can start with the group ring element constructed above from the inversion formula.

If none of the exponents the of f_i is divisible by $q-1$, then no other basis monomials afford the same character as f_i and we can take h_i to be the above idempotent. Now suppose that some exponents of f_i are divisible by $q-1$. We proceed successively for each exponent of f_i which is either 0 or $q-1$. Without loss of generality, assume that f_i has $b_0 = q-1$. We construct an element $h \in RG$ which annihilates every basis monomial in $\mathcal{M}_R$ for which $b_0 = 0$ and acts as the identity on f_i. (If f_i instead has $b_0 = 0$, then the element we want is $1-h$.)

Without loss of generality, we will take $b_1 = a_{1,t-1}p^{t-1} + \cdots + a_{1,0}$ to be an exponent lying strictly between 0 and $q-1$ with $a_{1,j} < p-1$ for some j. Then we take the element $h_1 = g(j) \in RG$ from Lemma 5.3.3 that shifts p^j from b_0 to b_1. We get

$$h_1 f_i = T(x_0^{q-1-p^j} x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b^n}).$$

If e is any other basis monomial of the form $e = T(x_0^{q-1} x_1^{b_1} \cdots)$, then we similarly have

$$h_1 e = T(x_0^{q-1-p^j} x_1^{b_1+p^j} \cdots);$$

and if x_0 has exponent 0 in e then from Corollary 5.3.3, we have

$$h_1 e = 0.$$

Next we set $h_2 = g'(j) \in RG$ to be the analog of $g(j)$ but with the roles of x_0 and x_1 interchanged. Noting that here $b_1 + p^j \neq p^j$ (we assumed that $0 < b_1 < q-1$),

we get

$$\begin{aligned} h_2h_1f_i &= -J(T^{-p^j}, T^{b_1+p^j})f_i \\ h_2h_1e &= -J(T^{-p^j}, T^{b_1+p^j})e, \quad \text{if the exponent of } x_0 \text{ in } e \text{ is } q-1 \\ h_2h_1e &= 0 \quad \text{otherwise.} \end{aligned}$$

Since there is no carry in the sum $p^j + b_1$, the Jacobi sum $J(T^{-p^j}, T^{b_1+p^j})$ is a unit in R (cf. Lemma 5.3.1). Hence the element h of RG we want is $-\frac{1}{J(T^{-p^j}, T^{b_1+p^j})}h_2h_1$.

We can repeat the above process for each exponent of f_i which is divisible by $q-1$. The product of all the elements we have constructed is the element $h_i \in RG$ which kills every basis monomial in $\mathcal{M}_R$ except f_i. □

We now prove the main result in this section.

Lemma 5.3.6. *Assume $q > 2$. There exists an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$, whose reduction modulo $\mathfrak{p}$ is $\mathcal{M}$, and which contains all the basis monomials of $\mathcal{M}_R$ having at least one exponent lying strictly between 0 and $q-1$.*

Proof: By Corollary 5.2.4, there exists an SNF basis $\mathcal{B} = \cup_{j=0}^{\ell-1}\mathcal{B}_j$ of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$ such that the reduction of $\mathcal{B}$ modulo $\mathfrak{p}$ is $\mathcal{M}$. Let $f \in \mathcal{B}$, and let the reduction of f modulo $\mathfrak{p}$ be

$$\overline{f} = x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n} \in \mathcal{M},$$

with some b_j satisfying $0 < b_j < q-1$. Let $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ with $f_1 = T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})$, where $v = |\mathcal{L}_1|$. We write

$$f = c_1f_1 + c_2f_2 + \cdots + c_vf_v, \ c_i \in R.$$

Since $\overline{f} = \overline{f_1}$, we see that $\overline{c_1} = 1$. Hence c_1 is a unit in R. Since there is an exponent b_j lying strictly between 0 and $q-1$, by Lemma 5.3.5, we can find $h_1 \in RG$ such that $h_1f = c_1f_1$. In the notation of Definition 5.2.2 with $M = R^{\mathcal{L}_1}$, we see that if $f \in \mathcal{B}_j$, then $f_1 \in M_j$ since M_j is an RG-submodule , so that $\mathcal{B}' = (\mathcal{B} \setminus \{f\}) \cup \{f_1\}$

is again an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$. We can repeat this process for every element in $\mathcal{B}$ whose reduction modulo $\mathfrak{p}$ has one exponent strictly lying between 0 and $q-1$. At the end, we obtain the required SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$. □

We will use $\mathcal{M}'_R$ to denote the special SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$ produced by Lemma 5.3.6. Again the *type* of $f \in \mathcal{M}'_R$ is defined to be that of $\overline{f} \in \mathcal{M}$.

Lemma 5.3.7. *The invariants of $\eta_{1,r}$ corresponding to two elements of $\mathcal{M}'_R$ of types $(s_0, \ldots, s_{t-1})$ and $(s_1, s_2, \ldots, s_{t-1}, s_0)$, respectively, are equal.*

Proof: We may assume $t \geq 2$ since there is nothing to prove otherwise. For any type $\xi \in \mathcal{H}$, we can always find a basis monomial $f \in \mathcal{M}_R$ of type ξ and with at least one exponent lying strictly between 0 and $q-1$. Hence $f \in \mathcal{M}'_R$. By Corollary 5.2.5, the invariants of $\eta_{1,r}$ corresponding to two elements in $\mathcal{M}'_R$ of the same type are equal. Therefore we may assume that the two elements of $\mathcal{M}'_R$ in the statement of the lemma are actually in $\mathcal{M}_R$.

The Frobenius field automorphism

$$\begin{aligned} \rho : \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ x_i &\mapsto x_i^p \end{aligned}$$

applied to the coordinates of V is an automorphism of the projective geometry. It maps points to points, subspaces to subspaces, and preserves incidence . The image of a point $Z = (x_0, \ldots, x_n)$ is $Z^\rho = (x_0^p, \ldots, x_n^p)$ and for an r-subspace Y, Y^ρ is the r-subspace containing the images of all the points incident with Y. Given a monomial function $f_i = T(x_0^{b_0} \cdots x_n^{b_n})$ we have

$$f_i^\rho = T(x_0^{pb_0} \cdots x_n^{pb_n}).$$

Clearly if f_i is of type $(s_0, \ldots, s_{t-1})$ then f_i^ρ is of type $(s_{t-1}, s_0, \ldots, s_{t-2})$ because λ_j becomes λ_{j+1} in (3.5). It is also clear that

$$f_i(Z^\rho) = f_i^\rho(Z)$$

so that

$$\eta_{1,r}(f_i)(Y^\rho) = \eta_{1,r}(f_i^\rho)(Y).$$

As Y runs through $R^{\mathcal{L}_r}$ so does Y^ρ. Thus, the coordinates of $\eta_{1,r}(f_i)$ are the same as the coordinates of $\eta_{1,r}({f_i}^\rho)$ but permuted by ρ, so that the invariants corresponding to f_i and f_i^ρ are equal. □

5.4 The proof of Theorem A

Our aim in this section to prove Theorem 3.5.1 (Theorem A). We will achieve this by proving the more detailed result Theorem 5.4.2 below. Our proof depends on Lemma 5.1.1, which gives lower bounds on the p-adic valuations of the coordinates of $\eta_{1,r}(f)$, where $f \in \mathcal{M}_R$, and the results in Section 5.2 and Section 5.3.

We first prove a lemma.

Lemma 5.4.1. *Let f be a nonconstant basis monomial in $\mathcal{M}_R$. Then p does not divide $\eta_{1,r}(f)$ if and only if f has type $(s_0, s_1, \ldots, s_{t-1})$, with $s_j \geq r$ for all $0 \leq j \leq t-1$.*

Proof: Let $\overline{f}$ be the image modulo $\mathfrak{p}$ of f. Then p does not divide $\eta_{1,r}(f)$ if and only if the image of $\overline{f}$ under the induced map $\overline{\eta}_{1,r} : \mathbb{F}_q^{\mathcal{L}_1} \to \mathbb{F}_q^{\mathcal{L}_r}$ is nonzero. Suppose that $s_j < r$ for some j. By Lemma 5.1.1, $p \,|\, \eta_{1,r}(f)$. That is, only those basis monomials $\overline{f}$ of type $(s_0, s_1, \ldots, s_{t-1})$, where $s_j \geq r$ for all $0 \leq j \leq t-1$, could possibly have nonzero image under $\overline{\eta}_{1,r}$. On the other hand, by Hamada's formula, rank of $\overline{\eta}_{1,r}$ is equal to one plus the number of $\overline{f}$'s with this property. Therefore, the images of all such basis monomials must be linearly independent, in particular, nonzero. Hence $p \nmid \eta_{1,r}(f)$, if and only if f has type $(s_0, s_1, \ldots, s_{t-1})$, where $s_j \geq r$ for all $0 \leq j \leq t-1$. This completes the proof. □

Theorem 5.4.2. *Let $f_i' \in \mathcal{M}_R'$ be of type $(s_0, \ldots, s_{t-1})$ and let p^{β_i} be the invariant of f_i' with respect to $\eta_{1,r}$. Then*

$$\beta_i = \sum_{i=0}^{t-1} \max\{0, r - s_i\}.$$

Proof: We shall assume that $t \geq 2$. When $t = 1$ a similar and easier argument works, but we omit the details to keep the notation simple and the argument clear, since this case is already known [37]. (However if $t = 1$ and $q = 2$, arguments based

on Jacobi sums do not work. It is still possible, though, to construct elements of RG to get an SNF basis in a favorable form.) Let $\alpha_i = \sum_{j=0}^{t-1} \max\{0, r - s_j\}$. Let $f_i \in \mathcal{M}'_R$ and let $f_i \in \mathcal{M}_R$ be the basis monomial which has the same reduction modulo $\mathfrak{p}$ as f'_i, namely $f_i := T(\bar{f}'_i)$. We use the notation of Definition 5.2.2 with $M = R^{\mathcal{L}_1}$ and $\phi = \eta_{1,r}$. By Lemma 5.1.1, we have $f_i \in M_{\alpha_i}$. Since the image of $\bar{f}_i = \bar{f}'_i$ in $\overline{M}_{\beta_i}/\overline{M}_{\beta_i+1}$ is not zero, it follows that $\alpha_i \leq \beta_i$.

Suppose by way of contradiction that $\beta_k > \alpha_k$ for some k. Let $f_k = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n})$ be of type $(s_0, s_1, \ldots, s_{t-1})$. Assume that we have picked k so that if $\alpha_j < \alpha_k$ then $\alpha_j = \beta_j$. By Lemma 5.3.7 we can assume for convenience that $s_1 = \min\{s_0, \ldots, s_{t-1}\}$. We have

$$\lambda_0 = ps_1 - s_0 \leq n(p-1)$$

with equality only if $s_0 = s_1 = \cdots = s_{t-1} = n$ and

$$\lambda_1 = ps_2 - s_1 \geq 1.$$

We note that the case $s_0 = s_1 = \cdots = s_{t-1} = n$ will not occur by our assumption that $\beta_k > \alpha_k$. The reason is as follows. If f_k has type $(s_0, s_1, \ldots, s_{t-1}) = (n, n, \ldots, n)$, by Lemma 5.4.1, we see that $p \nmid \eta_{1,r}(f_k)$. Since $\bar{f}'_k = \bar{f}_k$, we have $p \nmid \eta_{1,r}(f'_k)$. But the invariant corresponding to f'_k is p^{β_k}, and we assumed that $\beta_k > \alpha_k = 0$, so $p \,|\, \eta_{1,r}(f'_k)$, a contradiction.

By Lemma 5.2.5, basis vectors in $\mathcal{M}'_R$ of the same type correspond to the same invariant, so in the sum $\lambda_0 = \sum_{i=0}^{n} a_{i,0}$ we can assume that $a_{0,0} = 0$, and we can also assume that $a_{1,0} < p - 1$ since the case $s_0 = s_1 = \cdots = s_{t-1} = n$ has been excluded. In the sum $\lambda_1 = \sum_{i=0}^{n} a_{i,1}$, we can assume that $a_{0,1} \geq 1$. By these assumptions, we see that $0 < p \leq b_0 < q - 1$. Hence from our definition of $\mathcal{M}'_R$ we have

$$f'_k = f_k.$$

Since the exponent b_0 in f_k is not equal to 1, applying the group ring element $h \in RG$ in Lemma 5.3.2, we get

$$hf'_k = hf_k = -J(T^{-1}, T^{b_0})T(x_0^{b_0-1}x_1^{b_1+1}x_2^{b_2}\cdots x_n^{b_n}). \tag{5.8}$$

Set $T(x_0^{b_0-1}x_1^{b_1+1}x_2^{b_2}\cdots x_n^{b_n}) := f_\ell \in \mathcal{M}_R$. The type of f_ℓ is $(s_0, s_1+1, s_2, \ldots, s_{t-1})$ because we have increased λ_0 by p and decreased λ_1 by 1. Also note that $b_0 - 1$ is still strictly between 0 and $q-1$, so $f_\ell = f'_\ell \in \mathcal{M}'_R$. As for the coefficient of f_ℓ in (5.8), Lemma 5.3.1 tells us that p divides $J(T^{-1}, T^{b_0})$ exactly once because when 1 is added to $q-1-b_0$ there is exactly one carry: from the ones place to the p place of the sum. Since $p^{\beta_k} \,|\, \eta_{1,r}(f'_k)$ and $\eta_{1,r}$ is an RG-module homomorphism, we have

$$p^{\beta_k} \mid \eta_{1,r}(hf'_k).$$

Since $p \parallel J(T^{-1}, T^{b_0})$, we get

$$p^{(\beta_k-1)} \mid \eta_{1,r}(f'_\ell),$$

where the type of f'_ℓ is $(s_0, s_1+1, s_2, \ldots, s_{t-1})$. Since we assumed that α_k was the smallest such that $\alpha_k < \beta_k$, we must conclude that

$$\sum_{j=0}^{t-1} \max\{0, r-s_j\} = \sum_{j=0, j\neq 1}^{t-1} \max\{0, r-s_j\} + \max\{0, r-(s_1+1)\}.$$

That is, $s_1 \geq r$. Since s_1 is assumed to be the smallest among $s_j, 0 \leq j \leq t-1$, we see that

$$s_j \geq r,\ 0 \leq j \leq t-1, \text{ and hence } \alpha_k = 0.$$

By Lemma 5.4.1, $p \nmid \eta_{1,r}(f_k)$, so $p \nmid \eta_{1,r}(f'_k)$ since $f'_k = f_k$. However we have assumed that $\beta_k > \alpha_k = 0$, that is, $p \,|\, \eta_{1,r}(f'_k)$, which is a contradiction. The theorem is proved. □

The theorem shows that the bound in Theorem 2.5.8 is exact.

Corollary 5.4.3. *The monomial basis $\mathcal{M}_R$ is an SNF basis of $R^{\mathcal{L}_1}$ for the map $\eta_{1,r}$ and the invariant of a monomial of type $(s_0, \ldots, s_{t-1})$ is equal to*

$$\sum_{i=0}^{t-1} \max\{0, r - s_i\}.$$

Remark 5.4.4. We have seen that, for each r, the $R\mathrm{GL}(n+1,q)$ homomorphism $\eta_{1,r}$ defines a filtration $\{\overline{M}_i\}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ by $\mathbb{F}_q\mathrm{GL}(n+1,q)$-modules. In the case $r = n$, it follows from Theorem 5.4.2 and [7, Theorems A, B] that this filtration is equal to the radical filtration, the most rapid descending filtration with semisimple factors. Equivalently, $M_i = J^i(\mathbb{F}_q^{\mathcal{L}_1})$, where J is the Jacobson radical of the group algebra $\mathbb{F}_q\mathrm{GL}(n+1,q)$.

5.5 Proof of the Bardoe/Sin module structure result

In this section we give a proof of Theorem 3.4.2. First, we need to supplement Lemma 5.3.5 with the following lemma to cover those monomials in which every exponent is divisible by $q-1$, which were excluded from Lemma 5.3.5.

Lemma 5.5.1. *Let $f_i = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in M_R$ be a basis monomial with every exponent either 0 or $q-1$, let $b_k = 0$, and let $f_i^* = T(x_k^{q-1}) f_i$. For any*

$$f = c_1 f_1 + c_2 f_2 + \cdots + c_v f_v$$

in $R^{\mathcal{L}_1}$. There is an element $g_i \in RG$, which depends on f, such that

$$g_i f = c_i (f_i + \frac{q}{1-q} f_i^*)$$

Proof: Without loss of generality we can take $b_0 = q-1$ and $k = 1$ (*i.e.*, $b_1 = 0$). We will first treat the case where $f_i = T(x_0^{q-1} x_1^0 x_2^{q-1} \cdots x_n^{q-1})$. In this case we have

$$f_i^* = T(x_0^{q-1} x_1^{q-1} x_2^{q-1} \cdots x_n^{q-1}),$$

which is not a basis monomial—but we can write this f_i^* as a linear combination of some basis monomials in $\mathcal{M}_R$ with coefficients ± 1. Explicitly,

$$f_i^* = T(x_0^{q-1} \cdots x_n^{q-1}) - \prod_{j=0}^{n} \big(T(x_j^{q-1}) - 1\big). \tag{5.9}$$

Note that here we are dealing with functions from $\mathcal{L}_1$ to R, so at least one x_j is nonzero. By Corollary 5.3.3, we can find an element $g_1 = g(0) \in RG$ such that

$$g_1 f_i = T(x_0^{q-2} x_1 x_2^{q-1} \cdots x_n^{q-1}). \tag{5.10}$$

No other basis monomial will have the monomial (5.10) in its image. Since the exponent of x_0 is $q-2$, lying strictly between 0 and $q-1$, we can apply Lemma 5.3.5 to get an element $g_3 \in RG$ such that

$$g_3 g_1 f = c_i T(x_0^{q-2} x_1 x_2^{q-1} \cdots x_n^{q-1}).$$

Now apply Corollary 5.3.3 to the above monomial (with the roles of x_0 and x_1 interchanged), we get an element $g_2 = \frac{1}{q-1}g'(0) \in RG$ such that

$$g_2 g_3 g_1 f = c_i(f_i + \frac{q}{1-q} f_i^*).$$

Therefore the lemma is proved in this case.

From now on we assume that at least two of the exponents of f_i are 0. By this assumption, we see that $f_i^* = T(x_0^{q-1} x_1^{q-1} x_2^{b_2} \cdots x_n^{b_n})$ is actually a basis monomial. Let $f_i^* = f_j \in \mathcal{M}_R$. Using the element $g_1 = g(0) \in RG$ from Corollary 5.3.3 we have

$$g_1 f_i = g_1 f_j = T(x_0^{q-2} x_1 x_2^{b_2} \cdots x_n^{b_n}).$$

No other monomials will have exactly this monomial as its image, so by the previous lemma there is $g_3 \in RG$ such that

$$g_3 g_1 f = (c_i + c_j) T(x_0^{q-2} x_1 x_2^{b_2} \cdots x_n^{b_n}).$$

If $\nu_p(c_i) \neq \nu_p(c_j)$, then

$$g_i = \frac{c_i}{c_i + c_j} g_2 g_3 g_1,$$

with g_2 as above, will be exactly the element of RG we want. Otherwise, we need to premultiply f by an element of RG which raises the p-adic valuation of c_j while leaving the valuation of c_i unchanged.

Suppose in f_i that $\kappa \geq 2$ is the number of coordinates whose exponent is 0, and $(n+1-\kappa)$ is the number which are $q-1$. For this construction, we will relabel the monomials and renumber the coordinates so that

$$\begin{aligned}
f_i = f_1' &= T(x_0^{q-1} x_1^0 x_2^0 \cdots x_\kappa^0 x_{\kappa+1}^{q-1} x_{\kappa+2}^{q-1} \cdots x_n^{q-1}) \\
f_2' &= T(x_0^{q-1} x_1^{q-1} x_2^0 \cdots x_\kappa^0 x_{\kappa+1}^{q-1} x_{\kappa+2}^{q-1} \cdots x_n^{q-1}) \\
f_3' &= T(x_0^{q-1} x_1^{q-1} x_2^{q-1} x_3^0 \cdots x_\kappa^0 x_{\kappa+1}^{q-1} x_{\kappa+2}^{q-1} \cdots x_n^{q-1}) \\
\vdots \quad &\vdots \qquad\qquad \vdots \\
f_\kappa' &= T(x_0^{q-1} \cdots x_{\kappa-1}^{q-1} x_\kappa^0 x_{\kappa+1}^{q-1} \cdots x_n^{q-1})
\end{aligned}$$

and with the renumbering we have

$$f = c'_1 f'_1 + \cdots + c'_\kappa f'_\kappa + c'_{\kappa+1} f'_{\kappa+1} + \cdots c'_v f'_v.$$

We consider two cases. First suppose that the coefficients

$$c'_1, c'_2, \ldots, c'_\iota, \ \iota < \kappa$$

all have the same p-adic valuation, but that the valuations of c'_ι and $c'_{\iota+1}$ are different. Then by the above argument there exists $g_\iota \in RG$ for which

$$g_\iota f = c'_\iota f_\iota + \frac{c'_\iota q}{1-q} f_{\iota+1}$$

and

$$(1-g)f = c'_1 f'_1 + \cdots + c'_{\iota-1} f'_{\iota-1} + 0 \cdot f'_\iota + \cdots .$$

Now the valuations of $c'_{\iota-1}$ and c'_ι are different. By induction we have the required premultiplier.

Now suppose that the coefficients $c'_1, c'_2, \ldots, c'_\kappa$ all have the same p-adic valuation. We apply the element $g_4 \in RG$ to f, which in particular shifts 1 from the exponent of $x_{\kappa-1}$ to the exponent of x_κ in the basis monomial f'_κ. Then we apply $g_5 \in RG$ from the previous lemma to $g_4 f$, which kills every monomial except

$$T(x_0^{q-1} \cdots x_{\kappa-2}^{q-1} x_{\kappa-1}^{q-2} x_\kappa x_{\kappa+1}^{q-1} \cdots x_v^{q-1}).$$

Next we apply $g_6 \in RG$ which shifts 1 from the exponent of x_κ back to the exponent of $x_{\kappa-1}$. Since $T(x_\kappa^{q-1} f'_\kappa)$ is not in our basis, the calculation above gives

$$g_6 g_5 g_4 f = c'_\kappa (q-1) f'_\kappa - c'_\kappa q T(x_\kappa^{q-1}) f'_\kappa.$$

The expression

$$T(x_\kappa^{q-1}) f'_\kappa = T(x_0^{q-1} \cdots x_n^{q-1})$$

is not a basis monomial, but by (5.9), it can be written as a linear combination of basis monomials with ± 1 coefficients. Using (5.9), we calculate that

$$(1 + g_6 g_5 g_4)f = (c'_1 \pm qc'_\kappa)f'_1 + (c'_2 \mp qc'_\kappa)f'_2 + \cdots + (c'_{\kappa-1} + qc'_\kappa)f'_{\kappa-1} + 0 \cdot f'_\kappa + \cdots$$

and we are back to the first case. This completes the proof. □

The following observation allows us to apply Lemma 5.3.5 and Lemma 5.5.1 to $\mathbb{F}_q^{\mathcal{L}_1}$.

Lemma 5.5.2. *Let $X \in R^{\mathcal{L}_1}$ and let $g \in RG$. By $g \pmod{\mathfrak{p}}$ we mean the element of $\mathbb{F}_q G$ obtained by reducing the coefficient of each element of G in g modulo $\mathfrak{p}$. Then*

$$gX \pmod{\mathfrak{p}} = [g \pmod{\mathfrak{p}}][X \pmod{\mathfrak{p}}].$$

Proof: Clear from the definitions. □

We are now ready to prove Theorem 3.4.2 for $q \neq 2$. The theorem is still true for $q = 2$, but using Jacobi sums and summing over $(q-1)^{\text{th}}$ roots of unity does not help when $q = 2$.

Proof: [Theorem 3.4.2] Since $|\mathcal{L}_1|$ is not divisible by p, $\mathbb{F}_q^{\mathcal{L}_1}$ is the direct sum of the module of the constant functions and the module of functions which sum to 0 over $\mathcal{L}_1$. We only need to consider functions of the second type, those with no constant term. To prove the theorem, we need to demonstrate four claims.

1. The module that is generated by any function contains all the monomials with nonzero coefficients in the representation of that function in the monomial basis.

2. The module generated by any monomial contains all the other monomials of the same type.

3. The module generated by a monomial of a given type generates at least one monomial of any given lower type, in the sense that if $(s_0, \ldots, s_{t-1})$

and $(s'_0, \ldots, s'_{t-1})$ are both in $\mathcal{H}$, then $(s'_0, \ldots, s'_{t-1})$ is a lower type than $(s_0, \ldots, s_{t-1})$ if $s'_i \leq s_i$ for each $i \in \{0, \ldots, t-1\}$.

4. The expression for the image of any monomial under the action of any group element has coefficient zero for any basis monomial whose type is higher than the original monomial. Thus each module described in the theorem is invariant under the group action.

The first claim is clear from Lemma 5.3.5 and Lemma 5.5.1, since we can start with any polynomial function and kill all the monomial terms except one, by applying the appropriate group ring element.

The second and third claims follow from Corollary 5.3.3. We write the p-adic expansions of the exponents of our given monomial.

$$b_i = a_{i,0} + \cdots + a_{i,t-1}p^{t-1}$$

The lemma allows us to subtract 1 from any nonzero digit of any exponent and add the corresponding power of p to any other exponent. The Jacobi sum will be a unit in R, (since the subtraction $b_i - p^j$ did not require borrowing), so its reduction mod $(\mathfrak{p})$ is not zero. Thus we can partition the sums

$$\lambda_j = a_{0,j} + \cdots + a_{n,j}$$

in any way we like, proving the second claim.

To change a monomial of type $(s_0, \ldots, s_j, \ldots, s_{t-1})$ to one of type $(s_0, \ldots, s_j - 1, \ldots, s_{t-1})$, we need to add 1 to the sum λ_j and subtract p from the sum λ_{j-1}. If $\lambda_{j-1} < p$, or if $\lambda_j = (n+1)(p-1)$, then $(s_0, \ldots, s_j - 1, \ldots, s_{t-1}) \notin \mathcal{H}$. Otherwise we pick b_i such that $a_{i,j} < p-1$, move enough units of p^{j-1} to b_i to cause a carry from $a_{i,j-1}$ to $a_{i,j}$, and we have the desired monomial. Then we note that if $(s_0, \ldots, s_{t-1})$ and $(s'_0, \ldots, s'_{t-1})$ are both in $\mathcal{H}$, and if $s'_j \leq s_j$ for each $i \in \{0, \ldots, t-1\}$, then the following algorithm gets us from $(s_0, \ldots, s_{t-1})$ to $(s'_0, \ldots, s'_{t-1})$ by way of t-tuples

which are all in $\mathcal{H}$ and with each step involving subtracting 1 from only one entry of the t-tuple. Of all those cases where $s_j \neq s'_j$, we pick one where s_j is as large as possible. We know that

$$0 \leq ps_{j+1} - s_j \leq (p-1)(n+1)$$

$$0 \leq ps_j - s_{j-1} \leq (p-1)(n+1)$$

$$2 \leq s_j \leq n$$

$$\text{either } s_{j+1} = s'_{j+1} \text{ or } s_{j+1} \leq s_j$$

$$\text{either } s_{j-1} = s'_{j-1} \text{ or } s_{j-1} \leq s_j.$$

We conclude that

$$0 \leq ps_{j+1} - (s_j - 1) \leq (p-1)(n+1)$$

$$0 \leq p(s_j - 1) - s_{j-1} \leq (p-1)(n+1)$$

so that $(s_0, \ldots, s_j - 1, \ldots, s_{t-1}) \in \mathcal{H}$.

To prove the last claim, let $f = x_0^{b_0} \cdots x_n^{b_n}$. Recall that $s_j(q-1)$ is the degree of

$$f^{p^{t-j}} = (x_0^{b_0} \cdots x_n^{b_n})^{p^{t-j}},$$

with all the exponents reduced by the substitution $x_i^q = x_i$. Then for any $g \in G$, the image gf has the form

$$(c_{0,0}x_0 + \cdots + c_{0,n}x_n)^{b_0} \cdots (c_{n,0}x_0 + \cdots + c_{n,n}x_n)^{b_n}$$

which is a homogeneous polynomial of degree $s_0(q-1)$ before reduction. After reduction, all the monomials are of degree at least $q-1$ and at most $s_0(q-1)$. Similarly,

$$(gf)^{p^{t-j}} = (c_{0,0}^{p^{t-j}} x_0^{p^{t-j}} + \cdots + c_{0,n}^{p^{t-j}} x_n^{p^{t-j}})^{b_0} \cdots (c_{n,0}^{p^{t-j}} x_0^{p^{t-j}} + \cdots + c_{n,n}^{p^{t-j}} x_n^{p^{t-j}})^{b_n}$$

is homogeneous of degree $s_j(q-1)$ before reduction. After reduction, all the monomials are of degree at least $q-1$ and at most $s_j(q-1)$. The proof is complete. $\square$

Chapter 6

AFFINE GEOMETRIES

6.1 The Invariant Factors of the Incidence between points and r-flats in $\mathrm{AG}(n,q)$

In this chapter, we consider the incidence between points and r-flats in the affine geometry $\mathrm{AG}(n,q)$. We will view $\mathrm{AG}(n,q)$ as obtained from $\mathrm{PG}(n,q)$ by deleting a hyperplane and all the subspaces it contains. Let H_0 be the hyperplane of $\mathrm{PG}(n,q)$ given by the equation $x_0 = 0$. Then for any integer r, $0 \leq r \leq n$, the set of r-flats of $\mathrm{AG}(n,q)$ is

$$\mathcal{F}_r = \{Y \setminus (Y \cap H_0) \mid Y \in \mathcal{L}_{r+1}\}.$$

(The empty set is not considered as an r-flat for any r.) In particular, the set of points of $\mathrm{AG}(n,q)$ is $\mathcal{F}_0$. We define the incidence map

$$\eta'_{0,r} : \mathbb{Z}^{\mathcal{F}_0} \to \mathbb{Z}^{\mathcal{F}_r} \tag{6.1}$$

by letting $\eta'_{0,r}(Z) = \sum_{Y \in \mathcal{F}_r, Z \subset Y} Y$ for every $Z \in \mathcal{F}_0$, and then extending $\eta'_{0,r}$ linearly to $\mathbb{Z}^{\mathcal{F}_0}$. Similarly, we define $\eta'_{r,0}$ to be the map from $\mathbb{Z}^{\mathcal{F}_r}$ to $\mathbb{Z}^{\mathcal{F}_0}$ sending an r-flat of $\mathrm{AG}(n,q)$ to the formal sum of all points incident with it. Let A_1 be the matrix of $\eta'_{0,r}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{F}_0}$ and $\mathbb{Z}^{\mathcal{F}_r}$. We have the following counterpart of Theorem 3.2.1.

Theorem 6.1.1. *The invariant factors of A_1 are all powers of p.*

Proof: The proof is parallel to that of Theorem 3.2.1. We will actually work with $A_1^\top$, which is the matrix of $\eta'_{r,0} : \mathbb{Z}^{\mathcal{F}_r} \to \mathbb{Z}^{\mathcal{F}_0}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{F}_r}$ and $\mathbb{Z}^{\mathcal{F}_0}$. We define

$$\epsilon' : \mathbb{Z}^{\mathcal{F}_0} \to \mathbb{Z}$$

to be the function sending each element in $\mathcal{F}_0$ to 1. Clearly ϵ' maps $\mathbb{Z}^{\mathcal{F}_0}$ onto $\mathbb{Z}$ and $\operatorname{Im}\eta'_{r,0}$ onto $q^r\mathbb{Z}$. Thus, $\mathbb{Z}^{\mathcal{F}_0}/(\operatorname{Ker}\epsilon' + \operatorname{Im}\eta'_{r,0}) \cong \mathbb{Z}/q^r\mathbb{Z}$, and we are reduced to proving that $(\operatorname{Ker}\epsilon' + \operatorname{Im}\eta'_{r,0})/\operatorname{Im}\eta'_{r,0}$ is a p-group. The proof goes in exactly the same way as that in Theorem 3.2.1. Note that $\operatorname{Ker}(\epsilon')$ is spanned by elements in $\mathbb{Z}^{\mathcal{F}_0}$ of the form $u-w$, where u and w are distinct points of $\mathrm{AG}(n,q)$; so it is enough to show that $q^r(u-w) \in \operatorname{Im}(\eta'_{r,0})$ for any two distinct points u and w. We pick an $(r+1)$-flat containing the two distinct points u and w and let $\tilde{\eta}'_{0,r}$ be the restricted map. The number of r-flats through one point in $\mathrm{AG}(r+1,q)$ is $(q^{r+1}-1)/(q-1)$ while the number of r-flats through two points in $\mathrm{AG}(r+1,q)$ is $(q^r-1)/(q-1)$ so we get

$$\eta'_{r,0}(\tilde{\eta}'_{0,r}(z)) = q^r z + \frac{q^r-1}{q-1}\mathbf{j}_U$$

for any point z. Therefore

$$\eta'_{r,0}(\tilde{\eta}'_{0,r}(u-w)) = q^r(u-w).$$

This completes the proof. □

In view of the above theorem, we view A_1 as a matrix with entries from $R = \mathbb{Z}_p[\xi_{q-1}]$. The Smith normal form of A_1 over R will completely determine the Smith normal form of A_1 over $\mathbb{Z}$. We will get the p-adic invariants of A_1 from the invariants of the incidence between points and $(r+1)$-spaces in $\mathrm{PG}(n,q)$ and those of the incidence between points and $(r+1)$-spaces in $\mathrm{PG}(n-1,q)$.

Let A be the matrix of the incidence map $\eta_{1,r+1} : R^{\mathcal{L}_1} \to R^{\mathcal{L}_{r+1}}$ with respect to the standard bases of $R^{\mathcal{L}_1}$ and $R^{\mathcal{L}_{r+1}}$. We want to partition A into a certain block form. For this purpose, we define

$$\mathcal{L}_1^{H_0} = \{Z \in \mathcal{L}_1 \mid Z \subseteq H_0\},$$

and

$$\mathcal{L}_{r+1}^{H_0} = \{Y \in \mathcal{L}_{r+1} \mid Y \subseteq H_0\}.$$

So we have the partitions

$$\mathcal{L}_1 = \mathcal{F}_0 \cup \mathcal{L}_1^{H_0},$$

and

$$\mathcal{L}_{r+1} = \mathcal{F}_r \cup \mathcal{L}_{r+1}^{H_0}.$$

We now partition A as

$$A = \left[\begin{array}{c|c} \overbrace{A_1}^{\mathcal{F}_0} & \overbrace{A_2}^{\mathcal{L}_1^{H_0}} \\ \hline 0 & A_3 \end{array}\right] \begin{array}{l} \} \, \mathcal{F}_r \\ \} \, \mathcal{L}_{r+1}^{H_0} \end{array}$$

where A_3 is the incidence matrix of the incidence between $\mathcal{L}_1^{H_0}$ and $\mathcal{L}_{r+1}^{H_0}$, which can be thought as the matrix of the incidence between points and $(r+1)$-spaces in $\mathrm{PG}(n-1, q)$.

In order to obtain the SNF of A_1, we need to modify the monomial basis $\mathcal{M}_R$ of $R^{\mathcal{L}_1}$ slightly. We replace the constant monomial in $\mathcal{M}_R$ by $T(x_0^{q-1}x_1^{q-1}\cdots x_n^{q-1})$ and denote the resulting set by $\mathcal{M}_R^*$. Note that $\mathcal{M}_R^*$ is still a basis of $R^{\mathcal{L}_1}$ because $(1-a_0^{q-1})(1-a_1^{q-1})\cdots(1-a_n^{q-1}) = 0$ for each point $(a_0, a_1, \ldots, a_n)$ of $\mathrm{PG}(n, q)$. Furthermore $\mathcal{M}_R^*$ is an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r+1}$ since $\mathcal{M}_R$ is an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r+1}$ and the invariant corresponding to $T(x_0^{q-1}x_1^{q-1}\cdots x_n^{q-1})$ is 1. So we have the factorization

$$P^*D = AQ^*, \tag{6.2}$$

where the columns of Q^* are the basis vectors in M_R^* written with respect to the standard basis of $R^{\mathcal{L}_1}$, P^* is nonsingular over R and D is the Smith normal form of A.

We now partition $\mathcal{M}_R^*$ as $\mathcal{B}_1 \cup \mathcal{B}_2$, where

$$\mathcal{B}_1 = \{T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \mid b_0 \neq 0, T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R^*\},$$

and

$$\mathcal{B}_2 = \{T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \mid b_0 = 0, T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R^*\}.$$

We partition the matrix Q^* according to the partition of $\mathcal{M}_R^*$ as $\mathcal{B}_1 \cup \mathcal{B}_2$ and the partition of $\mathcal{L}_1$ as $\mathcal{F}_0 \cup \mathcal{L}_1^{H_0}$. Explicitly we have

$$Q^* = \left[\begin{array}{c|c} \overbrace{Q_1}^{\mathcal{B}_1} & \overbrace{Q_2}^{\mathcal{B}_2} \\ \hline 0 & Q_3 \end{array}\right] \begin{array}{l} \} \, \mathcal{F}_0 \\ \} \, \mathcal{L}_1^{H_0} \end{array}$$

where the columns of Q_3 are the basis vectors in $\{f|_{H_0} \mid f \in \mathcal{B}_2\}$ written with respect to the standard basis of $R^{\mathcal{L}_1^{H_0}}$.

Now we rewrite (6.2) according to the block forms of the matrices A and Q^*. We have

$$\begin{pmatrix} P_1 & P_3 & P_5 \\ 0 & P_2 & P_4 \end{pmatrix} \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix} \begin{pmatrix} Q_1 & Q_2 \\ 0 & Q_3 \end{pmatrix} \tag{6.3}$$

which gives us

$$P_1 D_1 = A_1 Q_1,$$

and

$$P_2 D_2 = A_3 Q_3.$$

Since P_1 and Q_1 inherit the property that the reductions modulo $\mathfrak{p}$ of their columns are linearly independent, D_1 must be the Smith normal form of A_1. By Corollary 5.4.3, $\{f|_{H_0} \mid f \in \mathcal{B}_2\}$ is an SNF basis of $R^{\mathcal{L}_1^{H_0}}$ for the incidence map $\eta_{1,r+1}$

between points and $(r+1)$-spaces in $\mathrm{PG}(n-1,q)$. We see that D_2 is the Smith normal form of A_3.

For any $n \geq 2$, $1 < i \leq n$, and $\alpha \geq 0$, let $m(\alpha, n, i)$ denote the multiplicity of p^α as a p-adic invariant of the incidence between points and projective $(i-1)$-dimensional subspaces in $\mathrm{PG}(n,q)$. (The numbers $m(\alpha, n, i)$ are determined by Theorem 3.5.1.) We have the following theorem.

Theorem 6.1.2 (Theorem B). *The p-adic invariants of A_1 are p^α, $0 \leq \alpha \leq rt$, with multiplicity $m(\alpha, n, r+1) - m(\alpha, n-1, r+1)$.*

Proof: From (6.3), we see that the multiplicity of p^α as an invariant of A_1 is equal to the number of times p^α appears in D minus the number of times p^α appears in D_2. □

Chapter 7

THE INCIDENCE AMONG OTHER SETS OF SUBSPACES

In this chapter we present what we know about the incidence matrix $A_{r,s}$ between r-subspaces and s-subspaces of the n-dimensional vector space V over $\mathbb{F}_q$ when $1 < s < r < n$. In this case we do not have a 2-design, because the number of r-subspaces which are incident with two distinct s-subspaces depends on the dimension of the intersection of those two s-subspaces. We do still have a 1-design, because each s-subspace is incident with $\begin{bmatrix} n+1-s \\ r-s \end{bmatrix}_q$ r-subspaces and each r-subspace is incident with $\begin{bmatrix} r \\ r-s \end{bmatrix}_q$ s-subspaces. Recall that the "generalized" binomial coefficient

$$\begin{bmatrix} r \\ r-s \end{bmatrix}_q = \begin{bmatrix} r \\ s \end{bmatrix}_q = \Big(\prod_{i=1}^{s}(q^{r+1-i}-1)\Big)/\Big(\prod_{i=1}^{s}(q^i-1)\Big)$$

is the number of s-subspaces of an r-dimensional vector space over $\mathbb{F}_q$.

7.1 The cross-characteristic invariants

In [17], Frumkin and Yakir proved the following theorem giving the rank of $A_{r,s}$ over any field whose characteristic is not p (the cross-characteristic rank). Let $A_{r,s}$ be as before.

Theorem 7.1.1. *Let $s \leq r$, let $s + r \leq n + 1$, and let K be any field whose characteristic is not p. Let*

$$Y = \left\{ i \mid 0 \leq i \leq s, \ \begin{bmatrix} r-i \\ s-i \end{bmatrix}_q \neq 0 \right\}.$$

Then with the convention $\begin{bmatrix} n+1 \\ -1 \end{bmatrix}_q = 0$,

$$\operatorname{rank}_K(A_{r,s}) = \sum_{i \in Y} \begin{bmatrix} n+1 \\ i \end{bmatrix}_q - \begin{bmatrix} n+1 \\ i-1 \end{bmatrix}_q .$$

Thus the rank is full if the characteristic of K is 0. As far as we know, the following result, which gives a diagonal form for $A_{r,s}$, is new.

Theorem 7.1.2 (Theorem C). *Let* $s \leq r,\ s+r \leq n+1$, *and* $A_{r,s}$ *be as before. Let* ℓ *be any prime not dividing* q. *Then over* $\mathbb{Z}_\ell$, *the* ℓ*-adic integers,* $A_{r,s}$ *has a diagonal form whose entries are* $\begin{bmatrix} r-i \\ s-i \end{bmatrix}_q$ *with multiplicity* $\begin{bmatrix} n+1 \\ i \end{bmatrix}_q - \begin{bmatrix} n+1 \\ i-1 \end{bmatrix}_q$.

Proof: The proof is exactly the same as the proof of Theorem 7.1.1, except at the very end. We give some highlights of that proof. In [23], James develops the theory of *Specht* submodules of the KG-module $K^{\mathcal{L}_r}$ where K is some field. When the characteristic of K does not divide q, he has some strong results.

The Specht submodule $S_r \subset K^{\mathcal{L}_r}$ can be viewed as follows. If $r < n/2 + 1$ then

$$S_r = \cap_{i=0}^{r-1} \ker(\eta_{r,i}),$$

where, as before, $\eta_{r,s} : K^{\mathcal{L}_r} \to K^{\mathcal{L}_s}$ is the incidence map. James calls this the kernel intersection theorem.

If K has characteristic 0, the kernels are nested. In this case, $S_r = \ker(\eta_{r,r-1})$. Since this map has full rank, the dimension of S_r is $\begin{bmatrix} n+1 \\ r \end{bmatrix}_q - \begin{bmatrix} n+1 \\ r-1 \end{bmatrix}_q$. If $K = \mathbb{F}_\ell$, then $\eta_{r,r-1}$ does not in general have full rank, but the dimension of the Specht submodule S_r is still $\begin{bmatrix} n+1 \\ r \end{bmatrix}_q - \begin{bmatrix} n+1 \\ r-1 \end{bmatrix}_q$. We can obtain it from the ℓ-adic Specht module. Let S_r be the ℓ-adic Specht submodule of the $\mathbb{Q}_\ell G$-module $\mathbb{Q}_\ell^{\mathcal{L}_r}$. Then the finite-field Specht submodule is

$$\bar{S}_r = \left\{ X \pmod{\ell} \mid X \in S_r \cap \mathbb{Z}_\ell^{\mathcal{L}_r} \right\}.$$

The main result of James used in this proof is the submodule theorem.

Theorem 7.1.3. *If $X \in K^{\mathcal{L}_r}$ and X is not orthogonal to every vector in S_r under the ordinary inner product, then the KG-submodule generated by X contains S_r.*

In particular, it is easily shown in [17] that for $r > i,\ r + i \leq n + 1$, we have $S_i \subseteq \mathrm{Im}(\eta_{r,i})$. Using this last fact, and some other properties of Specht submodules, we get the following result.

Theorem 7.1.4. *Let $s \leq r,\ s + r \leq n + 1$. Let $char(K) \neq p$. Then the vector space spanned over K by all the rows of the matrices $A_{i,r},\ 0 \leq i \leq s$ has dimension $\begin{bmatrix} n+1 \\ s \end{bmatrix}_q$ and it has a basis consisting of $\begin{bmatrix} n+1 \\ i \end{bmatrix}_q - \begin{bmatrix} n+1 \\ i-1 \end{bmatrix}_q$ rows from $A_{i,r}$ for each $i,\ 0 \leq i \leq s$.*

Now we use the well-known formula for $i \leq s \leq r$

$$A_{i,s} \circ A_{s,r} = \begin{bmatrix} r-i \\ s-i \end{bmatrix}_q A_{i,r}, \tag{7.1}$$

which says there are $\begin{bmatrix} r-i \\ s-i \end{bmatrix}_q$ s-subspaces which contain a given i-subspace and are contained by a given r-subspace, if the given i-subspace is contained in the r-subspace, and no such s-subspaces otherwise. Then we apply Theorem 7.1.4 twice with $K = \mathbb{F}_\ell$. First we pick $|\mathcal{L}_s|$ linearly independent rows from the matrices $A_{i,s}$ for $0 \leq i \leq s$ as specified in Theorem 7.1.4. If we stack up those rows, we get a matrix P, which is invertible over $\mathbb{F}_\ell$. By Nakayama's Lemma, it is also invertible viewed as a matrix over $\mathbb{Z}_\ell$. Then stacking up the corresponding rows of (7.1), $0 \leq i \leq s$, we get the matrix equation in $\mathbb{Z}_\ell$

$$PA_{s,r} = DQ'$$

where P is invertible in the ℓ-adic ring, D is the diagonal form specified in Theorem C, and Q' is some $|\mathcal{L}_s| \times |\mathcal{L}_r|$ matrix. Therefore the diagonal matrix D (suitably arranged) can be taken as a lower bound on the ℓ-adic Smith normal form of $A_{s,r}$.

Then we use Theorem 7.1.4 again to pick $|\mathcal{L}_s|$ linearly independent (over $\mathbb{F}_\ell$) rows from the matrices $A_{i,r}$ for $0 \leq i \leq s$. We can extend this set of vectors to get

an $|\mathcal{L}_r| \times |\mathcal{L}_r|$ matrix which is invertible over $\mathbb{F}_\ell$. Again by Nakayama's lemma, the Teichmüller lifting of this matrix is invertible over $\mathbb{Z}_\ell$. Stacking up the corresponding rows of (7.1) we get

$$P' A_{s,r} = D' Q$$

where D' is the same as D with $|\mathcal{L}_r| - |\mathcal{L}_s|$ columns of zeros added, Q is invertible over $\mathbb{Z}_\ell$, and P' is some $|\mathcal{L}_s| \times |\mathcal{L}_s|$ matrix. This equation shows that D can be viewed as giving an upper bound on the ℓ-adic Smith normal form. Together, we find that the ℓ-adic invariants of $A_{s,r}$ are exactly the diagonal entries of D. □

7.2 The open question

Since we have determined the ℓ-adic invariants for $\ell \neq p$, the question that remains is the p-adic part of the Smith normal form, including the p-rank. It turns out that we can calculate the eigenvalues and eigenspaces of $A_{s,r}A_{r,s}$. In particular, if $r + s = n + 1$, that is, if $A_{r,s}$ is a square matrix, we can calculate the determinant of $A_{r,s}$. The p-part of this determinant will be the product of the p-adic invariants. In this section we shall work over $\mathbb{Q}$. That is, we view the incidence matrix $A_{s,r}$ as a matrix over $\mathbb{Q}$ and use $\eta_{s,r}$ to denote the incidence map from $\mathbb{Q}^{\mathcal{L}_s}$ to $\mathbb{Q}^{\mathcal{L}_r}$.

Theorem 7.2.1. *Let $0 \leq i \leq s \leq r$ and let $s+r \leq n+1$. Let $S_i = \mathrm{Ker}\,(\eta_{i,i-1}) \subset \mathbb{Q}^{\mathcal{L}_i}$ be the Specht submodule and let $\eta_{i,s}(S_i)$ be the image of S_i in $\mathbb{Q}^{\mathcal{L}_s}$ under the incidence map. Then $\eta_{i,s}(S_i)$ is an eigenspace of $A_{s,r}A_{r,s}$ with eigenvalue*

$$q^{i(r-s)} \begin{bmatrix} r-i \\ r-s \end{bmatrix}_q \begin{bmatrix} n+1-i-s \\ r-s \end{bmatrix}_q .$$

Proof: First, we claim that $A_{s,r}A_{r,s}$ is invertible over a field of characteristic 0. We use Frumkin's and Yakir's result (see [17]) that $A_{s,r}$ has full rank over such a field. We have $|\mathcal{L}_s| \leq |\mathcal{L}_r|$ so $\eta_{r,s}$ is surjective and $\eta_{s,r}$ is injective. Thus $\eta_{s,r} \circ \eta_{r,s}$ has rank equal to $|\mathcal{L}_s|$. Since $A_{r,s}A_{s,r}$ is symmetric, it is diagonizable, and eigenspaces of nonequal eigenvalues are mutually orthogonal. In effect, $\eta_{r,s}$ maps the eigenspaces

of the nonzero eigenvalues of $A_{r,s}A_{s,r}$ onto the eigenspaces of $A_{s,r}A_{r,s}$ with the same eigenvalues, and $\eta_{s,r}$ maps the eigenspaces of $A_{s,r}A_{r,s}$ onto the eigenspaces of $A_{r,s}A_{s,r}$ having nonzero eigenvalues. We conclude that $\mathbb{Q}^{\mathcal{L}_r}$ is the direct sum of the orthogonal subspaces $\eta_{s,r}(\mathbb{Q}^{\mathcal{L}_s})$ and $\mathrm{Ker}(\eta_{r,s})$. In particular, $\mathbb{Q}^{\mathcal{L}_i} = \mathrm{Im}(\eta_{i-1,i}) \oplus S_i$.

Next we show that $\mathbb{Q}^{\mathcal{L}_s}$ is the direct sum of subspaces

$$\mathbb{Q}^{\mathcal{L}_s} = \eta_{0,s}(S_0) \oplus \eta_{1,s}(S_1) \oplus \cdots \oplus \eta_{i-1,s}(S_{s-1}) \oplus S_s \tag{7.2}$$

where the first $i+1$ terms of the sum give us $\mathrm{Im}(\eta_{i,s})$. (We view $\eta_{0,-1}$ as mapping a one-dimensional space to a zero-dimensional space, so that $S_0 = \mathrm{Ker}(\eta_{0,-1}) \cong \mathbb{Q}$, and $\eta_{0,s}(S_0)$ is the span of the all-one vector in $\mathbb{Q}^{\mathcal{L}_s}$.) By the transitivity property (3.2) of incidence maps, $\eta_{\ell,s} \circ \eta_{i,\ell} = \begin{bmatrix} s-i \\ \ell-i \end{bmatrix}_q \eta_{i,s}$, $i \le \ell \le s$, we have the nesting of subspaces

$$\mathrm{Im}(\eta_{0,s}) \subset \mathrm{Im}(\eta_{1,s}) \subset \cdots \subset \mathrm{Im}(\eta_{s-1,s}) \subset \mathbb{Q}^{\mathcal{L}_s}.$$

We use induction. Assume we have the direct sum

$$\mathrm{Im}(\eta_{i-1,s}) = \eta_{0,s}(S_0) \oplus \eta_{1,s}(S_1) \oplus \cdots \oplus \eta_{i-1,s}(S_{i-1}).$$

By injectivity of $\eta_{i,s}$ and transitivity we have

$$\begin{aligned} \eta_{i,s}(\mathbb{Q}^{\mathcal{L}_i}) &= \eta_{i,s}\big(\eta_{i-1,i}(\mathbb{Q}^{\mathcal{L}_{i-1}}) \oplus S_i\big) \\ &= \eta_{i-1,s}(\mathbb{Q}^{\mathcal{L}_{i-1}}) \oplus \eta_{i,s}(S_i) \\ &= \eta_{0,s}(S_0) \oplus \cdots \oplus \eta_{i-1,s}(S_{i-1}). \end{aligned}$$

Since the base case is trivial, (7.2) is a direct sum.

Now we pick $Z \in \mathbb{Q}^{\mathcal{L}_i}$. We will define $M_\ell^{(Z)}$ to be the following subspace of $\mathbb{Q}^{\mathcal{L}_\ell}$ (which is not an invariant subspace with respect to the action of G). Let Y be any element of $\mathcal{L}_\ell$. We require that every element $f \in M_\ell^{(Z)}$, viewed as a function from $\mathcal{L}_\ell$ to the rational numbers, can be specified by a function h from the integers to the rationals via

$$f(Y) = h\Big(\dim(Y \cap Z)\Big) \tag{7.3}$$

so that the value of $f(Y)$ depends only on the size of the intersection of Y with the fixed i-subspace Z inside V. Note that if $i \leq \ell \leq n+1-i$, then $M_\ell^{(Z)}$ is an $(i+1)$-dimensional subspace of $\mathbb{Q}^{\mathcal{L}_\ell}$. It is also clear that $\eta_{\ell,r}$ maps $M_\ell^{(Z)}$ to $M_r^{(Z)}$, and that $M_\ell^{(Z)} \subset \mathrm{Im}(\eta_{i,\ell})$. If we assume that $\ell \leq r \leq n+1-\ell$ then $\eta_{\ell,r}$ and $\eta_{r,\ell} \circ \eta_{\ell,r}$ are injective, so we can represent the restriction $\eta_{r,\ell}\,|_{(Z)} \circ \eta_{\ell,r}\,|_{(Z)}$ to $M_\ell^{(Z)}$ and $M_r^{(Z)}$ as an invertible $\big((i+1)\times(i+1)\big)$-matrix. If we know the first i eigenvalues, then there can be at most one more. Furthermore, since the original $(|\mathcal{L}_i| \times |\mathcal{L}_i|)$-matrix was symmetric, the eigenspace of this last eigenvector must be orthogonal to the other eigenspaces (with respect to the ordinary dot product of vectors of length $|\mathcal{L}_i|$).

Next, define $\mathfrak{W}$ to be the set of all those $(i-1)$-dimensional subspaces contained in Z. For each $W \in \mathfrak{W}$ we can set up an i-dimensional subspace of $\mathbb{Q}^{\mathcal{L}_\ell}$ similar to what we did for Z. What we want is to combine them into a single i-dimensional space. Take any vector $f \in M_\ell^{(\mathfrak{W})}$ to be a vector of the form

$$f = \sum_{W \in \mathfrak{W}} \sum_{j=0}^{i-1} c_j \sum_{\substack{Y \in \mathcal{L}_\ell, \\ \dim(Y \cap W) = j}} Y.$$

We know that $M_\ell^{(\mathfrak{W})}$ is i-dimensional because if $c_0 = c_1 = \cdots = c_{j-1} = 0$ but $c_j \neq)$ then the coefficient of an element of $\mathcal{L}_\ell$ whose intersection with Z has size j is nonzero, but the coefficient of any element with smaller intersection is zero. Also $M_\ell^{(\mathfrak{W})} \subset M_\ell^{(Z)}$ because the total coefficient of an element of $\mathcal{L}_\ell$ can depend only on its intersection size with Z. The eigenvalues of $M_\ell^{(W)}$ also have eigenvectors in $M_\ell^{(\mathfrak{W})}$, because we can sum the corresponding eigenvector in $M_\ell^{(W)}$ over each $W \in \mathfrak{W}$.

We claim that the one extra eigenvector that is in $M_\ell^{(Z)}$ but not in $M_\ell^{(\mathfrak{W})}$ lies inside $\eta_{i,\ell}(S_i)$. We know that S_i is orthogonal to $\mathrm{Im}(\eta_{i-1,i})$. By inductive hypothesis we have the first i eigenvalues of $\eta_{\ell,i} \circ \eta_{i,\ell}$, corresponding to $\mathrm{Im}(\eta_{i-1,i})$. The other eigenvector must be orthogonal to these, so it is in S_i. Now assume that this last eigenvalue is different from the others. When we map it to $M_\ell^{(Z)}$ via $\eta_{i,\ell}$, we get an

eigenvector of $\eta_{i,\ell} \circ \eta_{\ell,i}$ with the same eigenvalue. Therefore $M_\ell^{(\mathfrak{W})}$ is also orthogonal to $\eta_{i,\ell}(S_i)$. Again by inductive hypothesis we have i eigenspaces inside $M_\ell^{(\mathfrak{W})}$ for $\eta_{r,\ell} \circ \eta_{\ell,r}$, so the last eigenspace must be orthogonal to $M_\ell^{(\mathfrak{W})}$, that is, in $\eta_{i,\ell}(S_i)$.

Now we claim that

$$\sum_{Z \in \mathcal{L}_i} M_\ell^{(Z)} = \mathrm{Im}(\eta_{i,\ell}).$$

In (7.3), let h be the function which maps i to 1 and all other integers to 0. The corresponding vector is exactly the image of Z. Therefore $\eta_{i,\ell}(Z) \in M_\ell^{(\mathfrak{W})}$. Since Z could be any i-space, we get all of $= \mathrm{Im}(\eta_{i,\ell})$.

Finally, we calculate the eigenvalues and verify that they are all different, as claimed. Our typical eigenvector lies in $M_\ell^{(Z)} \cap \eta_{i,\ell}(S_i) = M_\ell^{(Z)} \cap \mathrm{Ker}(\eta_{\ell,i-1}$. We assume that $i \leq \ell \leq n - i$.

We begin by calculating the eigenvalue for the map $\eta_{\ell+1,\ell} \circ \eta_{\ell,\ell+1}$. First we get information about the eigenvector from the fact that it lies in $\mathrm{Ker}(\eta_{\ell,i-1})$. Let $W \in \mathcal{L}_{i-1}$ be contained in Z. The coefficient of W must be zero in the image of the eigenvector under the map $\eta_{\ell,i-1}$. We calculate the coefficients of the eigenvector corresponding to intersection dimension with Z of i and $i-1$. These are the only coefficients which contribute to W under the map $\eta_{\ell,i-1}$. There are $\begin{bmatrix} n+2-i \\ \ell-i+1 \end{bmatrix}_q$ elements of $\mathcal{L}_\ell$ which contain W. Of these, $\begin{bmatrix} n+1-i \\ \ell-i \end{bmatrix}_q$ contain Z and the rest, $\begin{bmatrix} n+2-i \\ \ell-i+1 \end{bmatrix}_q - \begin{bmatrix} n+1-i \\ \ell-i \end{bmatrix}_q = q^{\ell+1-i} \begin{bmatrix} n+1-i \\ \ell-i+1 \end{bmatrix}_q$ have intersection dimension $i-1$. We let 1 be the coefficient of those elements of $\mathcal{L}_\ell$ which contain Z and let $-\begin{bmatrix} n+1-i \\ \ell-i \end{bmatrix}_q \Big/ \left(q^{\ell+1-i} \begin{bmatrix} n+1-i \\ \ell-i+1 \end{bmatrix}_q\right) = -\left(q^{\ell-i+1}-1\right) q^{i-\ell-1} \Big/ \left(q^{n-\ell+1}-1\right)$ be the coefficient of those elements of $\mathcal{L}_\ell$ intersecting Z in dimension $i-1$.

Let $Y \in \mathcal{L}_\ell$ contain Z. We calculate its coefficient after applying $\eta_{\ell+1,\ell} \circ \eta_{\ell,\ell+1}$, which will be the eigenvalue. This coefficient will be the sum over the three classes of ℓ-spaces of the coefficient in the starting vector times the multiplicity times the corresponding entry of the matrix for $\eta_{\ell+1,\ell} \circ \eta_{\ell,\ell+1}$. No element of $\mathcal{L}_\ell$ whose intersection dimension with Y is less than $i-1$ contributes because no element of

$\mathcal{L}_{\ell+1}$ contains both it and Y. We count the contribution of Y itself, from elements of $\mathcal{L}_\ell$ containing Z but intersecting Y in dimension $\ell-1$, and from those intersecting Z in dimension $i-1$ and Y in dimension $\ell-1$. The matrix entries are $(q_{n+1-\ell}-1)/(q-1)$, 1, and 1, respectively. The multiplicities of the elements are

$$1, \left(\frac{q^{\ell-i}-1}{q-1}\right)\left(\frac{q^{n+2-\ell}-1}{q-1}-1\right), \text{ and}$$

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

Set $\left(\frac{q^{n+2-\ell}-1}{q-1}-1\right)=\psi$. Summing up, we find the eigenvalue to be

$$\begin{aligned}(1)\left(\frac{q^{n+1-\ell}-1}{q-1}\right)(1) &+ (1)(1)\left(\frac{q^{\ell-i}-1}{q-1}\right)\psi\\ &- q^{i-\ell-1}\frac{q^{\ell-i+1}-1}{q^{n-\ell+1}-1}(1)\left(\frac{q^{\ell}-q^{\ell-i}}{q-1}\right)\psi\\ &= \frac{q^{n+2-i}-q^{n+1-\ell}-q^{\ell+1}+q^{i}}{(q-1)(q-1)}\\ &= q^{i}\frac{(q^{\ell+1-i}-1)(q^{n+1-i-\ell}-1)}{(q-1)(q-1)}\\ &= q^{i}\begin{bmatrix}\ell+1-i\\1\end{bmatrix}_q\begin{bmatrix}n+1-i-\ell\\1\end{bmatrix}_q.\end{aligned}$$

We get the eigenvalue for the map $\eta_{r,s}\circ\eta_{s,r}$ by induction. Setting $\ell=r-1$ in the above calculation, we multiply the eigenvalue for $\eta_{r-1,s}\circ\eta_{s,r-1}$ by the eigenvalue for $\eta_{r,r-1}\circ\eta_{r-1,r}$ to get the eigenvalue for $\eta_{r-1,s}\circ\eta_{r,r-1}\circ\eta_{r-1,r}\circ\eta_{s,r-1}$. Using (3.2) again, we divide by $\left(\begin{bmatrix}r-s\\1\end{bmatrix}_q\right)^2$ to get the eigenvalue for $\eta_{r,s}\circ\eta_{s,r}$ as stated. □

Chapter 8

TWO OTHER FAMILIES OF DIFFERENCE SETS

8.1 Introduction

Recall that for a prime power $q = p^t$, the parameters for a Singer difference set are

$$v = \frac{q^m - 1}{q - 1}, \qquad k = \frac{q^{m-1} - 1}{q - 1}, \qquad \lambda = \frac{q^{m-2} - 1}{q - 1}. \tag{8.1}$$

or the complementary These parameters, or the complementary parameters, $v = (q^m - 1)/(q - 1)$, $k = q^{m-1}$, $\lambda = q^{m-2}(q - 1)$, where m is a positive integer greater than 2, are called *c*lassical parameters. Difference sets with classical parameters exist in abundance when m is composite. See [43] for a survey of known constructions up to 1999.

In the study of difference sets with classical parameters, one typically faces the following question. After constructing a family of difference sets with classical parameters, how can one tell whether the difference sets constructed are equivalent to the known ones or not? The standard proof of inequivalence has been comparison of p-ranks of the difference sets involved (see [16], [13], [1]). Recent constructions of difference sets with classical parameters provided us with examples of $(\frac{3^m-1}{2}, 3^{m-1}, 2 \cdot 3^{m-2})$ difference sets having the same 3-ranks, the HKM difference sets and the Lin difference sets. It remained to decide whether these difference sets are equivalent or not. We will use the Smith normal forms of the designs associated with the HKM and Lin difference sets to show not only that the HKM and Lin difference sets are inequivalent, but also that the associated designs are nonisomorphic.

We now define the HKM and Lin difference sets. Let $\mathbb{F}_{q^m}$ denote the finite field with q^m elements, let $\mathbb{F}_{q^m}^*$ be the multiplicative group of $\mathbb{F}_{q^m}$, let $\mathrm{Tr}_{q^m/q}$ denote the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, and let the map $\rho : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ denote the natural epimorphism.

Definition 8.1.1. *Let $q = 3^t$, $t \geq 1$, let $m = 3k$, k a positive integer, $d = q^{2k} - q^k + 1$, and set*

$$R = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}. \tag{8.2}$$

We will call the set $\rho(R)$ the HKM difference set.

Helleseth, Kumar, and Martinsen proved that $\rho(R)$ is a $((q^m - 1)/(q - 1), q^{m-1}, q^{m-2}(q-1))$ difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, in the case $q = 3$, using the language of sequences with ideal 2-level autocorrelation in [20]. See [13] for the proof when q is any 3-power ([13] also showed that R is a relative difference set).

Definition 8.1.2. *Let $m \geq 3$ be an odd integer, let $d = 2 \cdot 3^{(m-1)/2} + 1$, and set*

$$R = \{x \in \mathbb{F}_{3^m} \mid \mathrm{Tr}_{3^m/3}(x + x^d) = 1\}. \tag{8.3}$$

We will call the set $\rho(R)$ the Lin difference set.

Arasu, Dillon and Player recently proved that $\rho(R)$ is a $((3^m - 1)/2, 3^{m-1}, 2 \cdot 3^{m-2})$ difference set in $\mathbb{F}_{3^m}^*/\mathbb{F}_3^*$ [2], as Lin conjectured.

In the case $q = 3$, $m = 3k$, $k > 1$, the 3-rank of the HKM difference set is $2m^2 - 2m$ (see [13, 33]). One can similarly show that the Lin difference set has 3-rank $2m^2 - 2m$, where $m > 3$ is odd (see [33]). Therefore when m is an odd multiple of 3, these two difference sets have the same 3-rank. It is natural to ask whether there are some other invariants beyond 3-rank which can be used to distinguish these two families of difference sets. We will show that these families are indeed inequivalent by using Smith normal forms of the incidence matrices of the symmetric designs developed from these difference sets.

8.2 The Smith Normal Forms of Difference Sets

Let G be a (multiplicative) abelian group of order v, and let D be a (v, k, λ) difference set in G. Recall that $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a (v, k, λ) symmetric design with a regular automorphism group G, where the set $\mathcal{P}$ of *points* of $\mathcal{D}$ is G, and where the set $\mathcal{B}$ of *blocks* of $\mathcal{D}$ is $\{Dg \mid g \in G\}$. We call this design the *development* of D. We will examine the Smith normal form of the incidence matrix of $\mathcal{D}$, the v by v matrix A whose rows are indexed by the blocks B of $\mathcal{D}$ and whose columns are indexed by the points g of $\mathcal{D}$, where the entry $A_{B,g}$ in row B and column g is 1 if $g \in B$, and 0 otherwise.

Since A is an integral matrix, we know that there exist two integral unimodular matrices P and Q such that $PAQ = \mathrm{diag}(d_1, d_2, \ldots, d_v)$ is the Smith normal form of A where d_i are integers, and $d_i | d_{i+1}$, for $i = 1, 2, \ldots, \mathrm{rank}(A) - 1$. Moreover the invariant factors, d_i, of A, are determined up to sign. For convenience, we define *the Smith normal form of the symmetric design* $\mathcal{D}$ to be the Smith normal form of its incidence matrix A. This Smith normal form is also called *the Smith normal form of the difference set* D, and the invariant factors of A are called *the invariant factors* of D.

Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be two (v, k, λ) symmetric designs, and let A_1 and A_2 be the incidence matrices of $\mathcal{D}_1$ and $\mathcal{D}_2$ respectively. If $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic, that is, there exist two permutation matrices U and V such that

$$UA_1V = A_2, \tag{8.4}$$

then it is clear that A_1 and A_2 should have the same Smith normal form. So the Smith normal forms can help us decide whether two symmetric designs are isomorphic or not.

If the design $\mathcal{D}$ is developed from a (v, k, λ) abelian difference set, then the following lemmas can be used to compute the number of invariant factors not divisible by p^α, where p is a prime not dividing v.

We will start with the local case, then move to the global case. The following notation will be used: p is a prime, ν_p is the p-adic valuation on $\mathbb{Q}$, $\mathbb{Q}_p$ is the field of p-adic rational numbers (the completion of $\mathbb{Q}$ with respect to ν_p), $\mathbb{Z}_p$ is the ring of p-adic integers, ζ_v is a primitive v^{th} root of unity in the algebraic closure of $\mathbb{Q}_p$, $K = \mathbb{Q}_p(\zeta_v)$, $\mathcal{O}_K$ is the ring of integers in K, and finally $\mathfrak{p}$ is the unique maximal ideal in $\mathcal{O}_K$ lying above p.

Lemma 8.2.1. *Let G be an abelian group of order v, and p be a prime not dividing v. Let D be a (v, k, λ) difference set in G, and let α be a positive integer. Then the number of invariant factors of D which are not divisible by p^α is equal to the number of characters $\chi : G \to K$ satisfying*

$$\chi(D) \not\equiv 0 \pmod{\mathfrak{p}^\alpha}. \tag{8.5}$$

Proof: Let $\sum_{g\in G} a_g g$, where $a_g = 0$ or 1, be the group ring element in $\mathbb{Z}[G]$ corresponding to the subset D of G. That is, $a_g = 1$ if $g \in D$, 0 otherwise. We associate with D the matrix $A = (a_{g^{-1}h})$ whose rows and columns are indexed by the group elements g and h. This matrix A can serve as the incidence matrix of the design $(G, \{Dg \mid g \in G\})$ developed from D.

Let $\big(\chi^{-1}(g)\big)$ be a matrix whose rows are labeled by the v characters $\chi : G \to K$ and whose columns are labeled by the v group elements g, so that the entry in row χ and column g is $\chi^{-1}(g)$. This matrix is invertible in $\mathcal{O}_K$, since $\gcd(p, v) = 1$ and $\frac{1}{v}\big(\chi^{-1}(g)\big)\big(\chi(g)\big)^\top$ is the identity matrix. We may diagonalize A over $\mathcal{O}_K$ as follows.

$$\big(\chi^{-1}(g)\big)A\big(\chi(g)\big)^\top = v \cdot \operatorname{diag}\big(\chi(D)\big), \tag{8.6}$$

where $\chi(D) = \sum_{g\in G} a_g \chi(g)$.

Viewing A as a matrix with entries in $\mathbb{Z}$, we use $S = \mathrm{diag}(d_1, d_2, \ldots, d_v)$ to denote the Smith normal form of A over $\mathbb{Z}$. Then there exist integral unimodular matrices P and Q such that $A = PSQ$. Therefore we have

$$\big(\chi^{-1}(g)\big)PSQ\big(\chi(g)\big)^{\top} = v \cdot \mathrm{diag}\big(\chi(D)\big). \tag{8.7}$$

This equation shows that S and $\mathrm{diag}\big(\chi(D)\big)$, viewed as matrices with entries in $\mathcal{O}_K$, are equivalent over $\mathcal{O}_K$. Noting that $\mathcal{O}_K$ is a principal ideal domain, we see that S and $\mathrm{diag}\big(\chi(D)\big)$ have the same invariant factors up to unit multipliers. Since $\mathcal{O}_K$ is local, and as $p \nmid v$ implies that K is unramified over $\mathbb{Q}_p$, each $\chi(D)$ can be written as the product of a power of p and a unit in $\mathcal{O}_K$. So if we arrange the elements on the diagonal of $\mathrm{diag}\big(\chi(D)\big)$ in such a way that the $\nu_p(\chi(D))$ are nondecreasing, then $\mathrm{diag}\big(\chi(D)\big)$ can serve as a Smith normal form of A over $\mathcal{O}_K$. Therefore the two lists $\nu_p(d_i)$ and $\nu_p(\chi(D))$ are exactly the same. Noting that $p \nmid v$, we have $\nu_{\mathfrak{p}}(\chi(D)) = \nu_p(\chi(D))$: the conclusion of the lemma follows. □

We now state the global version of Lemma 8.2.1.

Lemma 8.2.2. *Let G be an abelian group of order v, let p be a prime not dividing v, and let $\mathfrak{P}$ be a prime ideal in $\mathbb{Z}[\xi_v]$ lying above p , where ξ_v is a complex primitive vth root of unity. Let D be a (v, k, λ) difference set in G, and let α be a positive integer. Then the number of invariant factors of D which are not divisible by p^α is equal to the number of complex characters χ of G such that $\chi(D) \not\equiv 0 \pmod{\mathfrak{P}^\alpha}$.*

Proof: Let A be the matrix defined in the proof of Lemma 8.2.1. We may use A as the incidence matrix of the design $(G, \{Dg \mid g \in G\})$ developed from D. Similarly let $\big(\chi^{-1}(g)\big)$ be a matrix whose rows are labeled by the v complex characters χ and whose columns are labeled by the v group elements g, so that the entry in row χ and column g is $\chi^{-1}(g)$. Then we may diagonalize A over $\mathbb{Q}(\xi_v)$ as follows.

$$\big(\chi^{-1}(g)\big)A\big(\chi(g)\big)^{\top} = v \cdot \mathrm{diag}\big(\chi(D)\big), \tag{8.8}$$

where $\chi(D) = \sum_{g \in D} \chi(g)$.

Viewing A as a matrix with entries in $\mathbb{Z}$, we use $S = \mathrm{diag}(d_1, d_2, \ldots, d_v)$ to denote the Smith normal form of A over $\mathbb{Z}$. Then there exist integral unimodular matrices P and Q such that $A = PSQ$. Therefore we have

$$\big(\chi^{-1}(g)\big) PSQ \big(\chi(g)\big)^{\top} = v \cdot \mathrm{diag}\big(\chi(D)\big). \tag{8.9}$$

Let $L = \mathbb{Q}(\xi_v)$, and let $L_{\mathfrak{P}}$ be the completion of L at $\mathfrak{P}$. $L_{\mathfrak{P}}$ is an extension field of $\mathbb{Q}_p$, and we may view L as embedded in $L_{\mathfrak{P}}$. Since $\gcd(p, v) = 1$, L is unramified over $\mathbb{Q}$. Hence $L_{\mathfrak{P}}$ is unramified over $\mathbb{Q}_p$. Let $\mathcal{O}_{\mathfrak{P}}$ be the valuation ring in $L_{\mathfrak{P}}$, and let $\mathfrak{p}$ be the unique prime ideal in $\mathcal{O}_{\mathfrak{P}}$ lying above p. Then for every $a \in L_{\mathfrak{P}}$, we have

$$\nu_{\mathfrak{P}}(a) = \nu_{\mathfrak{p}}(a) \tag{8.10}$$

Now view all matrices in (8.9) as matrices with entries in $\mathcal{O}_{\mathfrak{P}}$. We see that S and $\mathrm{diag}\big(\chi(D)\big)$ are equivalent over $\mathcal{O}_{\mathfrak{P}}$. Noting that $\mathcal{O}_{\mathfrak{P}}$ is a principal ideal domain, we see that S and $\mathrm{diag}\big(\chi(D)\big)$ have the same invariant factors up to unit multipliers. Since $\mathcal{O}_{\mathfrak{P}}$ is local and $L_{\mathfrak{P}}$ is unramified over $\mathbb{Q}_p$, each $\chi(D)$ can be written as the product of a power of p and a unit in $\mathcal{O}_{\mathfrak{P}}$. So if we arrange the elements on the diagonal of $\mathrm{diag}\big(\chi(D)\big)$ appropriately so that the $\nu_p(\chi(D))$ are nondecreasing, then $\mathrm{diag}\big(\chi(D)\big)$ can serve as a Smith normal form of A over $\mathcal{O}_{\mathfrak{P}}$. Hence the two lists $\nu_p(d_i)$ and $\nu_p(\chi(D))$ are exactly the same. Note that by (8.10), we have $\nu_{\mathfrak{P}}(\chi(D)) = \nu_{\mathfrak{p}}(\chi(D))$, and $\nu_{\mathfrak{p}}(\chi(D)) = \nu_p(\chi(D))$. The conclusion of the lemma follows. □

Remark 8.2.3. *Lemma 8.2.2 generalizes a result of MacWilliams and Mann [32], which asserts that the* GF(p)*-rank of A is equal to the number of complex characters χ such that $\chi(D) \not\equiv 0$ (mod $\mathfrak{P}$).*

Finally, we note that if $\mathcal{D}$ is a $((q^m-1)/(q-1), q^{m-1}, q^{m-2}(q-1))$ symmetric design, where $q = p^s$, p is prime, and A is the incidence matrix of $\mathcal{D}$, then

$$\det(A) = q^{(m-2)(v-1)/2+(m-1)}, \tag{8.11}$$

where $v = (q^m-1)/(q-1)$. Therefore the invariant factors of A are all powers of p. The number of invariant factors of A which are 1 is exactly the rank of A over $\mathbb{Z}/p\mathbb{Z}$, which is usually called *the p-rank of* $\mathcal{D}$. In the next section, we will be interested in not only the number of ones among the invariant factors of A, but also the number of p's among the invariant factors of A.

8.3 The Invariant Factors of the HKM and Lin Difference Sets

In this section we will show that the Lin difference sets and the HKM difference sets are in general inequivalent when they are comparable. Note that both these difference sets have parameters $((q^m-1)/(q-1), q^{m-1}, q^{m-2}(q-1)), q = 3^e$, so by the discussion at the end of the previous section, the invariant factors of these difference sets are all powers of 3. Although the numbers of ones among the invariant factors of these two difference sets are the same in the case $e = 1$ (cf. [13], [33]), we will show that the numbers of 3's are different.

Let $q = 3^e$, $e \geq 1$, let $m = 3k$ and $d = q^{2k} - q^k + 1$ (this is the HKM case); or let $q = 3^e$, $e = 1$, $m = 2n+1$ and $d = 2 \cdot 3^n + 1$ (this is the Lin case). Let $\rho : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ be the natural epimorphism, and let

$$D = \{\rho(x) \mid x \in \mathbb{F}_{q^m} \text{ and } \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}$$

be the difference sets defined in Section 1. We first give explicit expressions for the character sums $\chi(D)$, where χ is any complex character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. This was done in [13]; we include these computations here for the convenience of the reader.

Let L be a complete system of coset representatives of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^m}^*$, and let $L_0 = \{x \in L \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 0\}$. If $x \in L$ and $\mathrm{Tr}_{q^m/q}(x + x^d) = a \neq 0$, then we may replace x by x/a, and

$$\mathrm{Tr}_{q^m/q}\left(\frac{x}{a} + (\frac{x}{a})^d\right) = \mathrm{Tr}_{q^{3k}/q}(x + x^d)/a = 1.$$

Therefore we may choose L such that $L = L_0 \cup L_1$, where $L_1 = \{x \in L \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}$. It is then easy to see that

$$L_1 = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\} \text{ and } D = \rho(L_1).$$

Given any multiplicative character χ of $\mathbb{F}_{q^m}$, we define the sum

$$S_d(\chi) = \sum_{x \in \mathbb{F}_{q^m}^*} \chi(x) \xi_3^{\mathrm{Tr}_{q^m/3}(x+x^d)}. \tag{8.12}$$

Writing $x = ay$, with $a \in \mathbb{F}_q^*$ and $y \in L$, we have

$$\begin{aligned} S_d(\chi) &= \sum_{a \in \mathbb{F}_q^*} \chi(a) \sum_{y \in L} \chi(y) \xi_3^{\mathrm{Tr}_{q/3}\left(a\mathrm{Tr}_{q^m/q}(y+y^d)\right)} \\ &= \sum_{y \in L_0} \chi(y) \sum_{a \in \mathbb{F}_q^*} \chi(a) + \sum_{y \in L_1} \chi(y) \sum_{a \in \mathbb{F}_q^*} \chi(a)\, \xi_3^{\mathrm{Tr}_{q/3}(a)} \end{aligned}$$

If $\chi = 1$, then $S_d(1) = (q-1)\,|L_0| - |L_1| = q^m - 1 - q\,|L_1|$.

If $\chi \neq 1$, but $\chi|_{\mathbb{F}_q^*} = 1$, then $S_d(\chi) = -q\,\chi(L_1)$.

If $\chi \neq 1$, and $\chi|_{\mathbb{F}_q^*} \neq 1$, then $S_d(\chi) = \chi(L_1) \cdot g_1(\chi_1)$, where χ_1 is the restriction of χ to $\mathbb{F}_q^*$, and $g_1(\chi_1)$ is the Gauss sum over the finite field $\mathbb{F}_q$ with respect to χ_1.

In summary, if χ is a nontrivial multiplicative character of $\mathbb{F}_{q^m}$, then

$$\chi(L_1) = \begin{cases} -\frac{1}{q}\, S_d(\chi)\,, & \text{if } \chi|_{\mathbb{F}_q^*} = 1\,, \\ \frac{S_d(\chi)}{g_1(\chi_1)}\,, & \text{if } \chi|_{\mathbb{F}_q^*} \neq 1\,. \end{cases} \tag{8.13}$$

For $\mathfrak{P}$ a prime ideal in $\mathbb{Z}[\xi_{q^m-1}]$ lying over 3, let $\omega_{\mathfrak{P}}$ be the Teichmüller character on $\mathbb{F}_{q^m}$. Then any nontrivial character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ takes the form $\omega_{\mathfrak{P}}^{-a}$,

$0 < a < (q^m - 1)$ with $(q-1)|a$. By (8.13), for any a, $0 < a < (q^m - 1)$ and $(q-1)|a$, we have

$$\omega_{\mathfrak{P}}^{-a}(D) = \omega_{\mathfrak{P}}^{-a}(L_1) = -\frac{1}{q} S_d(\omega_{\mathfrak{P}}^{-a}). \tag{8.14}$$

Let $\tilde{\mathfrak{P}}$ be the prime of $\mathbb{Z}[\xi_{q^m-1}, \xi_3]$ lying above $\mathfrak{P}$, and let

$$t_d(a) = \nu_{\tilde{\mathfrak{P}}}(S_d(\omega_{\mathfrak{P}}^{-a})) \tag{8.15}$$

be the $\tilde{\mathfrak{P}}$-adic valuation of $S_d(\omega_{\mathfrak{P}}^{-a})$.

Lemma 8.3.1. *With the above notation, for any nonnegative integer $\alpha \leq m-2$, the number of invariant factors of D which are 3^α is*

$$|\{a \mid 0 < a < (q^m - 1),\ (q-1)|a,\ t_d(a) = 2e + 2\alpha\}|.$$

Proof: By Lemma 8.2.2, the number of invariant factors of D which are 3^α is equal to the number of $\omega_{\mathfrak{P}}^{-a}$, $0 < a < (q^m - 1)$ and $(q-1)|a$, such that $\mathfrak{P}^\alpha || \omega_{\mathfrak{P}}^{-a}(D)$. As ideals in $\mathbb{Z}[\xi_{q^m-1}, \xi_3]$, $\mathfrak{P} = \tilde{\mathfrak{P}}^2$. Hence the number of invariant factors of D which are 3^α is equal to the number of $\omega_{\mathfrak{P}}^{-a}$, $0 < a < (q^m - 1)$ and $(q-1)|a$, such that $\tilde{\mathfrak{P}}^{2\alpha} || \omega_{\mathfrak{P}}^{-a}(D)$.

To simplify notation, we will usually drop the index in $\omega_{\mathfrak{P}}$ if there is no confusion. By (8.14), we have $\omega^{-a}(D) = -\frac{1}{3^e} S_d(\omega^{-a})$. By definition, we have

$$\nu_{\tilde{\mathfrak{P}}}(S_d(\omega^{-a})) = t_d(a).$$

Also it is clear that $\nu_{\tilde{\mathfrak{P}}}(3^e) = 2e$. Therefore, the number of a, $0 < a < (q^m - 1)$, $(q-1)|a$ such that $\tilde{\mathfrak{P}}^{2\alpha} \parallel \omega^{-a}(D)$ is equal to the cardinality of the set

$$\mathcal{T}_\alpha = \{a \mid 0 < a < (q^m - 1),\ (q-1)|a,\ t_d(a) = 2e + 2\alpha\}. \tag{8.16}$$

We will denote this cardinality by T_α, and we have shown that the number of invariant factors of D which are 3^α is equal to T_α. This completes the proof. □

In order to compute explicitly the number of invariant factors of D which are 3^α, we need to compute $t_d(a)$ first. By the definition of Gauss sums, we have

$$g(\omega^b) = \sum_{x \in \mathbb{F}_{q^m}^*} \omega^b(x) \xi_3^{\mathrm{Tr}_{q^m/3}(x)}.$$

Using Fourier inversion, we find that

$$\xi_3^{\mathrm{Tr}_{q^m/3}(x^d)} = \frac{1}{q^m - 1} \sum_{b=0}^{q^m-2} g(\omega^{-b}) \omega^b(x^d).$$

Therefore

$$\begin{aligned} S_d(\omega^{-a}) &= \frac{1}{q^m - 1} \sum_{x \in \mathbb{F}_{q^m}^*} \omega^{-a}(x) \xi_3^{\mathrm{Tr}_{q^m/3}(x)} \sum_{b=0}^{q^m-2} g(\omega^{-b}) \omega^{bd}(x) \\ &= \frac{1}{q^m - 1} \sum_{b=0}^{q^m-2} g(\omega^{-b}) g(\omega^{bd-a}) \end{aligned}$$

As usual, for any integer x not divisible by $q^m - 1$ we use $s(x)$ to denote the 3-adic weight (the base-3 digit sum) of $x \pmod{q^m - 1}$. In addition, if $x \equiv 0 \pmod{q^m - 1}$, we set $s(x) = 0$. With this convention, using Stickelberger's theorem on the prime ideal decomposition of Gauss sums [21, p. 212], we find that

$$t_d(a) \geq \min_{0 \leq b \leq q^m - 2} \{s(b) + s(a - bd)\}. \tag{8.17}$$

Moreover, if the above minimum is attained at **exactly one** value of b in the range $[0, q^m - 2]$, then

$$t_d(a) = \min_{0 \leq b \leq q^m - 2} \{s(b) + s(a - bd)\}.$$

In general, the function $t_d(a)$ is hard to control. Hence it is difficult to compute explicitly the cardinality of $\mathcal{T}_\alpha$ (see (8.16) for definition). In [13], we computed T_0 in the case $q = 3$. In the following, we will assume that $q = 3$, *i.e.,* $e = 1$, and find explicit formulas for the cardinality T_1 of

$$\mathcal{T}_1 = \{a \mid 0 < a < 3^m - 1, 2|a, t_d(a) = 4\},$$

for both d given at the beginning of this section.

When calculating the 3-ranks of the HKM and Lin difference sets in [13] in the case $q = 3$, that is computing the number of even a, $0 < a < 3^m - 1$, for which $t_d(a) = 2$, we first list all a, $0 < a < 3^m - 1$, such that $\min_{0 \le b \le 3^m - 2} \{s(b) + s(a - bd)\} = 2$; in both the HKM and Lin cases, there are exactly two values of a, up to cyclic shift, for which $s(b) + s(a - bd) = 2$ at more than one value of b when $m > 3$. (For all other a in the list, there is a unique b in the range $[0, 3^m - 2]$ such that $s(b) + s(a - bd) = 2$: thus $t_d(a) = 2$.) For these two "exceptional" values of a, we had to do more detailed analysis to decide whether $t_d(a) = 2$ or $t_d(a) > 2$. In the former case, we count the a towards the 3-rank, and in the latter case we do not. The final conclusion is that both HKM and Lin difference sets have 3-rank $2m^2 - 2m$ when $m > 3$ (see [13] and [33]).

Now if we want to count the number of invariant factors which are 3 for the HKM and Lin difference sets, we need to compute the number T_1 of even a, $0 < a < 3^m - 1$, for which $t_d(a) = 4$. Again we need to pay special attention to those a, for which $s(b) + s(a - bd) = 4$ at more than one value of b (we again call these a "exceptional"). Unfortunately, the list of such a's already becomes awkwardly large. Instead of analyzing each "exceptional" a individually, we argue that, except for small m, T_1 is a fourth degree polynomial in m with leading term $\frac{2}{3}m^4$, or differs from it by exactly m. Then we use a computer to calculate T_1 for various m to pin down the remaining coefficients of the fourth degree polynomial.

Lemma 8.3.2. *With the notation above, for $m > 7$ in the Lin case, and for $m > 9$ in the HKM case, the number of even values of a for which $\min_{0 \le b \le 3^m - 2} \{s(b) + s(a - bd)\} = 4$ is a fourth degree polynomial in m. Furthermore, the leading term is $\frac{2}{3}m^4$.*

Proof: First we count the total number of pairs (a, b), $0 < a \le 3^m - 2$, $0 \le b \le 3^m - 2$, for which $s(b) + s(a - bd) = 4$. If $s(b) = 4$ and $s(a - bd) = 0$, then $a = bd$

and b has 3-adic representation as one of the following: four 1's and the rest 0's; two 1's, one 2, and the rest 0's; or two 2's and the rest 0's. Similarly if $s(b) = 3$ then b is either three 1's and the rest 0's; or one 1, one 2, and the rest 0's; while $a = bd + 3^i$ for some i between 0 and $m - 1$. If $s(b) = 2$ then b has either two 1's and the rest 0's; or one 2 and the rest 0's; while $a - bd$ also has one of those forms. The cases $s(b) = 1$ and $s(b) = 0$ mirror the cases $s(b) = 3$ and $s(b) = 4$.

Since $s(a - bd) = 4 - s(b)$, we can write $a = bd + x$, where $s(x) = 4 - s(b)$. So we may think of a as represented by the sum of 4 terms, each either a shift of d, or a shift of 1. Here if the 3-adic representation of b or $a - bd$ has a digit 2, then the corresponding copy of d or of 1 is viewed as $3^i d + 3^i d$, or $3^i + 3^i$ (*i.e.,* a sum of two terms). Observe that $a = bd + x$ is necessarily even because d is odd and $s(b) + s(x) = 4$ implies $b + x$ is even. Thus from the discussion in the previous paragraph the total number of pairs (a, b) for which $s(b) + s(a - bd) = 4$ and a is even is

$$\begin{aligned} & 2\binom{m}{4} + 2\binom{m}{2}(m-2) + 2\binom{m}{2} + 2\binom{m}{3}m + 2m^2(m-1) + (\binom{m}{2} + m)^2 \\ = \; & \frac{2}{3}m^4 + 2m^3 - \frac{13}{6}m^2 + \frac{1}{2}m \end{aligned} \tag{8.18}$$

In order to prove the assertion of the lemma we need to subtract from this polynomial the number of pairs (a, b) which are redundant for any value of a, as well as the number of those a's included here but which can also be represented as $bd + x$, with $s(b) + s(x) = 2$.

For convenience we will sometimes think of a and d as written using the digits 0,1, and -1 (mostly in the HKM case). Thus, if a has a 2 in it, replace it with -1 and carry 1 to the next higher place. Similarly, -2 gets replaced by 1 and -1 gets carried. With this convention, it is easy to see that the possible number of nonzero digits in a does not grow as m grows.

We now partition the above a's into classes according to the sums of four shifts of 1 or of d which produce them. If there is a carry (in the addition of the

four terms which produces a) from one place to another, we group those places together (and call these places a segment of the sum). Two values of a are in the same class if these segments of the sum involving nonzero digits have shifted, but the corresponding nonzero digits come from corresponding digits of shifts of d or shifts of 1. If the nonzero digits of two addends are disjoint from each other, and from each other's carry digits, then they are free to shift relative to each other and the sums would be considered in the same class. For instance, the following sums would produce a's in the same class:

$$\begin{array}{ccccccccc}
0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & & & & & & & & \\
1 & & & & & & & & \\
\hline
2 & 2 & 0 & 2 & 0 & 1 & 0 & 1 & 0
\end{array}
\qquad
\begin{array}{ccccccccc}
0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
 & & & & 1 & & & & \\
 & & & & 1 & & & & \\
\hline
1 & 0 & 0 & 2 & 2 & 2 & 0 & 1 & 0
\end{array}$$

but the following would represent two other classes:

$$\begin{array}{ccccccccc}
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\
 & & & 1 & & & & & \\
 & & & 1 & & & & & \\
\hline
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 2
\end{array}
\qquad
\begin{array}{ccccccccc}
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\
 & 1 & & & & & & & \\
 & & & 1 & & & & & \\
\hline
0 & 1 & 2 & 1 & 2 & 0 & 1 & 0 & 1
\end{array}$$

In the first example the addends have three degrees of freedom to shift, while in the last example there are four degrees of freedom and in the middle one there is only one degree of freedom. Thus, in the first example, there are $m = 9$ choices of shift for the first copy of d. There are only $m - 3$ choices for the second copy of d, $m - 4$ choices for the first copy of 1, and the second copy of 1 is determined by the first. Here we ignore the possibility that other values of b might be associated with some of these a's. It is also clear that the pattern remains the same if we increase m by inserting extra pairs of columns of 0's.

Now we continue the definition of classes where a given value of a is associated with more than one value of b. The following sums give an example of such a situation.

$$\begin{array}{ccccccccccc}
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & & & & & 1 & & & & & \\
1 & & & & & & & & & = & & & & & & & & & 1 \\
1 & & & & & & & & & & & & & & & & & & 1 \\
\hline
2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 2 & & 2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 2 \\
 & & & & & & & & & & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 \\
 & & & & & & & & & & 1 & & & & & & & & \\
 & & & & & & & & & = & 1 & & & & & & & & \\
 & & & & & & & & & & & & & & 1 & & & & \\
 & & & & & & & & & & \hline
 & & & & & & & & & & 2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 2
\end{array}$$

Here, two values of a_1 and a_2 will be considered to be in the same class only if the pairs (a_1, b_{1i}) and (a_2, b_{2i}) are in one-to-one correspondence such that the sum $a_1 = b_{1i}d + x_{1i}$ is a shift of $a_2 = b_{2i}d + x_{2i}$ for each i.

Each class of a has some number of degrees of freedom. The maximum is 4, in the case that the nonzero digits of the addends are totally disjoint. If two different sums $b_1d + x_1$ and $b_2d + x_2$ are the same, say both equal a, the degree of freedom of that class of a is at most 3. Otherwise, the nonzero digits of the addends are totally disjoint; hence the positions of the 2's in a, in the Lin case, or of (-1)'s in a, in the HKM case, reflect the positions of copies of d in the sum. Thus $b_1 = b_2$, contradicting our assumption that there are two different sums producing the same a.

In general, for each degree of freedom, we can pick any shift from 0 to $m-1$, except for a fixed number of possibilities that cause sectors of a to overlap. In cases

such as

$$\begin{array}{cccccccccc}
0 & 0 & & 1 & 0 & 0 & -1 & 0 & 0 & 1 \\
0 & 0 & & 1 & 0 & 0 & 1 & 0 & 0 & -1 \\
0 & 0 & -1 & 0 & 0 & & 1 & 0 & 0 & 1 \\
1 & & & & & & & & & \\
\hline
1 & 0 & & 1 & 0 & 0 & & 1 & 0 & 0 & 1
\end{array}$$

shifts of the three copies of d have a period of $m/3$. Thus the size of this class of a (ignoring other values of b) would be $(m/3)(m-3)$. So each class of a's has cardinality of a polynomial of degree equal to the number of degrees of freedom and each a in a class has the same number of associated b's. In order to prove the assertion of the lemma, we subtract from (8.18) a polynomial of degree at most three for each class of a for which the number of associated b is more than one. We also have to subtract the number of a's which we have counted but for which $\min_{0\le b\le q^m-2}\{s(b)+s(a-bd)\}=2$. These cases have at most two degrees of freedom, so we subtract from (8.18) another polynomial of degree at most two.

Finally the following sums for $m=7$ (in the Lin case) and $m=9$ (in the HKM case) represent the only classes of a for those m for which a sequence of carries continues from one nonzero digit of d to the next.

$$\begin{array}{cccccccccc}
0 & 0 & 0 & 2 & 0 & 0 & 1 & = & d \\
0 & 0 & 2 & 0 & 0 & 1 & 0 & = & 3d \\
0 & 2 & 0 & 0 & 1 & 0 & 0 & = & 9d \\
2 & 0 & 0 & 1 & 0 & 0 & 0 & = & 27d \\
\hline
0 & 0 & 0 & 0 & 1 & 1 & 2 & = & 3^2+3+2
\end{array} \tag{8.19}$$

$$
\begin{array}{cccccccccc}
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & = & d \\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & = & d \\
0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & = & 3d \\
1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & = & 9d \\
\hline
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & &
\end{array}
$$

$$
\begin{array}{cccccccccc}
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & = & 3^6 d \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & = & 3^7 d \\
1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & = & 3^8 d \\
 & & & & & 1 & & & & = & 3^3 \\
\hline
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & &
\end{array}
\tag{8.20}
$$

In each of these two cases we have two values of b associated with the same a, while for all higher m, we get two different values of a for the corresponding sums. That is, these sums are special, and would not happen if the number m of digits is large. So for $m > 7$ in the Lin case, and for $m > 9$ in the HKM case, the number of even a such that $\min_{0 \le b \le 3^m - 2} \{s(b) + s(a - bd)\} = 4$ is a fourth degree polynomial in m with leading term $\frac{2}{3}m^4$. □

We proceed to compute $T_1 = |\mathcal{T}_1| = |\{a \mid 0 < a < 3^m - 1, 2|a, t_d(a) = 4\}|$. By (8.17), we see that

$$T_1 = |\mathcal{A} \setminus \mathcal{B}| + |\mathcal{C}|,$$

where

$$
\begin{aligned}
\mathcal{A} &= \{a \mid 0 < a < 3^m - 1, 2|a, \min_{0 \le b \le 3^m - 2}\{s(b) + s(a - bd)\} = 4\}, \\
\mathcal{B} &= \{a \mid 0 < a < 3^m - 1, 2|a, \min_{0 \le b \le 3^m - 2}\{s(b) + s(a - bd)\} = 4 \text{ and } t_d(a) > 4\}, \\
\mathcal{C} &= \{a \mid 0 < a < 3^m - 1, 2|a, \min_{0 \le b \le 3^m - 2}\{s(b) + s(a - bd)\} = 2 \text{ and } t_d(a) = 4\}.
\end{aligned}
$$

By Lemma 3.2, for $m > 7$ in the Lin case, and for $m > 9$ in the HKM case, $|\mathcal{A}|$ is a polynomial in m of degree 4 with leading term $\frac{2}{3}m^4$. We will show that

$|\mathcal{B}|$ is a polynomial in m of degree at most 3. In order to compute $|\mathcal{B}|$, we have to distinguish those classes of a in $\mathcal{A}$ for which $t_d(a) = 4$, and those for which $t_d(a) > 4$, that is, decide whether

$$\tilde{\mathfrak{P}}^4 \parallel \frac{1}{3^m - 1} \sum_{b=0}^{3^m-2} g(\omega^{-b}) g(\omega^{bd-a})$$

or

$$\tilde{\mathfrak{P}}^5 \mid \frac{1}{3^m - 1} \sum_{b=0}^{3^m-2} g(\omega^{-b}) g(\omega^{bd-a}).$$

The distinction can be made with the help of Stickelberger's congruence for Gauss sums as stated in the following theorem.

Theorem 8.3.3. ([29, p. 7]) *Let r be an integer with $0 \leq r < q - 1 = p^m - 1$ and with p-adic expansion*

$$r = r_0 + r_1 p + \cdots + r_{m-1} p^{m-1}$$

with $0 \leq r_i \leq p - 1$. Define

$$\gamma(r) = r_0! r_1! \cdots r_{m-1}!$$

Then with $s(r)$ and ω as above we have the congruence

$$\frac{g(\omega^{-r})}{(\xi_p - 1)^{s(r)}} \equiv \frac{-1}{\gamma(r)} \pmod{\tilde{\mathfrak{P}}}.$$

Lemma 8.3.4. *For $m > 7$ in the Lin case, and for $m > 9$ in the HKM case, $|\mathcal{B}|$ is a polynomial in m of degree at most 3.*

Proof: Given an integer r, $0 \leq r < 3^m - 1$, since $\tilde{\mathfrak{P}} \mid 3$, we have $\gamma(r) \equiv 1$ or $\gamma(r) \equiv -1 \pmod{\tilde{\mathfrak{P}}}$, depending on whether the 3-adic representation of r has an even number of twos or an odd number of twos. Given $a \in \mathcal{A}$, applying Stickelberger's congruence to those terms in the sum $\sum_{b=0}^{3^m-2} g(\omega^{-b}) g(\omega^{bd-a})$ for which $s(b) + s(a - bd) = 4$ we get

$$\frac{g(\omega^{-b}) g(\omega^{bd-a})}{(\xi_3 - 1)^4} \equiv \gamma(b)\gamma(a - bd) \pmod{\tilde{\mathfrak{P}}}.$$

Summing over these b's, noting that $\tilde{\mathfrak{P}}||(\xi_3 - 1)$, we see that $a \in \mathcal{B}$ iff

$$\sum_{s(b)+s(a-bd)=4} \gamma(b)\gamma(a-bd) \equiv 0 \pmod 3.$$

For example in (8.19), $m = 7$, for $a = 3^2 + 3 + 2$, we have two b's such that $s(b) + s(a - bd) = 4$. The first is $b = 1111$ (and $a - bd = 0$). The second is $b = 0$ (and $a - bd = 112$). Since $\gamma(1111)\gamma(0)+\gamma(0)\gamma(112) = 1\cdot 1+1\cdot(-1) = 0$, we conclude that this a is in $\mathcal{B}$. Similarly, in (8.20), $m = 9$, for $a = -3 - 3^2 - 3^3 - \cdots - 3^8$, we also have two b's such that $s(b) + s(a - bd) = 4$, namely, $b = 112$ (and $a - bd = 0$), or $b = 111$ (and $a - bd = 1000$). Again the sum $\gamma(112)\gamma(0) + \gamma(111)\gamma(1000)$ is 0, and so this a is in $\mathcal{B}$.

We observe that if an $a \in \mathcal{A}$ is in $\mathcal{B}$, then the whole class to which a belongs is in $\mathcal{B}$. The reason is given as follows. By definition, within each class of a's, the set of b's for which $s(b) + s(a - bd) = 4$ for one a have 3-adic representations which are permutations of the 3-adic representations of the b's corresponding to any other a in that class, and since the 3-adic representations of the corresponding values of $a - bd$ are also permutations of each other, the set of values of $\gamma(b)\gamma(a - bd)$ are the same for each a in a class, therefore for two a's in the same class, the corresponding $t_d(a)$'s are either both equal to 4 or both greater than 4.

Finally note that if an element $a \in \mathcal{A}$ is in $\mathcal{B}$ then there are more than one b such that $s(b) + s(a - bd) = 4$. By the discussion in the proof of Lemma 3.2, the size of these classes of a is a polynomial in m of degree at most 3 when $m > 7$ in the Lin case, and $m > 9$ in the HKM case. Hence the conclusion of the lemma follows. □

We were not able to determine $\mathcal{C}$ completely. However from our work in [13], we know that when $m > 3$, in both the Lin and HKM cases, there is only one value of a (and its cyclic shifts) satisfying

$$\min_{0\le b\le q^m-2} \{s(b) + s(a - bd)\} = 2$$

but $t_d(a) > 2$. Hence $|\mathcal{C}| = 0$ or m. The a's which are possibly in $\mathcal{C}$ are given below. In the Lin case we have:

$$\begin{array}{cccccccccc} 0 & 0 & \cdots & 0 & 2 & 0 & \cdots & 1 & = & d \\ 0 & 0 & \cdots & 0 & 2 & 0 & \cdots & 1 & = & d \\ \hline 0 & 0 & \cdots & 1 & 1 & 0 & \cdots & 2 & = & a \end{array} \qquad \begin{array}{cccccccccc} 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 2 & = & 3^{\frac{m+1}{2}}d \\ & & \cdots & & 1 & & \cdots & & = & 3^{\frac{m-1}{2}} \\ \hline 0 & 0 & \cdots & 1 & 1 & 0 & \cdots & 2 & = & a \end{array} \tag{8.21}$$

while in the HKM case we have:

$$\begin{array}{ccccccccccccc} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -1 & 0 & \cdots & 0 & 1 & = & d \\ 0 & \cdots & 0 & -1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1 & = & 3^{m/3}d \\ \hline 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 2 & = & a \end{array} \tag{8.22}$$

Using MAPLE to compute $|\mathcal{A}\backslash\mathcal{B}|$ up to $m = 27$, we get the following theorem.

Theorem 8.3.5. *Let $q = 3$. The number of 3's in the Smith normal form of the Lin difference sets when $m > 7$ is*

$$\frac{2}{3}m^4 - 4m^3 - \frac{14}{3}m^2 + 39m + \delta(m) \cdot m.$$

The number of 3's in the Smith normal form of the HKM difference sets when $m > 9$ is

$$\frac{2}{3}m^4 - 4m^3 - \frac{28}{3}m^2 + 62m + \epsilon(m) \cdot m.$$

The values of $\delta(m)$ and $\epsilon(m)$ are 0 or 1.

Based on numerical evidence, we conjecture that δ and ϵ above are always 1.

By direct calculations (i.e., not using Gauss sums), the Smith normal form of the Lin difference set with $m = 9$ is:

$$1^{144}3^{1440}9^{1572}27^{1764}81^{1764}243^{1572}729^{1440}2187^{144}6561^{1},$$

where for example, 3^{1440} means the number of invariant factors of the Lin difference set which are 3 is 1440. The Smith normal form of the HKM difference set with $m = 9$ is:

$$1^{144}3^{1251}9^{1842}27^{1683}81^{1683}243^{1842}729^{1251}2187^{144}6561^{1}.$$

These computations were done by Saunders using a "LinBox" package [35, 14].

Since the two "almost" polynomial functions in Theorem 3.5 are never equal, and since the Smith normal forms of the Lin and HKM difference sets are also different when $m = 9$, we have the following conclusion:

Theorem 8.3.6. *Let m be an odd multiple of 3. The Lin and HKM difference sets with parameters $(\frac{3^m-1}{2}, 3^{m-1}, 2 \cdot 3^{m-2})$ are inequivalent when $m > 3$, and the associated designs are nonisomorphic when $m > 3$.*

The investigation reported in this chapter prompts the following question: If two cyclic difference sets with classical parameters have the same Smith normal form, are the associated designs necessarily isomorphic?

We note that certainly there are examples of nonisomorphic symmetric designs with classical parameters having the same Smith normal form. Projective planes of order 9 provide such examples. From Theorem 2.2.4 (see also [3]), we calculate that the Smith normal form of a projective plane of order p^2, p prime, is

$$1^r p^{(p^4+p^2-2r+2)} (p^2)^{(r-2)} ((p^2+1)p^2)^1,$$

where the exponents indicate the multiplicities of the invariant factors and r is the p-rank of the plane. That is, the p-rank of the plane determines the Smith normal form of the plane. There are four projective planes of order 9. The desarguesian one has 3-rank 37, while the other three all have 3-rank 41 (cf. [34]), so the three non-desarguesian projective planes have the same Smith normal form, yet they are nonisomorphic.

So far, we do not know any examples of difference sets with classical parameters which provide a negative answer to the question above. Difference set designs are special; it is of interest to investigate the above problem.

BIBLIOGRAPHY

[1] K. T. Arasu, K. J. Player, A new family of cyclic difference sets with Singer parameters in characteristic three, *Designs, Codes and Cryptography* **28** (2003), 75–91.

[2] K. T. Arasu, private communication, July, 2001.

[3] E. F. Assmus, Jr., Applications of algebraic coding theory to finite geometric problems, in *Finite Geometries: Proceedings of a Conference in Honor of T. G. Ostrom* (eds. N. L. Johnson, M. J. Kallaher, and C. T. Long), Lecture Notes in Pure and Applied Mathematics **82** (1983), 23–32.

[4] E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, Cambridge University Press, Cambridge, 1992.

[5] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra,* Addison-Wesley Publishing Company, Reading, 1969.

[6] J. Ax, The zeroes of polynomials over finite fields, *American Journal of Mathematics* **86** (1964), 255–261.

[7] M. Bardoe and P. Sin, The permutation modules for $\mathrm{GL}(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, *Journal of the London Mathematical Society* **61** (2000), 58–80.

[8] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Volume 1, Second Edition, Cambridge University Press, Cambridge, 1999.

[9] S. Black and R. List, On certain abelian groups associated with finite projective geometries, *Geometriae Dedicata* **33** (1990), 13–19.

[10] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms,* Cambridge University Press, Cambridge, 1994.

[11] D. B. Chandler, P. Sin, and Q. Xiang, The invariant factors of the incidence matrices of points and subspaces in $\mathrm{PG}(n, q)$ and $\mathrm{AG}(n, q)$, submitted to *Transactions of the American Mathematical Society.*

[12] D. B. Chandler and Q. Xiang, The invariant factors of some cyclic difference sets, *Journal of Combininatorial Theory, Series A* **101** (2003), 131-146.

[13] D. B. Chandler and Q. Xiang, Cyclic relative difference sets and their p-ranks, *Designs, Codes and Cryptography* **30** (2003), 325–343.

[14] J.-G. Dumas, F. Heckenbach, B. D. Saunders, and V. Welker, *Simplicial Homology, a share package for GAP*, http://linalg.org/gap.html (March 2000).

[15] B. Dwork, On the rationality of the zeta function of an algebraic variety, *Amererican Journal of Mathematics* **82** (1960), 631–648.

[16] R. Evans, H. D. L. Hollmann, C. Krattenthaler, and Q. Xiang, Gauss sums, Jacobi sums and p-ranks of difference sets, *Journal of Combinatorial Theory, Series A* **87** (1999), 74–119.

[17] A. Frumkin and A. Yakir, Rank of inclusion matrices and modular representation theory, *Israel Journal of Mathematics* **71** (1990), 309–320.

[18] C. D. Godsil, Problems in algebraic combinatorics, *The Electronic Journal of Combinatorics* **2** (1995), #F1.

[19] N. Hamada, The rank of the incidence matrix of points and d-flats in finite geometries, *Journal of Science of the Hiroshima University, Series A-I* **32** (1968), 381–396.

[20] T. Helleseth, P. V. Kumar, and H. M. Martinsen, A new family of ternary sequences with ideal two-level autocorrelation, *Designs, Codes and Cryptography*, **23** (2001), 157–166.

[21] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, Springer, 1990.

[22] I. M. Isaacs, *Algebra, A Graduate Course*, Brooks/Cole Publishing Company, Pacific Grove, CA, 1994.

[23] G. D. James, *Representations of General Linear Groups*, Cambridge University Press, Cambridge, 1984.

[24] W. M. Kantor, On incidence matrices of finite projective and affine spaces, *Mathematische Zeitschrift* **124** (1972), 315–318.

[25] M. Klemm, Elementarteiler von Inzidenzmatrizen symmetrischer Blockpläne, *Geometriae Dedicata* **21** (1986), 349–356.

[26] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Second Edition, Springer, 1984.

[27] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Mathematical Society Lecture Note Series **74**, Cambridge University Press, 1983.

[28] E. S. Lander, *Topics in algebraic coding theory*, D. Phil. Thesis, Oxford University, 1980.

[29] S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.

[30] R. Liebler, personal communication (2002).

[31] C. C. MacDuffee, *The Theory of Matrices*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Volume 2, Chelsea Publishing Company, 1946.

[32] J. MacWilliams and H. B. Mann, On the p-rank of the design matrix of a difference set, *Information and Control* **12** (1968), 474–488.

[33] J.-S. No, D.-J. Shin, T. Helleseth, On the p-ranks and characteristic polynomials of cyclic difference sets, *Designs, Codes and Cryptography* **33** (2004), 23–37.

[34] H. E. Sachar, *Error-correcting Codes Associated with Finite Projective Planes*, Ph.D. Thesis, Lehigh University, Bethlehem, PA, 1973.

[35] B. D. Saunders, personal communication.

[36] P. Sin, The invariant factors of the incidence matrices of points and hyperplanes in $P^n(\mathbb{F}_q)$, preprint.

[37] P. Sin, The elementary divisors of the incidence matrices of points and linear subspaces in $P^n(\mathbb{F}_p)$, *Journal of Algebra* **232** (2000), 76–85.

[38] K. J. C. Smith, *Majority Decodable Codes Derived from Finite Geometries*, (Ph.D. Thesis), Mimeograph Series 561, Institute of Statistics, Chapel Hill, NC, 1967.

[39] L. Stickelberger, Über eine Verallgemeinerung der Kreistheilung, *Mathematische Annalen* **37** (1890), 321–367.

[40] D. Wan, A Chevalley-Warning approach to p-adic estimates of character sums, *Proceedings of the Amererican Mathematical Society* **123** (1995), 45–54.

[41] L. C. Washington, *Introduction to Cyclotomic Fields*, Second edition. Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.

[42] R. M. Wilson, A diagonal form for the incidence matrix of t-subsets *vs.* k-subsets, *European Journal of Combinatorics* **11** (1990), 609–615.

[43] Q. Xiang, Recent results on difference sets with classical parameters, *Proceedings of the NATO ASI: Difference Sets, Sequences and their Correlation Properties* (A. Pott *et al.*, eds.) (1999), 419–437.